# Staatsexamenskurs Algebra

David Heider, WS18/19 & SS19

# 1 Gruppentheorie

## 1.1 Grundlagen der Gruppentheorie

**Definition (Gruppe & Kommutativität)** Eine nicht-leere Menge $G$ heißt *Gruppe*, falls eine Verknüpfung $\cdot : G \times G \to G$ mit den folgenden Eigenschaften existiert: (1) Die Verknüpfung ist *assoziativ*, d.h., $g \cdot (h \cdot k) = (g \cdot h) \cdot k$ für alle $g, h, k \in G$, (2) es gibt ein *Neutralelement* $e \in G$ mit $g \cdot e = g = e \cdot g$ für alle $g \in G$ und (3) jedes Element besitzt ein *Inverses*, d.h., für alle $g \in G$ gibt es ein $h \in G$ mit $g \cdot h = h \cdot g = e$. Gilt zudem für alle $g, h \in G$, dass $g \cdot h = h \cdot g$, so heißt die Verknüpfung *kommutativ* und die Gruppe $G$ *abelsche Gruppe*.

**Definition (Untergruppe)** Sei $G$ eine Gruppe, $U \subseteq G$. $U$ heißt *Untergruppe*, wenn gilt (1) $e \in U$, (2) $u \cdot v \in U$ für alle $u, v \in U$ und (3) $v^{-1} \in U$ für alle $v \in U$, wobei $v^{-1}$ das Inverse von $v$ in $G$ ist. Im Zeichen schreibt man $U \leq G$.

**Definition (Gruppenhomomorphismus & Kern)** Seien $G, H$ Gruppen. Eine Abbildung $\phi : G \to H$ heißt *Gruppenhomomorphismus*, falls für alle $g, h \in G$ jeweils $\phi(g \cdot_G h) = \phi(g) \cdot_H \phi(h)$ gilt, wobei $\cdot_G, \cdot_H$ die jeweiligen Verknüpfungen auf $G$ bzw. $H$ sind. Der *Kern* des Homomorphismus ist $\ker \phi = \{g \in G : \phi(g) = e_H\}$.

**Definition (Erzeugte Gruppe & Zyklische Gruppe)** Sei $G$ eine Gruppe und $S \subseteq G$ nichtleer. Wir bezeichnen mit $\langle S \rangle$ die kleinste Untergruppe von $G$ bzgl. der Inklusion, die $S$ enthält. Sie heißt *die von $S$ erzeugte Untergruppe*. Für eine einelementige Menge $S = \{g\}$ schreiben wir $\langle g \rangle = \{g^m | m \in \mathbb{Z}\rangle$ und nennen die in diesem Fall resultierende Untergruppe *zyklisch*.

**Definition (Ordnung)** Sei $G$ eine Gruppe. Die *Ordnung* eines Elements $g \in G$ ist definiert als $\mathrm{ord}(g) = |\langle g \rangle|$. Die *Gruppenordnung* der Gruppe $G$ ist $|G|$.

**Proposition (Charakterisierung der Ordnung)** Sei $G$ eine Gruppe mit Neutralelement $e$ und sei $g \in G$. Die folgenden Aussagen sind jeweils äquivalent.
(1) Für endliche Ordnungen: (i) $n = \mathrm{ord}(g)$, (ii) $n$ ist die minimale natürliche Zahl mit $g^n = e$, (iii) $g^m = e_G \Leftrightarrow n | m$ und (iv) $\langle g \rangle \simeq \mathbb{Z}/n\mathbb{Z}$.
(2) Für unendliche Ordnung: (i) $\mathrm{ord}(g) = \infty$, (ii) für alle $m \in \mathbb{N}$ ist $g^m \neq e$, $\langle g \rangle \simeq \mathbb{Z}$.

**Proposition (Kleiner Satz von Fermat)** Sei $G$ eine endliche Gruppe und $g \in G$. Dann gilt $g^{|G|} = e$.

**Rezept (Euler-Φ-Funktion)** Die Anzahl der Elemente der Ordnung $d$ in einer zyklischen Gruppe endlicher Ordnung $n$ kann mithilfe der *Euler-Φ-Funktion* bestimmt werden. Diese ist definiert als $\Phi(d) = |\{m \in \mathbb{N} | m \leq d, \mathrm{ggT}(d,m) = 1\}|$. Falls $d|n$, gibt es genau $\Phi(d)$ Elemente der Ordnung $d$ in $G$. Eine effektive Berechnung ist mithilfe der folgenden Identitäten möglich: (i) Sind $l, m \in \mathbb{N}$ teilerfremd, so gilt $\Phi(l \cdot m) = \Phi(l) \cdot \Phi(m)$. Für eine Primzahl $p$ und $m \in \mathbb{N}$ ist $\Phi(p^m) = (p-1)p^{m-1}$.

**Definition (Linksnebenklasse & Repräsentanten)** Sei $G$ eine Gruppe und $U \leq G$. Eine *Linksnebenklasse* von $U$ in $G$ ist dann eine Menge der Form $gU = \{gu | u \in U\}$, wobei das Element $g \in G$ als *Repräsentant* der Nebenklasse bezeichnet wird.

**Proposition (Charakterisierung von Linksnebenklassen)** Folgende Aussagen sind äquivalent:
(1) $gU = hU$
(2) $gU \cap hU \neq \emptyset$
(3) $g \in hU$
(4) $h^{-1}g \in U$.

**Definition (Index)** Bezeichne die Menge der Linksnebenklassen einer Untergruppe $U$ von einer Gruppe $G$ als $G/U$. Der *Index von $U$ in $G$* ist definiert als $(G : U) = |G/U|$.

**Satz (Satz von Lagrange)** Sei $G$ eine endliche Gruppe und $U \leq G$. Dann ist $\|G| = (G : U)|U|$.

**Definition (Normalteiler)** Sei $G$ eine Gruppe und $N \leq G$. $N$ heißt *Normalteiler von $G$*, im Zeichen, $N \trianglelefteq G$, wenn eine der folgenden, äquivalenten Bedingungen erfüllt ist:
(1) $gN = Ng$ für alle $g \in G$
(2) $gNg^{-1} = N$ für alle $g \in G$
(3) $gNg^{-1} \subseteq N$ für alle $g \in G$.

**Proposition (Hilfreiches über Normalteiler)** (1) Jede Untergruppe vom Index 2 ist ein Normalteiler.
(2) Normalteiler sind genau die Kerne von Homomorphismen. Ist $\phi : G \to H$ ein Gruppenhomomorphismus, so gilt $\ker \phi \trianglelefteq G$. Umgekehrt ist jeder Normalteiler $N \trianglelefteq G$ Kern des *Kanonischen Epimorphismus* $\pi : G \to G/N, g \mapsto gN$.

**Definition (Faktorgruppe)** Sei $G$ eine Gruppe, $N \trianglelefteq G$. Mit der Verknüpfung $\cdot_{G/N} : G/N \times G/N \to G/N, (gN, hN) \mapsto (gN) \cdot_{G/N} (hN) = (g \cdot_G h)N$ wird $G/N$ zu einer Gruppe, der sogenannten *Faktorgruppe*.

**Satz (Homomorphiesatz)** Seien $G, H$ Gruppen, sowie $N \trianglelefteq G$ ein Normalteiler. Ist $\phi : G \to H$ ein Homomorphismus mit $N \subseteq \ker \phi$. Dann gibt es einen eindeutig bestimmten Homomorphismus $\bar{\phi} : G/N \to H$, sodass $\bar{\phi} \circ \pi = \phi$, wobei $\pi$ der kanonische Epimorphismus $\pi : G \to G/N$ ist und sodass gilt (1) $\bar{\phi}$ ist injektiv genau dann wenn $\ker \phi = N$ und (2) $\bar{\phi}$ ist genau dann surjektiv, wenn $\phi$ surjektiv ist. Insbesondere induziert $\phi$ einen Isomorphismus $\bar{\phi} : G/\ker \phi \simeq G$.

**Satz (Isomorphiesätze)** Sei $G$ eine Gruppe.
(1) Ist $U \subseteq G$ Untergruppe, $N \trianglelefteq G$ ein Normalteiler, so ist das Komplexprodukt $UN \subseteq G$ eine Untergruppe, $N \trianglelefteq UN$ und $U \cap N \trianglelefteq U$ und es gilt $U/(U \cap N) \simeq UN/N$.
(2) Sind $N, M \trianglelefteq G$ und $N \subseteq M \subseteq G$, so gilt auch $N \trianglelefteq M$ und $M/N \trianglelefteq G/N$ sowie $(G/N)/(M/N) \simeq G/M$.

**Satz (Elementarteilersatz)** Sei $G$ eine endliche erzeugte abelsche Gruppe. Dann gibt es eindeutig bestimmte Zahlen $r, s \in \mathbb{N}$ sowie $\epsilon_1 ... \epsilon_s \in \mathbb{N}$ mit $\epsilon_1 | ... | \epsilon_s$ und $G \simeq \mathbb{Z}/\epsilon_1\mathbb{Z} \oplus ... \oplus \mathbb{Z}/\epsilon_s\mathbb{Z} \oplus \mathbb{Z}^r$. Die $\epsilon_1, ..., \epsilon_s$ heißen *Elementarteiler* von $G$. $r$ heißt *Rang* von $G$.

**Satz (Hauptsatz über endlich erzeugte abelsche Gruppen)** Sei $G$ eine endlich erzeugte abelsche Gruppe. Dann gibt es eindeutig bestimmte $r, s \in \mathbb{N}$ sowie nicht notwendigerweise verschiedene Primzahlen $p_1, ..., p_s$ und $n_1, ..., n_s \in \mathbb{N}$ mit $G \simeq \mathbb{Z}/p_1^{n_1}\mathbb{Z} \oplus ... \oplus \mathbb{Z}/p_s^{n_s}\mathbb{Z} \oplus \mathbb{Z}^r$.

**Proposition (Nützliches über Gruppen von Primzahl-(quadrat-)Ordnung)** Sei $G$ eine Gruppe, $p$ eine Primzahl.
(1) Ist $|G| = p$, so ist $G$ zyklisch.
(2) Ist $|G| = p^2$, so ist $G$ abelsch.

## 1.2 Gruppenoperationen

**Definition (Gruppenoperation)** Sei $G$ eine Gruppe und $X$ eine beliebige Menge. Eine *Gruppenoperation von $G$ auf $X$* ist eine Abbildung $\cdot : G \times X \to X$, sodass für $g, h \in G$ die Gleichungen $e \cdot x = x \, \forall x \in X$ und $g \cdot (h \cdot x) = (g \cdot_G h) \cdot x \, \forall x \in X$ erfüllt sind.Dabei bezeichnet $e$ das Neutralelement von $G$.

**Proposition (Zusammenhang Homorphismen und Gruppenoperation)** Sei $G$ eine Gruppe, $X$ eine Menge.
(1) Ist $\cdot : G \times X \to X$ eine Gruppenoperation, so ist die Abbildung $G \to \mathrm{Per}(X), g \mapsto \tau_g$ mit $\tau_g : X \to X, x \mapsto g \cdot x$ ein Gruppenhomomorphismus.
(2) Sei umgekehrt $\phi : G \to \mathrm{Per}(X)$ ein Gruppenhomomorphismus. Dann definiert $\cdot : G \times X \to X, (g, x) \mapsto \phi(g)(x)$ eine Gruppenoperation.

**Definition (Bahnen und Stabilisator)** Sei $G$ eine Gruppe, $X$ eine beliebige Menge und $\cdot : G \times X \to X$ eine Gruppenoperation.

(1) Die *Bahn* eines Elements $x \in X$ ist die Menge $G(x) = \{g \cdot x | g \in G\} \subseteq X$.
(2) Der Stabilisator von $x \in X$ ist die Menge $G_x = \{g \in G | g \cdot x = x\} \subseteq G$. Es gilt sogar $G_x \leq G$.

**Proposition (Zerlegungseigenschaft)** Die Menge aller Bahnen einer Gruppenoperation $\cdot : G \times X \to X$ einer Gruppe $G$ auf einer Menge $X$ bilden einer Zerlegung von $X$, d.h., gegeben zwei Bahnen $G(x), G(y)$ für $x, y \in X$, gilt entweder $G(x) \cap G(y) = \emptyset$ oder $G(x) = G(y)$ und die Vereinigung aller Bahnen ist ganz $X$.

**Definition (Transitive Gruppenoperation)** Sei $G$ Gruppe, $X$ Menge und $\cdot : G \times X \to X$ Gruppenoperation. Gibt es ein $a \in X$, sodass $G(a) = X$, heißt die Operation *transitiv*.

**Lemma (Berechnung der Bahnlänge)** Sei $G$ eine Gruppe und $X$ eine beliebige, aber endliche Menge. Dann gilt $|G(x)| = (G : G_x)$. Im Falle, dass auch $G$ eine endliche Gruppe ist, sind die Bahnlängen insbesondere Teiler der Gruppenordnung.

**Definition (Fixpunkt)** Sei $G$ Gruppe, $X$ Menge und $\cdot : G \times X \to X$ eine Gruppenoperation. Unter einem *Fixpunkt* der Operation versteht man ein $x \in X$, sodass $g \cdot x = x$ für alle $g \in G$ gilt. Anders formuliert sind Fixpunkte also gerade diejenigen Elemente aus $X$, deren Bahnen die Länge 1 haben.

**Satz (Bahnengleichung)** Sei $G$ eine Gruppe, die auf einer endlichen Menge $X$ operiert. Sei weiter $R$ ein Repräsentantensystem der Menge aller Bahnen der Länge $> 1$ und $F$ die Menge aller Fixpunkte der Operation. Dann gilt

$$|X| = |F| + \sum_{x \in R} (G : G_x), \tag{1}$$

die sogenannte *Bahnengleichung*.

**Proposition (Operation durch Konjugation)** $G \times G \to G, (g, h) \mapsto ghg^{-1}$ definiert eine Gruppenoperation der Gruppe $G$ auf sich selbst, die sogenannte *Operation durch Konjugation*.

**Definition (Zentrum & Zentralisator)** Operiere eine Gruppe $G$ auf sich selbst durch Konjugation.
(1) Die Menge $Z(G) = \{g \in G | gh = hg \forall h \in G\}$ heißt *Zentrum von* $G$. Es ist eine abelsche Untergruppe der i.A. nicht-abelschen Gruppe $G$ und ein Normalteiler von $G$. Es besteht aus den Fixpunkten der Operation durch Konjugation.
(2) Die Menge $C(h)$ für beliebiges $h \in G$ ist definiert als $C(h) = \{g \in G | ghg^{-1} = h\}$ und besteht aus all denjenigen Elementen aus $G$, die mit $h$ kommutieren. Dies ist der Stabilisator des Elements $h$ unter der Operation durch Konjugation.

**Satz (Klassengleichung)** Sei $G$ eine endliche Gruppe, die auf sich selbst durch Konjugation operiert. Sei $R$ ein Repräsentantensystem der Bahnen der Länge $> 1$ der Operation. Dann gilt

$$|G| = |Z(G)| + \sum_{h \in R} (G : C(h)), \tag{2}$$

die sogenannte *Klassengleichung*.

**Lemma (Auflösbarkeit von $p$-Gruppen)** Sei $G$ eine $p$-Gruppe für eine Primzahl $p$, d.h., es gibt ein $n \in \mathbb{N}$, sodass $|G| = p^n$. Dann ist das Zentrum vom $G$ nicht-trivial, also $|Z(G)| > 1$. Insbesondere sind $p$-Gruppen auflösbar.

## 1.3 Direkte und semidirekte Produkte

**Definition (Komplexprodukt)** Sei $G$ eine Gruppe und $N, M \leq G$. Das *Komplexprodukt* $NM$ ist definiert als die Menge $NM = \{nm \in G | n \in N, m \in M\}$.

**Lemma (Bijektion und Komplexprodukt)** Sei $G$ eine Gruppe, $N, M \leq G$, sodass $G = NM, N \cap M = \{e\}$ gelten. Dann ist $\sigma : G \to N \times M, nm \mapsto (n, m)$ eine (wohldefinierte) Bijektion.

**Definition (Direktes Produkt)** Sei $G$ Gruppe, $N, M \trianglelefteq G$ und $N \cap M = \{e\}$. Dann ist $NM = \{nm | n \in N, m \in M\}$ mit der von $G$ geerbten Verknüpfung eine Untergruppe von $G$, das sogenannte *innere direkte Produkt*.

**Lemma (Homomorphismus und direktes Produkt)** Seien in der Situation der obigen Definition $N, M$ dergestalt, dass $NM = G$. Dann ist $\sigma : G \to N \times M, nm \mapsto (n, m)$ Bijektion und Gruppenhomomorphismus. Anders formuliert ist das innere direkte Produkt von zwei Normalteilern isomorph zu ihrem äußeren direkten Produkt.

**Definition (Inneres Semidirektes Produkt)** Seien $N, M$ Untergruppen von $G$, sodass $N \trianglelefteq G$. Dann heißt $NM$ das *innere semidirekte Produkt* von $N$ und $M$ und es gilt $NM \leq G$.

**Definition (Äußeres Semidirektes Produkt)** Seien $N, M$ Gruppen, $\phi : M \to \mathrm{Aut}(N)$ ein Homomorphismus. Dann wird $N \times M$ mit der Verknüpfung $(n_1, m_1) * (n_2, m_2) = (n_1 \phi(m_1)(n_2), m_1 m_2)$ zu einer Gruppe. Diese heißt *äußeres semidirektes Produkt* von $N$ und $M$ und wird als $N \rtimes_\phi M$ notiert.

**Satz (Klassifikation von inneren direkten bzw. semidirekten Produkten)** Sei $G$ eine Gruppe, $N, M \leq G$.
(1) Ist $G$ inneres direktes Produkt von $N$ und $M$, d.h., gilt $N, M \trianglelefteq G$, $G = NM$ und $N \cap M = \{e\}$, so ist $G \simeq N \times M$.
(2) Ist $G$ inneres semidirektes Produkt von $N$ und $M$, d.h., ist $N \trianglelefteq G$, $G = NM$

und $N \cap M = \{e\}$, so ist $G$ isomorph zu $N \rtimes_\phi M$, wobei $\phi : M \to \mathrm{Aut}(N)$ gegeben ist durch $m \mapsto \{n \mapsto mnm^{-1}\}$.

**Proposition (Koinzidenz von direktem und semidirekten Produkt)** Seien $N, M$ Gruppen und $N$ abelsch. Das semidirekte Produkt $N \rtimes_\phi M$ ist genau dann abelsch, wenn $M$ abelsch ist und der Homomorphismus $\phi : M \to \mathrm{Aut}(N)$ trivial ist, d.h., $\phi(m) = \mathrm{id}_N$ für alle $m \in M$. In diesem Falle gilt $N \rtimes_\phi M = N \times M$.

**Proposition (Nützliche Identitäten zum Rechnen)** Sei $G = \langle g \rangle$ eine zyklische Gruppe der Ordnung $n$.
(1) Ist $H$ eine weitere Gruppe und $h \in H$ ein Element, sodass $\mathrm{ord}(h) | \mathrm{ord}(g) = n$, so existiert ein eindeutig bestimmter Homomorphismus $\phi : G \to H$ mit $\phi(g) = h$.
(2) Die Abbildung $(\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}(G), \bar{r} \mapsto \{g \mapsto g^r\}$ ist ein Isomorphismus.

**Rezept (Konstruktion nicht-abelscher Gruppen)** Ziel ist es, eine nicht-abelsche Gruppe der Ordnung $n$ zu konstruieren.
(1) Finde Zahlen $l, m$, sodass $n = lm$ und $\mathrm{ggT}(\Phi(m), l) > 1$.
(2) Sind wir in der Lage, einen nicht-trivialen Homomorphismus $\phi : \mathbb{Z}/l\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/m\mathbb{Z})$ zu finden, so liefert die vorangegangene Proposition, dass $\mathbb{Z}/m\mathbb{Z} \rtimes_\phi \mathbb{Z}/l\mathbb{Z}$ eine nicht-abelsche Gruppe der Ordnung $ml = n$ ist. Dazu gehen wir wie folgt vor:

- Da $\mathrm{Aut}(\mathbb{Z}/m\mathbb{Z}) \simeq (\mathbb{Z}/m\mathbb{Z})^\times$ und letztere Gruppe oftmals zyklisch ist, finden wir aufgrund der Anforderung an $l$, nicht-trivialer Teiler von $\Phi(m)$ zu sein, ein $a \in \mathrm{Aut}(\mathbb{Z}/m\mathbb{Z})$ mit einer Ordnung, die $l$ teilt.

- Der erste Teil der Proposition erlaubt es nun, einen Homomorphismus $\psi : \mathbb{Z}/l\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/m\mathbb{Z})$ anzugeben, sodass $\psi(\bar{1}) = a$ für das $a$ aus dem vorangegangenen Schritt. Der Homomorphismus ist ferner genau dann nichttrivial, wenn $a \neq \mathrm{id}$. Die Proposition über die Koinzidenz von direktem und semidirekten Produkt liefert nun, dass das dazugehörige äußere semidirekte Produkt nicht-abelsch ist.

## 1.4 Sylowsätze und ihre Anwendungen

**Definition ($p$-Gruppe & $p$-Sylowgruppe)** Sei $G$ eine endliche Gruppe der Ordnung $|G| = p^r m$ mit $r, m \in \mathbb{N}$ und $p$ einer Primzahl mit $p \nmid m$. Eine *$p$-Untergruppe* ist eine Untergruppe, deren Ordnung eine $p$-Potenz ist. Eine *$p$-Sylowgruppe* von $G$ ist eine maximale $p$-Untergruppe von $G$, d.h., eine Untergruppe, deren Ordnung gleich $p^r$ ist.

**Satz (0-ter Sylowsatz)** Sei $G$ eine endliche Gruppe, $p$ eine Primzahl und $p^k$ eine $p$-Potenz, sodass $p^k || G|$. Dann gibt es eine Untergruppe $U$ von $G$, sodass $|U| = p^k$.

**Satz (Sylowsätze)** Sei $G$ eine endliche Gruppe der Ordnung $|G| = p^r m$ mit $r, m \in \mathbb{N}$ und einer Primzahl $p$ mit der Eigenschaft, dass $p \nmid m$. Dann gilt:
(1) Jede $p$-Untergruppe von $G$ liegt in einer $p$-Sylowgruppe von $G$.

(2) Sind $P$ und $P'$ zwei $p$-Sylowgruppen, so existiert ein $g \in G$ mit $P = gP'g^{-1}$, d.h., je zwei $p$-Sylowgruppen sind zueinander konjugiert.
(3) Für die Anzahl $\nu_p$ der $p$-Sylowgruppen von $G$ gilt $\nu_p | m$ und $\nu_p \equiv 1 \bmod(p)$.

**Proposition (Normalteiler und Sylowsätze)** Sei $G$ eine Gruppe und $P$ eine $p$-Sylowgruppe von $G$. $P \trianglelefteq G$ genau dann, wenn $\nu_p = 1$.

**Definition (Einfache Gruppe)** Eine Gruppe $G$ heißt einfach, wenn sie neben den trivialen Normalteilern $\{e\}$ und $G$ keine weiteren Normalteiler besitzt, d.h., es gibt kein $N \leq G$, sodass $\{e\} \subsetneq N \subsetneq G$ und $N \trianglelefteq G$.

**Rezept (Finden von Normalteilern durch Elemente zählen)** Sei $G$ eine Gruppe. Ziel ist es, zu zeigen, dass es einen Primfaktor $p$ der Ordnung von $G$ gibt, sodass die zugehörige $p$-Sylowgruppe ein Normalteiler ist.
(1) Betrachte einen Primteiler $p$ von $|G|$, der nur einmal in der Primfaktorzerlegung von $|G|$ vorkommt und sei $\nu_p$ die Anzahl der $p$-Sylowgruppen. Da $p$ eine Primzahl ist, sind laut dem Satz von Lagrange alle Elemente außer dem Neutralelement Erzeuger der $p$-Sylowgruppe. Das bedeutet, dass zwei verschiedene $p$-Sylowgruppen nur das Neutralelement gemeinsam haben können. Die Anzahl der Elemente der Ordnung $p$ ist also $\nu_p \cdot (p-1)$.
(2) Verfahre ebenso mit den anderen Primteilern.
(3) Tritt ein Primfaktor $q$ mehrfach in der Primfaktorzerlegung von $|G|$ auf, so stellt es sich als deutlich schwieriger heraus, die Anzahl der verschiedenen Elemente in der $q$-Sylowgruppe zu bestimmen. Immerhin kann man aber die Elementezahl der $q$-Sylowgruppe einmal addieren, weil aufgrund der Teilerfremdheit von $p$ und $q$ die Elemente der $q$-Sylowgruppe in keiner der oben gezählten $p$-Sylowgruppe enthalten sind. Hierbei vermeide man tunlichst Mehrfachzählungen des Neutralelements.
(4) Berechne schließlich die Gesamtzahl. Ist diese echt größer als $|G|$, so muss eine der Anzahlen bereits 1 sein und die zugehörige Sylowgruppe ist ein Normalteiler von $G$, was im Widerspruch zur Annahme, $G$ sei einfach, steht.
Der dritte Schritt kann selbstverständlich übersprungen werden, falls bereits vorher die Ordnung von $G$ überschritten worden ist.

**Rezept (Finden von Normalteilern durch Operation)** Sei $G$ eine Gruppe und $p$ ein Primteiler der Gruppenordnung. Wir setzen voraus, dass bereits bekannt ist, dass $\nu_p \in \{1, q\}$ für ein $q \in \mathbb{N}$.
(1) Annahme: $\nu_p = q$. Andernfalls wäre die einzige $p$-Sylowgruppe ein Normalteiler und wir wären bereits fertig. Bezeichne die Menge der $p$-Sylowgruppen mit $\mathrm{Syl}_p$.
(2) Betrachte die Operation von $G$ auf $\mathrm{Syl}_p$ gegeben durch $\cdot : (g, P) \mapsto gPg^{-1}$, sowie den daraus nach dem Korrespondenzsatz zwischen Homomorphismen und Gruppenoperationen den äquivalenten Homomorphismus $\phi : G \to \mathrm{Per}(\mathrm{Syl}_p), g \mapsto \tau_g$ mit $\tau_g(P) = gPg^{-1}$.
(3) Der Kern dieses Homomorphismus ist stets ein Normalteiler. Um zu beweisen, dass dieser nichttrivial ist, führt man zwei Widerspruchsbeweise: Wäre $\ker\phi = \{e\}$, so wäre $|\mathrm{im}\phi| = |G|$ und somit müsste $|G|||\mathrm{Per}(\mathrm{Syl}_p)| = q!$. Mit Glück stimmt das nicht. Wäre $\ker\phi = G$, so wäre $\tau_g = \mathrm{id}$ für alle $g \in G$. Damit folgt aber $gPg^{-1} = P$

und die $p$-Sylowgruppe ist somit ein Normalteiler von $G$. Das bedeutet aber, dass $\nu_p = 1$ im Widerspruch zu $\nu_p \neq 1$.

**Lemma (Mächtigkeit semidirekter Produkte)** Sei $N \trianglelefteq G$ und $M \leq G$ mit $N \cap M = \{e\}$ und $MN = G$. Dann gilt $|MN| = |M||N|$.

**Rezept (Isomorphie-Typ mittels Sylowsätze)** Sei $G$ eine endliche Gruppe, sodass die Primfaktorzerlegung von $|G|$ höchstens Quadrate (aber keine höhere Potenzen) enthält. Oft funktioniert Folgendes:
(1) Zeige, dass alle Sylowuntergruppen Normalteiler sind.
(2) Zeige, dass $G$ das innere direkte Produkt seiner Sylowuntergruppen ist (bilde hierzu ggf. schrittweise das innere direkte Produkt).
(3) Da das innere direkte Produkt stets isomorph zum äußeren direkten Produkt ist, lässt sich $G$ als äußeres direktes Produkt seiner Sylowuntergruppen schreiben.
(4) Eine Gruppe der Ordnung $p^2$ ist entweder isomorph zu $\mathbb{Z}/p^2\mathbb{Z}$ oder zu $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Eine Gruppe der Ordnung $p$ ist isomorph zu $\mathbb{Z}/p\mathbb{Z}$. Wende dies zusammen mit dem Chinesischen Restsatz sukzessive an, um die gewünschte Liste zu fabrizieren.

**Rezept (Isomorphie-Typ mittels Sylowsätze und semidirekter Produkte)** Sei $G$ eine Gruppe.
(1) Verwende die Sylowsätze, um die Anzahlen der jeweiligen Sylowgruppen von $G$ einzugrenzen. Optimalerweise ist dann eine Sylowgruppe oder ein Produkt von Sylowgruppen ein Normalteiler $N$ von $G$ und $N$ abelsch und von bekanntem Isomorphietyp, da z.B. die Ordnung von $N$ eine Primzahl ist.
(2) In aller Regel wird es nun eine Sylowgruppe $P$ von $G$ geben, die $G = NP$ und $N \cap P = \{e\}$ aus Ordnungsgründen erfüllt, von der man aber nicht weiß, ob sie ein Normalteiler ist. Dann ist $G$ zumindest isomorph zu $P \rtimes_\phi P$ mit einem Homomorphismus $\phi : P \to \mathrm{Aut}(N)$.
(3) Kann man ausschließen, dass es einen nicht-trivialen Homomorphismus $\phi : P \to \mathrm{Aut}(N)$ gibt, sodass $G \simeq P \times N$. Dazu kann man meist eine der beiden gleichwertigen Vorgehensweisen befolgen: (a) Ist $a \in P$, dann muss $\mathrm{ord}(\phi(a))|\mathrm{ord}(a)$. Sind $|P|$ und $|\mathrm{Aut}(N)|$ teilerfremd, so muss $\phi(a) = \mathrm{id}_N$ sein. Da $a$ beliebig gewählt war, folgt $\phi(a) = \mathrm{id}_N$ für alle $a \in P$ und somit ist $\phi$ trivial. (b) $\phi(P) \leq \mathrm{Aut}(N)$, sodass $|\phi(P)|||\mathrm{Aut}(N)|$. Laut Homomorphiesatz ist ebenfalls $P/\ker\phi \simeq \mathrm{Aut}(N)$, sodass $|\phi(P)|||P|$. Ist $\mathrm{ggT}(|P|, |\mathrm{Aut}(N)|) = 1$, so bleibt nur $\phi(P) = \{\mathrm{id}_N\}$, d.h., $\phi$ ist trivial.

## 1.5 Auflösbare Gruppen

**Definition (Auflösbarkeit)** Eine Gruppe $G$ heißt auflösbar, falls $G$ eine abelsche Normalreihe besitzt, d.h., es gibt ein $r \in \mathbb{N}_0$ und eine Kette von Untergruppen $G_i \subseteq G$ der Form $\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq ... \trianglelefteq G_r = G$, mit der Eigenschaft, dass $G_i/G_{i-1}$ für $i \in \{1, ..., r\}$ jeweils eine abeslche Gruppe ist.

**Lemma (Auflösbarkeit abelscher Gruppen)** Abelsche Gruppe sind auflösbar. $p$-Gruppen ebenfalls.

**Satz (Notwendiges und hinreichendes Kriterium für Auflösbarkeit)** Sei $G$ eine Gruppe, $N \trianglelefteq G$. $G$ ist auflösbar genau dann wenn $N$ und $G/N$ auflösbar sind.

**Definition (Radikalerweiterung)** Eine Körpererweiterung $L|K$ heißt *Radikalerweiterung*, wenn es ein $r \in \mathbb{N}_0$ gibt und eine Kette von Körpererweiterungen $L = K_r \supset\neq ... \supset\neq K_1 \supset\neq K_0 = K$ gibt, wobei für $i \in \{1, ..., r\}$ gilt $K_i = K_{i-1}(\alpha_i)$ mit $\alpha_i \in L$ und $\alpha_i^{e_i} \in K_{i-1}$ für ein $e_i \geq 2$. Ist $K_k$ mit $0 \leq k \leq r$ der Zerfällungskörper eines Polynoms $f \in K[x]$, so sind alle Nullstellen des Polynoms durch geschachtelte Wurzeln darstelbbar und wir nennen $f$ *durch Radikale auflösbar*.

**Satz (Notwendiges und hinreichendes Kriterium für Radikalerweiterungen)** Sei $K$ ein Körper mit der Charakteristik 0. $f \in K[x]$ ist genau dann durch Radikale auflösbar, wenn seine Galoisgruppe $\mathrm{Gal}(f) = \mathrm{Gal}(L|K)$ auflösbar ist, wo $L$ der Zerfällungskörper von $f$ ist-

**Lemma (Allgemeine Lösungsformel für Polynome vom Grad $\geq 5$)** Es gibt keine allgemeine Lösungsformel für Polynome vom Grad $\geq 5$.

**Rezept (Auflösbarkeit und Sylowsätze)** Sei $G$ eine endliche Gruppe.
(1) Finde mithilfe der Sylowsätze einen Normalteiler $N$ von $G$ und zeige, dass dieser auflösbar ist. Das ist bspw. der Fall, wenn $N$ Primzahl- oder Primzahlquadratordnung hat, da dann $N$ zyklisch bzw. abelsch, somit auflösbar, ist.
(2) Berechne die Ordnung der Faktorgruppe $G/N$ mit dem Satz von Lagrange. Ggf. reicht dies wie bei (1) bereits, um zu zeigen, dass die Faktorgruppe auflösbar ist. Sonst starte mit $G/N$ anstelle von $G$ bei (1).
(3) Das notwendige und hinreichende Kriterium für die Auflösbarkeit von Gruppen liefert dann die Auflösbarkeit der Gruppe $G$.

## 1.6 Symmetrische Gruppen

**Definition (Permutationsgruppe & Symmetrische Gruppe)** Sei $X$ eine beliebige Menge und $\mathrm{Per}(X)$ die Gruppe der bijektiven Abbildungen $X \to X$, versehen mit dem Komposition als Verknüpfung. Für den Fall, dass $X = \{1, 2, ..., n\}$ für ein $n \in \mathbb{N}$, nennen wir $\mathrm{Per}(X)$ die *symmetrische Gruppe* und bezeichnen sie mit $S_n$.

**Satz (Satz von Cayley)** Jede Gruppe der Ordnung $n$ ist zu einer Untergruppe von $S_n$ isomorph.

**Definition (Träger & Disjunktheit)** Sei $n \in \mathbb{N}$ und $\sigma \in S_n$. Dann heißt $\mathrm{supp}(\sigma) = \{k \in \{1, ..., n\} | \sigma(k) \neq k\}$ der *Träger* von $\sigma$. Zwei Permutationen $\sigma, \tau \in S_n$ heißen *disjunkt*, falls $\mathrm{supp}(\sigma) \cap \mathrm{supp}(\tau) = \emptyset$.

**Lemma (Kommutativität)** Seien $\sigma, \tau \in S_n$ zwei Permutationen mit disjunkten Trägern. Dann kommutieren $\sigma, \tau$, d.h., $\sigma \circ \tau = \tau \circ \sigma$.

**Lemma (Anzahl von $k$-Zykeln)** Sei $n \in \mathbb{N}$ und $k \in \mathbb{N}$ mit $k \leq n$. Dann gibt es genau $(k-1)! \begin{pmatrix} n \\ k \end{pmatrix}$ $k$-Zykel in der $S_n$.

**Proposition (Ordnungen in der symmetrischen Gruppe)** Seien $n, r \in \mathbb{N}$, $2 \leq k \leq n$ sowie $2 \leq k_1, ..., k_r \leq n$.
(1) Jeder $k$-Zykel in $S_n$ hat die Ordnung $k$.
(2) Sind $\sigma_1, ..., \sigma_r \in S_n$ disjunkte $k_i$-Zykel für $1 \leq i \leq r$, so hat das Produkt $\sigma_1 \circ ... \circ \sigma_r$ die Ordnung $\text{kgV}(k_1, ..., k_r)$.

**Proposition (Rechnen mit dem Signum)** Für den Signumshomomorphismus $\text{sgn} : S_n \to \{\pm 1\}$ gilt die folgende Charakterisierung: Sei $n \in \mathbb{N}$, $2 \leq k \leq n$.
(1) Jede Permutation in $S_n$ lässt sich als Produkt disjunkter Zykel darstellen.
(2) Ist $\sigma \in S_n$ ein $k$-Zykel, so gilt für diesen $\text{sgn}(\sigma) = (-1)^{k-1}$.

**Lemma (Konjugation in der symmetrischen Gruppe)** Seien $\sigma, \tau \in S_n$ und $\tau$ ein Zykel, $\tau = (a, b, ...)$. dann gilt $\sigma(a, b, ...)\sigma^{-1} = (\sigma(a), \sigma(b), ...)$.

**Definition (Alternierende Gruppe)** Der Kern des Signumshomomorphismus ist die *alternierende Gruppe*, $A_n \trianglelefteq S_n$ für alle $n \geq 1$.

**Lemma (Einfachheit von $A_n$)** Für $n \leq 4$ ist $A_n$ auflösbar, für $n \geq 5$ ist $A_n$ einfach.

**Definition (Zerlegungstyp)** Sei $\sigma \in S_n$ und $\sigma = \sigma_1 \circ ... \sigma_r$ eine Darstellung von $\sigma$ als Produkt disjunkter Zykel $\sigma_i$ der Länge $k_i$ mit $2 \leq k_1 \leq ... \leq k_r$. Das $r$-Tupel $(k_1, ..., k_r)$ heißt *Zerlegungstyp* von $\sigma$.

**Lemma (Zerlegungstyp und Konjugation)** Zwei Permutationen sind genau dann konjugiert zueinander wenn sie den gleichen Zerlegungstyp besitzen.

**Definition (Diedergruppe)** Die *Diedergruppe* $D_n$ ist die Symmetriegruppe des ebenen, regelmäßigen $n$-Ecks für $n \geq 2$.

**Satz (Klassifikation der Diedergruppe)** Sei $n \geq 2$ eine natürliche Zahl. Dann gibt es bis auf Isomorphie genau eine Gruppe $G$ mit den folgenden Eigenschaften:
(1) $|G| = 2n$.
(2) Es gibt Elemente $\sigma, \tau \in G$ mit $\text{ord}(\sigma) = n$ und $\text{ord}(\tau) = 2$, für die $\sigma\tau = \tau\sigma^{n-1}$ gilt.
(3) $G = \langle \sigma, \tau \rangle$.
Diese Gruppe ist gerade die oben definierte Diedergruppe $D_n$.

**Lemma (Kleinsche Vierergruppe)** Für $n = 2$ schreibt man $D_2 = V_4$ und bezeichnet $V_4$ als *Kleinsche Vierergruppe*. Für diese gilt $V_4 \trianglelefteq A_4$ und $V_4 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, sie ist also insbesondere abelsch.

# 2 Ringtheorie

## 2.1 Ringe und Ideale

**Definition (Ring)** Ein *Ring* ist eine Menge $R$ mit zwei Verknüpfungen $+ : R \times R \to R$ und $\cdot : R \times R \to R$, sodass
(1) $(R, +)$ eine kommutative Gruppe ist,
(2) $(R, \cdot)$ ein kommutatives Monoid ist,
(3) das Distributivgesetz gilt, d.h., für alle $r, s, t \in R$ die Gleichung $(r+s)t = rt+st$ erfüllt ist.
Das Neutralelement von $(R, +)$ heißt 0, das Neutralelement von $(R, \cdot)$ heißt 1.

**Definition (Teilring)** Ist $R$ ein Ring, so heißt eine Teilmenge $S \subseteq R$ *Teilring* von $R$, wenn $1 \in S$, $a - b \in S$ und $ab \in S$ für beliebige $a, b \in S$.

**Definition (Einheit, Nullteiler, Integritätsbereich, Körper)** Sei $R$ ein Ring.
(1) Ein Element $r \in R$ heißt *Einheit*, falls es ein $s \in R$ gibt, sodass $rs = 1$. Die Menge aller Einheiten von $R$ notiert man als $R^\times$ und nennt sie die *Einheitengruppe* von $R$.
(2) Ein Element $r \in R$ heißt *Nullteiler*, falls es ein $s \in R \setminus \{0\}$ gibt, sodass $rs = 0$. Es heißt *nilpotent*, falls es ein $n \in \mathbb{N}$ gibt, sodass $r^n = 0$.
(3) Ist 0 der einzige Nullteiler in $R$, so heißt $R$ *Integritätsbereich*. Äquivalent dazu ist, dass für Elemente $r, s \in R$ mit $rs = 0$ bereits $r = 0$ oder $s = 0$ gilt.
(4) Ein Ring $R$ heißt *Körper*, falls gilt $R^\times = R \setminus \{0\}$.

**Rezept (Endliche Integritätsbereiche)** Ist $R$ ein endlicher Integritätsbereich, so ist $R$ bereits Körper. Hierzu gibt es zwei Standardargumente:
(1) Sei $a \in R$ ein Element mit $a \neq 0$. Betrachte die Abbildung $\tau_a : R \to R, r \mapsto ar$, welche infolge der Integritätsbereichseigenschaft bereits injektiv ist. Da $\tau_a$ eine Abbildung zwischen endlichen und gleichmächtigen Mengen ist, muss sie bijektiv sein. Insbesondere hat also 1 ein eindeutiges Urbild $b \in R$, d.h., $1 = \tau_a(b) = ab$.
(2) Sei $a \in R$ mit $a \neq 0$. Da $R$ endlich ist, können die Potenzen von $a$ nicht alle verschieden sein, sodass es $n, m \in \mathbb{N}$ gibt, mit $n < m$ und $a^n = a^m$. Also $a^n(1 - a^{m-n}) = 0$. Da $R$ ein Integritätsbereich ist, gilt $1 - a^{m-n} = 0$ oder $a^n = 0$. Im ersten Fall ist $a$ eine Einheit, wie gewünscht. Im zweiten Fall zeigt man mittels Induktion, dass $a = 0$ ist.

**Definition (Primelement, irreduzibles Element)** Sei $R$ ein Integritätsbereich, $p \in R$ mit $p \neq 0$ und $p \notin R^\times$.
(1) $p$ heißt *Primelement*, falls für $x, y \in R$ die Implikation $p|(xy) \Rightarrow p|x$ oder $p|y$ erfüllt ist.
(2) $p$ heißt *irreduzibles Element*, falls für $x, y \in R$ die Implikation $p = xy \Rightarrow x \in R^\times$ oder $y \in R^\times$ erfüllt ist.

**Definition (Ideal, Hauptideal)** Sei $R$ ein Ring. Eine Menge $I \subseteq R$ heißt *Ideal*, falls (1) $0 \in I$, (2) $ar \in I$ und (3) $a + b \in I$ für alle $r \in R$, $a, b \in I$. Ein Ideal $I$ der

Form $I = (a) = \{ar | r \in R\}$ für ein $a \in R$ heißt *Hauptideal*. Sei $S = \{a_1, ..., a_r\} \subseteq R$ eine $r$-elementige Menge an Ringelementen, die paarweise verschieden sind und ungleich 0. Dann ist $(a_1, ..., a_r) = \{a_1 r_1 + .... + a_r r_r | r_1, ..., r_r \in R\}$ das von $S$ *erzeugte Ideal*.

**Definition (Primideal, maximales Ideal)** Sei $R$ ein Ring.
(1) Ein Ideal $\mathfrak{p} \subsetneq R$ heißt *Primideal*, falls für $x, y \in R$ die Implikation $xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p}$ oder $y \in \mathfrak{p}$.
(2) Ein Ideal $\mathfrak{m} \subsetneq R$ heißt *maximales Ideal*, falls für jedes Ideal $I \subseteq R$ die Implikation $\mathfrak{m} \subseteq I \subseteq R$ bereits folgt $I = \mathfrak{m}$ oder $I = R$.

**Satz (Nützliches über Faktorringe)** Sei $R$ ein Ring.
(1) Ein Ideal $\mathfrak{p} \subseteq R$ ist genau dann prim, wenn $R/\mathfrak{p}$ ein Integritätsbereich ist.
(2) Ein Ideal $\mathfrak{m} \subseteq R$ ist genau dann maximal, wenn $R/\mathfrak{m}$ ein Körper ist. Insbesondere ist jedes maximale Ideal auch prim, denn jeder Körper ist ein Integritätsbereich.

**Lemma (Einheitengruppen des Produktrings)** (1) Sei $R$ ein Ring. Zusammen mit der Multiplikation auf $R$, bilden die invertierbaren Elemente von $R$ eine Gruppe, die sogenannte *Einheitengruppe* $R^\times$.
(2) Sei $S$ ein weiterer Ring, dann gilt $(R \times S)^\times = R^\times \times S^\times$.

**Satz (Einheitengruppen der Restklassenringe)** Sei $n \in \mathbb{N}$ und $p$ einer Primzahl.
(1) $(\mathbb{Z}/n\mathbb{Z})^\times$ ist eine Gruppe der Ordnung $\Phi(n)$, wo $\Phi$ die Eulersche $\Phi$-Funktion bezeichnet.
(2) Ist $p$ ungerade, so gilt $(\mathbb{Z}/p^n\mathbb{Z})^\times \simeq \mathbb{Z}/(p^{n-1}(p-1)\mathbb{Z})$.
(3) Für $n \geq 2$ ist $(\mathbb{Z}/2^n\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}$.

**Definition (Normabbildung)** Sei $d \in \mathbb{Z}$ eine quadratfreie Zahl und $R = \mathbb{Z}[\sqrt{d}]$. Die *Normabbildung* ist dann definiert als $N : R \to \mathbb{Z}, a + b\sqrt{d} \mapsto a^2 - b^2 d$.

**Lemma (Eigenschaften der Normabbildung)** (1) Die Normabbildung ist *multiplikativ*, d.h., $N(rs) = N(r)N(s)$.
(2) Die Normabbildung bildet Einheiten auf Einheiten ab.

**Rezept (Verwendung der Normabbildung)** Gegeben sei ein Ring $R = \mathbb{Z}[\sqrt{d}]$, wobei $d \in \mathbb{Z}$ quadratfrei sei.
(1) Definiere die Normabbildung $N : R \to \mathbb{Z}$ durch $N(a + b\sqrt{d}) = a^2 - db^2$. Falls $d < 0$, hat diese die Darstellung $N(z) = z\bar{z}$, woran die Multiplikatvität direkt abgelesen werden kann.
(1) Die Normabbildung hat die nützliche Eigenschaft, dass $z \in R^\times$ genau dann, wenn $N(z) \in \mathbb{Z}^\times = \{\pm 1\}$.
(3) Die Einheiten $z = a + b\sqrt{d}$ in $R$ sind genau die Lösungen der Gleichung $N(z) = \pm 1$. Um die sogenannte *Pell-Fermat-Gleichung* $a^2 - b^2 d = n$ zu lösen, verwendet man meist eine der folgenden beiden Strategien: (i) Im falle, dass $d < 0$,

muss die rechte Seite positiv sein. Wir behandeln den Fall $n = 1$: Angenommen, $b \neq 0$, dann gilt $b^2 \geq 1$. Dies führt auf die Ungleichung $1 = a^2 - b^2 d \geq a^2 - d$. Falls $d \leq -2$ ist dies bereits ein Widerspruch, sodass $b = 0$. Für $d = -1$ hat man zusätzlich die Möglichkeiten $b \in \{\pm 1\}$. Man betrachtet nun den Fall $b = 0$. (ii) Man reduziere die Gleichung modulo einer geeigneten Primzahl und schließe Existenz von Lösungen $\neq \pm 1$ aus.
(4) Auch im Zusammenhang mit irreduziblen Elementen ist die Normfunktion nützlich. Denn es ist $N(z) = N(x)N(y)$ für $z = xy$. Falls $N(z)$ eine Primzahl ist, folgt bereits, dass $z$ irreduzibel ist. In allen anderen Fällen macht man die Annahme, dass $x, y \notin R^\times$. Also gilt $N(x) \neq \pm 1 \neq N(y)$. Man überprüft nun wie in in (3), ob die Pell-Fermat Gleichung lösbar ist.
(5) In Euklidischen Ringen ist jedes irreduzible Element auch ein Primelement. Daher kann das Vorgehen aus (4) dort für den Nachweis der Primelementeigenschaft herangezogen werden. Umgekehrt zeigt man, dass ein Ring nicht faktoriell ist, indem man ein irreduzibles Element findet, das nicht prim ist.

**Definition (Höhenfunktion, Hauptidealring, faktorieller Ring, euklidischer Ring)** Sei $R$ ein Integritätsbereich.
(1) Gibt es eine Abbildung $|.| : R \setminus \{0\} \to \mathbb{N}$, sodass es für beliebige $x, y \in R$ mit $y \neq 0$ stets $q, r \in R$ mit $x = qy + r$ und $|r| < |y|$ oder $r = 0$ gibt, so heißt $R$ *euklidischer Ring*. Die Abbildung $|.|$ wird als *Höhenfunktion* bezeichnet.
(2) Falls jedes Ideal $I \subseteq R$ ein Hauptideal ist, wird $R$ als *Hauptidealring* bezeichnet.
(3) Lässt sich jedes $a \in R$ mit $a \neq 0$ und $a \neq R^\times$ bis auf Assoziiertheit und Reihenfolge als Produkt irreduzibler Elemente schreiben, so ist $R$ ein *faktorieller Ring*.

**Satz (Relationen zwischen den Ringtypen)** (1) Jeder euklidische Ring ist ein Hauptidealring.
(2) Jeder Hauptidealring ist ein faktorieller Ring.
(3) Ist $K$ ein Körper, so ist $K[x]$ ein Hauptidealring.
(4) Ist $A$ ein faktorieller Ring, so ist $A[x]$ auch ein faktorieller Ring.
(5) In einem Hauptidealring ist jedes Primideal auch maximales Ideal.

**Proposition (Irreduzibilität und Primelemente in faktoriellen Ringen)** Sei $R$ ein faktorieller Ring und $p \in R \setminus \{0\}$ keine Einheit. Folgende Aussagen sind äquivalent:
(1) $p$ ist ein Primelement.
(2) $p$ ist ein irreduzibles Element.
(3) $(p)$ ist ein Primideal von $R$.

## 2.2 Rechnen in Restklassenringen

**Definition (Faktorring)** Sei $R$ ein Ring, $I \subseteq R$ Ideal. Mittels der Verknüpfungen $+ : R/I \times R/I \to R/I, (x + I, y + I) \mapsto (x + y) + I$ und $\cdot : R/I \times R/I \to R/I, (x+I, y+I) \mapsto (x \cdot y)+I$ wird $R/I$ zu einem Ring, dem sogenannten *Faktorring*.

**Rezept (Erweiterter euklidischer Algorithmus)** Sei $R$ ein euklidischer Ring mit Höhenfunktion $|.| : R \setminus \{0\} \to \mathbb{N}$. Der *euklidische Algorithmus* ist ein Verfahren, mit dem der größte gemeinsame Teiler $d$ zweier Elemente $a, b \in R$ sowie Elemente $x, y \in R$ mit $ax + by = d$ bestimmt werden können.
(1) Starte mit den folgenden beiden Zeilen

$$\begin{array}{c|cccc} 1 & - & a & 1 & 0 \\ 2 & - & b & 0 & 1 \end{array} . \tag{3}$$

(2) Dividiere nun in jedem Schritt $a_{k-1}$ durch $a_k$ mit Rest, d.h., finde $r_k, q_k$ sodass $a_{k-1} = q_k a_k + r_k$ und $|r_k| < |a_k|$ und führe die beiden Zeile aus dem Schritt (1) wie folgt weiter:

$$\begin{array}{c|cccc} k-1 & q_{k-1} & a_{k-1} & x_{k-1} & y_{k-1} \\ k & q_k & a_k & x_k & y_k \\ k+1 & q_{k+1} & r_k = a_{k-1} - q_k a_k & x_{k-1} - q_k x_k & y_{k-1} - q_k y_k \end{array} . \tag{4}$$

(3) Die letzten beiden Zeilen werden folgendermaßen aussehen.

$$\begin{array}{c|cccc} l-1 & q_{l-1} & a_{l-1} & x_{l-1} & y_{l-1} \\ l & q_l & 0 & - & - \end{array} . \tag{5}$$

Setze dann $d = a_{l-1}$ und $x = x_{l-1}$ und $y = y_{l-1}$. Das Verfahren kann bereits trunkiert werden, wenn in der Zeile eine Einheit steht.

**Rezept (Berechnung von Inversen)** Sei $R$ eine euklidischer Ring und $(p) \subseteq R$ ein Ideal. Wir berechnen das multiplikative Inverse von $q \in R$ in $R/(p)$.
(1) Bestimme mittels euklidischem Algorithmus $x, y \in R$, sodass $xp + yq = 1$.
(2) Modulo $(p)$ resultiert $(y + (p))(q + (p)) = 1 + (p)$, weswegen $y + (p) = (q + (p))^{-1}$.

**Satz (Homomorphiesatz für Ringe)** Sei $\phi : R \to S$ ein Homomorphismus von Ringen, $I \subseteq R$ ein Ideal mit $\ker \phi \subseteq I$. Dann gibt es einen eindeutig bestimmten Ringhomomorphismus $\bar{\phi} : R/I \to S$, sodass $\bar{\phi} \circ \pi = \phi$ mit dem kanonischen Ringepimorphismus $\pi : R \to R/I$. Ferner ist der Homomorphismus $\bar{\phi}$ genau dann injektiv wenn $\ker \phi = I$ und genau dann surjektiv, wenn $\phi$ surjektiv ist. Insbesondere induziert $\phi$ einen Isomorphismus von Ringen $R/\ker \phi \simeq \mathrm{im}\phi$.

**Satz (Korrespondenzsatz für Ringe)** Sei $R$ ein Ring, $I \subseteq R$ ein Ideal und $\pi : R \to R/I$ der knaonische Epimorphismus. Dann sind durch

$$\{J \subseteq R | J \text{ Ideal}, I \subseteq J\} \rightleftarrows \{\bar{J} \subseteq R/I | \bar{J} \text{ Ideal}\} \tag{6}$$

$$J \mapsto \bar{J} \equiv \pi(J) \tag{7}$$

$$J \equiv \pi^{-1}(J) \leftarrow \bar{J} \tag{8}$$

zueinander inverse Bijektionen gegeben. Es werden ferner Primideale auf Primideale abgebildet.

## 2.3 Chinesischer Restsatz und simultane Kongruenzen

**Definition (Relativ prime Ideale)** Sei $R$ ein Ring und $I, J \subseteq R$ Ideale. Gilt $I + J = R$, so nennt man $(I, J)$ ein *Paar koprimer* bzw. *relativ primer Ideale*.

**Satz (Allgemeiner chinesischer Restsatz)** Sei $R$ ein Ring, $I_1, ..., I_n \subseteq R$ eine endliche Anzahl paarweise relativ primer Ideale. Dann ist die Abbildung

$$\Pi : R/\bigcap_{i=1}^{n} I_i \to R/I_1 \times ... \times R/I_n \tag{9}$$

$$a + \bigcap_{i=1}^{n} I_i \mapsto (a + I_1, ..., a + I_n) \tag{10}$$

ein Isomorphismus von Ringen.

**Lemma (Lemma von Bézout)** Seien $a, b \in \mathbb{Z}$. Dann gibt es $x, y \in \mathbb{Z}$, sodass $xa + yb = \mathrm{ggT}(a, b)$.

**Satz (Chinesischer Restsatz in $\mathbb{Z}$)** Seien $n_1, ..., n_k \in \mathbb{Z}$ paarweise teilerfremd und definiere $n = \prod_{i=1}^{n} n_i$. Dann ist die Abbildung

$$\Pi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times ... \times \mathbb{Z}/n_k\mathbb{Z} \tag{11}$$

$$a + n\mathbb{Z} \mapsto (a + n_1\mathbb{Z}, ..., a + n_k\mathbb{Z}) \tag{12}$$

ein Isomorphismus von Ringen.

**Rezept (Lösung simultaner Kongruenzen – Strategie 1)** Gegeben sei ein System simultaner Kongruenzen $a \equiv a_i \bmod(a_i)$ für $i \in \{1, ..., l\}$.
(1) Stelle sicher, dass die $n_i$ teilerfremd sind.
(2) Löse zunächst die ersten beiden Kongruenzen. Da $n_1, n_2$ teilerfremd sind, gibt es nach Bézout $x, y \in \mathbb{Z}$, sodass $xn_1 + yn_2 = 1$. Diese Zahlen können mittels Euklidischem Algorithmus bestimmt werden. Sei nun $\Pi : \mathbb{Z}/(n_1n_2)\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ der Isomorphismus aus dem chinesischen Restsatz. Dann gilt $\Pi(\overline{xn_1}) = (\bar{0}, \bar{1})$ und $\Pi(\overline{yn_2}) = (\bar{1}, \bar{0})$. Damit findet man $\Pi(\overline{a_1yn_2 + a_2xn_1}) = (\bar{a}_1, \bar{a}_2)$. Setze nun $z = a_1yn_2 + a_2xn_1$.
(3) Gehe nun induktiv vor. Eine Lösung $z_{m-1}$ der ersten $m - 1$ Kongruenzen sei bereits konstruiert. Setze $M = \prod_{i=1}^{m-1} n_i$. Dann sind $M, n_m$ teilerfremd und eines Lösung $z_m$ des Systems $z_m \equiv z_{m-1} \bmod(M)$ und $z_m \equiv a_m \bmod(n_m)$ kann dann über das Verfahren aus Schritt (2) bestimmt werden. Da $n_i | M$ für $1 \leq i \leq m - 1$, ist dann $z_m \equiv z_{m-1} \equiv a_i \bmod(n_i)$. Insgesamt erhalten wir so, dass $z_m$ eine Lösung der ersten $m$ Kongruenzen ist.
(4) Probe: Überprüfe, dass $a = z_l$ eine Lösung der ursprünglichen Systems ist.

**Rezept (Lösung simultaner Kongruenzen – Strategie 2)** Gegeben sei ein System simultaner Kongruenzen $a \equiv a_i \bmod(n_i)$ für $i \in \{1, ..., l\}$.
(1) Stelle sicher, dass die $n_i$ paarweise teilerfremd sind.

(2) Setze $n_i' := \prod_{j=1, j\neq i}^{n} n_j$.
(3) Berechne für jedes der $n_j'$ ein Inverses $m_i$ modulo $n_i$.
(4) Setze $a = \sum_{i=1}^{l} a_i n_i' m_i$ und verifiziere, dass $a$ das Kongruenzensystem tatsächlich löst.
Die explizite Umkehrabbildung zum Isomorphismus aus dem Chinesischen Restsatz ist dann

$$\Pi^{-1} : \mathbb{Z}/n_1\mathbb{Z} \times ... \times \mathbb{Z}/n_l\mathbb{Z} \to \mathbb{Z}/\prod_{i=1}^{n} n_i\mathbb{Z}, \tag{13}$$

gegeben durch $\Pi^{-1}(\bar{a}_1, ..., \bar{a}_l) = \sum_{i=1}^{l} \bar{a}_i \bar{n_i'} \bar{m}_i$.

## 2.4 Quadrate und Legendre-Symbole

**Satz (Anzahl Quadrate in Einheitengruppen von und endlichen Körpern selbst)** Sei $q = p^n$ für ein $n \in \mathbb{N}$ und eine Primzahl $p$. (1) Der Homomorphismus $\tau : \mathbb{F}_q^\times \to \mathbb{F}_q^\times$ ist ein Gruppenhomomorphismus und wir nennen $\mathcal{Q} = \mathrm{im}\tau$ die Menge der Quadrate (ungleich Null). Es gilt $|\mathcal{Q}| = |\mathbb{F}_q/\{\bar{1}\}| = q - 1$ für $p = 2$ und $|\mathcal{Q}| = |\mathbb{F}_q^\times/\{\bar{1}, -\bar{1}\}| = (q-1)/2$ falls $p$ ungerade ist.
(2) Falls nach der Anzahl der Quadrate in ganz $\mathbb{F}_q$ gefragt ist, muss man die $\bar{0}$ noch dazuzählen.

**Definition (Quadratischer Rest, quadratischer Nicht-Rest)** Eine Zahl $a \in \mathbb{Z}$ heißt *quadratischer Rest modulo p*, falls es ein $x \in \mathbb{Z}$ gibt, sodass $x^2 \equiv a \,\mathrm{mod}(p)$. Andernfalls heißt $a$ *quadratischer Nicht-Rest modulo p*.

**Definition (Legendre-Symbol)** Für eine Primzahl $p \in \mathbb{Z}$ ist das *Legendre-Symbol* definiert als

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & x^2 \equiv a \,\mathrm{mod}(p), a \not\equiv 0 \,\mathrm{mod}(p) \\ -1 & x^2 \not\equiv a \,\mathrm{mod}(p) \\ 0 & a \equiv 0 \,\mathrm{mod}(p) \end{cases} . \tag{14}$$

**Proposition (Rechenregeln für das Legendre-Symbol)** Sei $p$ eine ungerade Primzahl und $a, b \in \mathbb{Z}$. Es gelten die folgenden Rechenregeln:
(1) $a \equiv b \,\mathrm{mod}(p) \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
(2) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \,\mathrm{mod}(p)$.
(3) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

**Satz (Quadratisches Reziprozitätsgesetz)** Seien $p \neq q$ ungerade Primzahlen. Dann gilt

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right). \tag{15}$$

**Proposition (Ergänzungssätze)** Sei $p$ eine ungerade Primzahl. Dann gilt:

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & p \equiv 1 \bmod(4) \\ -1 & p \equiv 3 \bmod(4) \end{cases}, \tag{16}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & p \equiv \pm 1 \bmod(8) \\ -1 & p \equiv \pm 3 \bmod(8) \end{cases}. \tag{17}$$

**Rezept (Berechnung von Legendre-Symbolen)** Sei $p$ eine Primzahl und $n \in \mathbb{Z}$.
(1) Zerlege $n$ in Primfaktoren, d.h., finde eine Darstellung $n = \pm \prod_{i=1}^{m} q_i^{\nu_i}$ mit Primzahlen $q_i$ und natürlichen Zahlen $\nu_i$.
(2) Nach den Rechenregeln für das Legendre-Symbol ist dann

$$\left(\frac{n}{p}\right) = \left(\frac{\pm 1}{p}\right) \prod_{i=1}^{m} \left(\frac{q_i}{p}\right)^{\nu_i}. \tag{18}$$

Hierbei reicht es, die Exponenten $\nu_i$ modulo 2 zu reduzieren, denn gerade Exponenten liefern $(\pm 1)^2 = 1$ und somit keinen Beitrag, der das Ergebnis ändert.
(3) Die einzelnen Faktoren berechnet man nun unter Verwendung des quadratischen Reziprozitätsgesetzes und anschließender Reduktion des vormaligen Nenners mittels der Kürzungsregel für das Legendre-Symbol, die in den Rechenregeln (1) aufgelistet wurde. Führt man das lange genug durch, kann man schließlich die Ergänzungssätze anwenden oder aber Rechenregel (2).

**Rezept (Nicht-Lösbarkeit quadratischer Gleichungen)** Eine häufige Anwendung des Legendre-Symbols besteht darin, die Existenz einer ganzzahligen Lösung einer Gleichung der Form $x^2 + ny^k = a$ für gewisse Zahlen $n, a \in \mathbb{Z}, k \in \mathbb{N}_0$ auszuschließen. Dazu geht man folgendermaßen vor:
(1) Wähle einen Primteiler $p$ von $n$ und reduziere die obenstehende Gleichung modulo $p$. Dann erhält man $x^2 \equiv a \bmod(p)$, d.h., $a$ ist ein quadratischer Rest modulo $p$.
(2) Berechne das Legendre-Symbol $\left(\frac{a}{p}\right)$. Ist das Ergebnis $-1$, so hat man den gewünschten Widerspruch und es kann keine ganzzahlige Lösung geben.

## 2.5 Irreduzibilität von Polynomen

**Proposition (Irreduzibilitätskriterium für Polynome kleinen Grads)** Sei $K[x]$ der Polynomring über einem Körper $K$. Ist $f$ ein Polynom aus $K[x]$ mit Grad 2 oder 3, so ist $f$ irreduzibel dann und nur dann, wenn $f$ keine Nullstellen in $K$ hat.

**Proposition (Rationale Nullstellen)** Sei $f = \sum_{k=0}^{n} a_k x^k \in \mathbb{Z}[x]$. Dann gilt für jede vollständig gekürzte Nullstelle $p/q \in \mathbb{Q}$, dass $q|a_n$ und $p|a_0$.

**Satz (Lemma von Gauss)** Sei $R$ ein Ring und $K$ sein Quotientenkörper.
(1) Jedes nicht-konstante Polynom $f \in R[x]$, das in $R[x]$ irreduzibel ist, ist auch in $K[x]$ irreduzibel.
(2) Ist $f$ primitiv, so ist $f$ genau dann irreduzibel, wenn es in $K[x]$ irreduzibel ist.

**Proposition (Zerlegung normierter Polynome über faktoriellen Ringen)** Sei $R$ ein faktorieller Ring mit Quotientenkörper $K$ und seien $f, g, h \in K[x]$ normierte Polynome mit $f = gh$. Ist $f \in R[x]$, dann gilt auch $g, h \in R[x]$.

**Lemma (Multivariater Polynomring)** Ist $R$ faktorieller Ring, so auch $R[x, y]$, was als *bivariater* bzw. allgemeiner *multivariater Polynomring* bezeichnet wird.

**Satz (Eisensteinkriterium)** Sei $R$ ein faktorieller Ring, $K$ sein Quotientenkörper und $f = \sum_{k=0}^{n} a_k x^k$ ein Polynom vom Grad $> 0$. Gibt es ein Primelement $p \in R$ mit $p \nmid a_n$, $p | a_i$ für $i \in \{0, ..., n-1\}$ und $p^2 \nmid a_0$, so ist $f$ irreduzibel über $K[x]$.

**Satz (Reduktionskriterium)** Sei $R$ ein faktorieller Ring, $p \in R$ ein Primelement und $f = \sum_{k=0}^{n} a_k x^k \in R[x]$ ein Polynom, dessen Leitkoeffizient nicht von $p$ geteilt wird. Weiter sei $\pi : R \to R/(p)$ der kanonische Epimorphismus. Ist $\pi(f) = \sum_{k=0}^{n} \pi(a_k) x^k$ irreduzibel in $R/(p)[x]$, so ist $f$ irreduzibel in $K[x]$, wobei $K$ den Quotientenkörper von $R$ bezeichnet.

**Rezept (Irreduzibilität mittels Koeffizientenvergleich)** Sei $f \in K[x]$ ein Polynom im Polynomring über einer Körper $K$ mit Grad $\geq 4$. Es genügt nun nicht mehr, die Nullstellenfreiheit von $f$ über $K$ nachzuweisen, da hier auch quadratische Faktoren in Frage kommen können.
(1) Prüfe zuerst, ob $f$ Nullstellen in $K$ hat. Wenn ja, so ist das Polynom in $K[x]$ reduzibel, da man einen Linearfaktor abspalten kann. Eine Zerlegung findet man explizit durch Ausklammern und Polynomdivision. Wenn nein, so enthält eine Zerlegung auf jeden Fall keinen Linearfaktor.
(2) Bestimme mittels Gradargumenten alle restlichen Möglichkeiten, welche Grade Teiler von $f$ haben können.
(3) Leite aus den Kombinationen von Schritt (2) Gleichungen für die Koeffizienten der in Frage stehenden Polynome ab.
(4) Aus dem Gleichungssystem aus Schritt (3) ergibt sich optimalerweise ein Widerspruch, dass so eine Zerlegung nicht möglich ist oder aber man findet eine Zerlegung für $f$. Ist die Zerlegung nicht möglich, dann ist $f$ bereits irreduzibel.

# 3 Körpertheorie

## 3.1 Algebraische Körpererweiterungen

**Definition (Körpererweiterung, Zwischenkörper)** Eine *Körpererweiterung* $L|K$ ist ein Paar von Körpern $L$ bzw. $K$ mit $K \subseteq L$. Ein *Zwischenkörper* dieser Erweiterung ist ein $M$ mit $K \subseteq M \subseteq L$.

**Definition (Grad einer Körpererweiterung, endliche Erweiterung)** Sei $L|K$ eine Körpererweiterung.
(1) Die Dimension $L$ bzw. $K$-Vektorraum wird *Grad* von $L$ über $K$ genannt und mit $[L : K]$ bezeichnet.

(2) Falls $[L : K]$ endlich ist bzw. unendlich ist, heißt $L|K$ *endliche* bzw. *unendliche* Körpererweiterung.

**Satz (Gradformel)** Sei $L|K$ eine Körpererweiterung und $M$ ein Zwischenkörper. Dann gilt $[L : K] = [L : M][M : K]$. Insbesondere ist $L|K$ genau dann endlich, wenn die Erweiterungen $L|M$ und $M|K$ beide endlich sind.

**Definition (algebraisches Element, transzendentes Element, algebraische Erweiterung)** Sei $L|K$ eine Körpererweiterung.
(1) Ein Element $\alpha \in L$ heißt *algebraisch* über $K$, wenn es ein Polynom $f \in K[x]$ gibt mit $f(\alpha) = 0$ gibt. Andernfalls heißt $\alpha$ *transzendent* über $K$.
(2) Ist jedes Element aus $L$ über $K$, so heißt $L|K$ *algebraische* Körpererweiterung.

**Proposition (Notwendiges und hinreichendes Kriterium für Algebraizität)** Sei $L|K$ eine Körpererweiterung und $M$ ein Zwischenkörper. Ist $\alpha \in L$ algebraisch über $M$ und $M|K$ algebraisch, so ist auch $\alpha$ algebraisch über $K$. Somit ist $L|K$ genau dann algebraisch, wenn $L|M$ und $M|K$ algebraisch ist.

**Proposition (Zusammenhang zur Ringtheorie)** Sei $L|K$ eine Körpererweiterung. $\alpha \in L$ ist algebraisch über $K$ genau dann wenn der *Einsetzungshomomorphismus* $\varphi_\alpha : K[x] \to L, f \mapsto f(\alpha)$ nicht injektiv ist.

**Definition (Minimalpolynom)** In der Situation der obigen Proposition und unter der zusätzlichen Forderung, dass das das Hauptideal $\ker \varphi_\alpha$ erzeugende Element $\mu_{\alpha,K}$ normiert ist, bezeichnen wir $\mu_{\alpha,K}$ als *Minimalpolynom* von $\alpha$ über $K$.

**Lemma (Nützliche Eigenschaft des Minimalpolynoms)** Sei $L|K$ eine Körpererweiterung und $\alpha \in L$ algebraisch über $K$ mit Minimalpolynom $\mu_{\alpha,K}$. Für alle $g \in K[x]$ mit der Eigenschaft $g(\alpha) = 0$ gilt $\mu_{\alpha,K}|g$.

**Proposition (Notwendiges und hinreichendes Kriterium für Minimalpolynom)** Sei $L|K$ eine Körpererweiterung, $\alpha \in L$ algebraisch über $K$ und $f \in K[x]$ ein Polynom. Dann sind die folgenden Aussagen jeweils paarweise äquivalent:
(1) $f$ ist das Minimalpolynom von $\alpha$.
(2) $f$ ist ein normiertes und irreduzibles Polynom mit der Eigenschaft $f(\alpha) = 0$.
(3) $f$ ist normiert und dasjenige Polynom minimales Grades, das $f(\alpha) = 0$ erfüllt.
(4) $f$ ist normiert und erzeugt den Kern des Einsetzungshomomorphismus $\varphi_\alpha : K[x] \to L$.

**Definition (Einfache Erweiterung)** Eine Körpererweiterung $L|K$ heißt *einfach*, falls gilt $L = K(\alpha)$ mit einem $\alpha \in L$.

**Proposition (Nützliches über Körpererweiterungen)** Sei $L|K$ eine Körpererweiterung. Dann sind (1)-(3) jeweils gleichwertig.
(1) $L|K$ ist eine endliche Erweiterung.
(2) $L|K$ ist endlich erzeugt und algebraisch.
(3) $L$ wird über $K$ von endlich vielen algebraischen Elementen erzeugt.
(4) Es gilt: $K(\alpha) = K[\alpha]$ falls $\alpha$ algebraisch über $K$.
(5) Es gilt $[K(\alpha) : K] = \deg \mu_{\alpha,K}$.

**Rezept (Berechnung von Körpererweiterung)** Viele Aufgaben erfordern das Berechnen von Graden von Körperweiterungen. Hierzu gibt es die folgenden Methoden:
(1) Der Körpererweiterungsgrad $[K(\alpha) : K]$ mit einem über $K$ algebraischen Element entspricht dem Grad des Minimalpolynoms von $\alpha$ über $K$.
(2) Erweiterungsgrade der Form $K[(\alpha, \beta) : K]$ lassen sich gegebenenfalls schrittweise bestimmen. Es ist $[K(\alpha) : K] = n, [K(\beta) : K] = m$ jeweils natürlich und nach der Gradformel gilt $n, m|[K(\alpha, \beta) : K]$, sodass $\mathrm{kgV}(n, m) \leq [K(\alpha, \beta) : K]$. Andererseits ist das Minimalpolynom von $\beta$ über $K(\alpha)$ ein Teiler vom Minimalpolynom von $\beta$ über $K$. Damit ist $[K(\alpha, \beta) : K(\alpha)] \leq [K(\beta) : K]$. Die Gradformel liefert nun die Abschätzung $[K(\alpha, \beta) : K] \leq nm$.
(3) Sind $n, m$ teilerfremd, so folgt bereits $[K(\alpha, \beta) : K] = nm$. Andernfalls kann man versuchen, das Minimalpolynom von $\alpha$ über $K(\beta)$ bzw. von $\beta$ über $K(\alpha)$ genauer zu bestimmen.
(4) Möchte man an einer gewissen Stelle $\mathbb{Q}(\alpha) = L$ ausschließen, d.h., $[L : \mathbb{Q}(\alpha)] = 1$, so bietet sich in ein Argument folgender Art an: Ist $\alpha \in \mathbb{R}$, so gilt auch $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$. Falls also $L \not\subseteq \mathbb{R}$, hat man bereits den gewünschten Widerspruch.

## 3.2 Normale und separable Erweiterungen

**Satz (Algebraischer Abschluss)** Sei $K$ ein Körper. Dann gibt es $\bar{K}$, sodass $\bar{K}|K$ algebraische Körpererweiterung ist und jedes nicht-konstante Polynom aus $K[x]$ über $\bar{K}$ in Linearfaktoren zerfällt. Dieser Körper wird *algebraischer Abschluss von* $K$ genannt.

**Definition (Zerfällungskörper)** Sei $K$ ein Körper und $f \in K[x]$ ein nicht-konstantes Polynom. Ein Erweiterungskörper $L$ von $K$ wird Zerfällungskörper von $f$ über $K$ genannt, falls (1) $f$ über $L$ Linearfaktoren zerfällt, d.h., es gibt $\alpha_1, ..., \alpha_n \in L$ und $c \in K^\times$ mit

$$f = c \prod_{i=1}^{n} (X - \alpha_i) \tag{19}$$

und (2) $L$ über $K$ von Nullstellen von $f$ erzeugt wird.

**Lemma (Form des Zerfällungskörpers)** Sei $K$ ein Körper und $\bar{K}$ ein algebraischer Abschluss, $f \in K[x]$ nicht-konstantes Polynom. Seien $\alpha_1, ..., \alpha_n \in \bar{K}$ die Nullstellen von $f$. Dann ist $L = K(\alpha_1, ..., \alpha_n)$ der eindeutige Zerfällungskörper von

$f$ über $K$ in $\bar{K}$. Verändert man den algebraischen Abschluss, dann erhält man einen zu $L$ isomorphen neuen Zerfällungskörper des Polynoms.

**Definition (Normale Erweiterung)** Eine algebraische Erweiterung $L|K$ heißt *normal*, wenn sie eine der folgenden, äquivalenten Bedingungen erfüllt:
(1) Jedes irreduzibles Polynom aus $K[x]$, das in $L$ eine Nullstelle besitzt, zerfällt über $L$ bereits in Linearfaktoren.
(2) Es gibt ein nicht-konstantes Polynom $f \in K[x]$, sodass $L$ der Zerfällungskörper von $f$ über $K$ ist.
(2) Für einen algebraischen Abschluss $\bar{L}$ von $L$ gilt die Gleichung $\mathrm{Hom}_K(L, \bar{L}) = \mathrm{Aut}_K(L)$, d.h., jeder $K$-Homomorphismus $L \to \bar{L}$ beschränkt sich zu einem $K$-Automorphismus von $L$.

**Lemma (Normalität von Erweiterungen vom Grad 2)** Sei $L|K$ eine Körperweiterung mit $[L : K] = 2$. Dann ist $L|K$ bereits normal.

**Definition (Separabilität)** Sei $L|K$ eine Körpererweiterung.
(1) Ein nicht-konstantes Polynom $f \in K[x]$ heißt *separabel*, wenn $f$ in einem algebraischen Abschluss $\bar{K}$ von $K$ nur einfache Nullstellen hat.
(2) Ein Element $\alpha \in L$ heißt *separabel*, wenn $\alpha$ algebraisch über $K$ ist und sein Minimalpolynom über $K$ separabel im Sinne von Teil (1) ist.
(3) Die gesamte Körpererweiterung $L|K$ heißt *separabel*, wenn jedes $\alpha \in L$ separabel über $K$ ist.

**Definition (Formale Ableitung)** Sei $f = \sum_{k=0}^{n} a_k x^k \in K[x]$. Die *formale Ableitung von* $f$, bezeichnet als $f'$, ist das Polynom $f' = \sum_{k=1}^{n-1} a_k k x^{k-1}$.

**Lemma (Separabilitätskriterien)** Sei $K$ ein Körper.
(1) Ein Element $\alpha \in \bar{K}$ ist genau dann mehrfache Nullstelle eines Polynoms $f \in K[x]$, wenn $f(\alpha) = 0 = f'(\alpha)$.
(2) Ein nicht-konstantes Polynom $f \in K[x]$ ist genau dann separabel wenn $f$ und $f'$ teilerfremd sind.
(3) Ein irreduzibles Polynom ist genau dann separabel wenn $f' \neq 0$.

**Proposition (Separabke Erweiterungen)** Jede algebraische Körpererweiterung eines Körpers der Charakteristik 0 und jede algebraische Erweiterung eines endlichen Körpers ist separabel.

**Definition (Vollkommene Körper)** Ein Körper $K$, für den jede Körpererweiterung $L|K$ separabel ist, heißt *vollkommener* oder *perfekter* Körper.

**Proposition (Separabilität und Zwischenkörper)** Eine Körpererweiterung $L|K$ ist genau dann separabel, wenn für jeden Zwischenkörper $M$ der Erweiterung gilt, dass $M|K$ und $L|M$ separable Erweiterungen sind.

**Satz (Satz vom primitiven Element)** Sei $L|K$ eine endliche und separable Körpererweiterung. Dann existiert ein sogenanntes *primitives* Element $\alpha \in L$, sodass $L = K(\alpha)$.

**Rezept (Bestimmung eines primitiven Elements)** Der Beweis des Satzes liefert für eine Körperweiterung der Form $L = K(\beta, \gamma)$ den Ansatz $\alpha = b\beta + c\gamma$, wobei $b, c \in K^\times$, sodass $K(\alpha) = K(\beta, \gamma)$. Bisweilen stellen sich aber andere Ansätze, wie bspw., $\gamma = \alpha\beta$ als ökonomischer heraus.

**Satz (Fortsetzungssatz)** Sei $L|K$ ein Körper, $\alpha \in L$ mit Minimalpolynom $f \in K[x]$ und $\sigma : L \to L'$ ein Körperhomomorphismus mit einem weiteren Körper $L'$. Dann gilt: (1) Ist $\tau : K(\alpha) \to L'$ eine Fortsetzung von $\sigma$, d.h., $\tau|_K = \sigma$, so ist $\tau(\alpha)$ eine Nullstelle von $f^\sigma$. (2) Ist $\beta \in L'$ eine Nullstelle von $f^\sigma$, so gibt es einen Homomorphismus $\tau : K(\alpha) \to L'$ mit $\tau(\alpha) = \beta$ und $\tau|_K = \sigma$.

**Definition ($K$-Homomorphismus, $K$-Automorphismus)** In der Situation des Fortsetzungssatzes bezeichnen wir Fortsetzungen der Identität $\mathrm{id}_K : K \to K$ als *$K$-Homomorphismus*. Die Menge der $K$-Homomorphismen von $L \to L'$ wird als $\mathrm{Hom}_K(L \to L')$. Entsprechend ist $\mathrm{Aut}_K(L \to L)$ die Menge der $K$-Automorphismen, also der bijektiven $K$-Homomorphismen von $L$ nach $L$.

## 3.3 Einheitswurzeln

**Definition (Einheitswurzeln)** Sei $K$ ein Körper und $f_n := X^n - 1 \in K[X]$. Die Menge der Nullstellen bilden eine Gruppe in $K$, die wir mit $\mu_n(K)$ bezeichnen.

**Proposition (Struktur der Gruppe der Einheitswurzeln)** Sei $n \in \mathbb{N}$ und $\bar{K}$ ein algebraisch abgeschlossener Körper. Dann ist $\mu_n(\bar{K})$ eine zyklische Gruppe. Falls $\mathrm{char}(\bar{K}) \not| n$, dann hat $\mu_n(\bar{K})$ die Ordnung $n$.

**Definition (Primitive $n$-te Einheitswurzel)** Ein Erzeuger von $\mu_n(\bar{K})$ heißt *primitive $n$-te Einheitswurzel*. Im Falle $\bar{K} = \mathbb{C}$ kann man auf kanonische Weise eine solche primitive $n$-te Einheitswurzel angeben, nämlich $\zeta_n = \exp(2\pi i/n)$.

**Definition (Kreisteilungskörper, Kreisteilungspolynom)** $\mathbb{Q}(\mu_n(\mathbb{C})) = \mathbb{Q}(\zeta_n)$ heißt $n$-ter *Kreisteilungskörper* oder *zyklotomischer Körper*. Das Minimalpolynom von $\zeta_n$ heißt *$n$-tes Kreisteilungspolynom* und wird als $\Phi_n$ notiert.

**Satz (Über Kreisteilungspolynome)** Sei $n \in \mathbb{N}$ und $\Phi_n$ das $n$-te Kreisteilungspolynom.
(1) $\Phi_n$ ist ein Polynom vom Grad $Phi(n)$, wobei $\Phi$ die Euler'sche $\Phi$-Funktion bezeichnet.
(2) Es gilt die Formel $x^n - 1 = \prod_{d|n} \Phi_d$.
(3) Für eine Primzahl $p$ gilt $\Phi_p = X^{p-1} + X^{p-2} + ... + X + 1$.

**Satz (Galoistheorie der Kreisteilungskörper)** Sei $n \in \mathbb{N}$ und $\zeta_n$ eine primitive $n$-te Einheitswurzel. Dann ist $\mathbb{Q}(\zeta)|\mathbb{Q}$ eine Galois-Erweiterung und die Abbildung $(\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q}), \bar{r} \mapsto \{\zeta_n \mapsto \zeta_n^r\}$ ist ein Isomorphismus von Gruppen.

## 3.4 Galois-Theorie

**Definition (Galois-Erweiterung, Galois-Gruppe)** Sei $L|K$ eine Körperweiterung, die normal und separabel ist. Dann heißt $L|K$ eine *Galoiserweiterung* oder *galoissch*. Die Gruppe der $K$-Automorphismen $\mathrm{Aut}_K(L)$ heißt *Galois-Gruppe* und wird als $\mathrm{Gal}(L|K)$ notiert.

**Lemma (Ordnung der Galois-Gruppe und Erweiterungsgrad)** Sei $L|K$ eine endliche Galois-Erweiterung. Dann gilt $|\mathrm{Gal}(L|K)| = [L : K]$.

**Definition (Fixkörper)** Sei $H \leq \mathrm{Gal}(L|K)$ für eine Galois-Erweiterung $L|K$. Dann heißt $L^H := \{a \in L | \sigma(a) = a \, \forall \sigma \in H\}$ *Fixkörper von* $H$.

**Lemma (Ordnung der Galois-Gruppe und Erweiterungsgrad Teil 2)** Sei $L|K$ Galois-Erweiterung mit Galois-Gruppe $\mathrm{Gal}(L|K)$. Sei ferner $H \leq \mathrm{Gal}(L|K)$ eine Untergruppe von endlichem Index. Dann gilt $(\mathrm{Gal}(L|K) : H) = [L^H : K]$.

**Satz (Hauptsatz der Galoistheorie)** Sei $L|K$ eine endliche Galoiserweiterung mit Galoisgruppe $G = \mathrm{Gal}(L|K)$. Dann sind durch

$$\begin{aligned} \{U | U \leq G\} &\longrightarrow \{M | M \text{ Zwischenkörper von } L|K\} \\ H &\mapsto L^H \end{aligned} \tag{20}$$

$$\begin{aligned} \{M | M \text{ Zwischenkörper von } L|K\} &\longrightarrow \{U | U \leq G\} \\ M &\mapsto \mathrm{Gal}(L|M) \end{aligned} \tag{21}$$

zueinander inverse, inklusionsumkehrende Bijektionen gegeben. Dabei ist $L^H|K$ genau dann normal und damit galoissch, wenn $H \trianglelefteq G$.

**Proposition (Nützliches über Galois-Erweiterungen I)** Sei $L|K$ eine endliche Galois-Erweiterung und $E$ ein Zwischenkörper, sodass auch $E|K$ galoissch ist. Die Restriktion $\mathrm{Gal}(L|K) \to \mathrm{Gal}(E|K), \sigma \mapsto \sigma|_E$ ist ein surjektiver Gruppenhomomorphismus mit Kern $\mathrm{Gal}(L|E)$. Insbesondere gilt die Isomorphie von Gruppen:

$$\mathrm{Gal}(E|K) \simeq \frac{\mathrm{Gal}(L|K)}{\mathrm{Gal}(L|E)}. \tag{22}$$

**Definition (Kompositum)** Sei $L|K$ eine Körpererweiterung und $E, E'$ seien zwei Zwischenkörper. Das Kompositum ist definiert als $E \cdot E' = E(E') = E'(E)$.

**Proposition (Nützliches über Galois-Erweiterungen II)** Sei $L|K$ eine Körpererweiterung und ferner $E, E'$ zwei Zwischenkörper dieser Erweiterung, mit der Eigenschaft, dass $E|K$ und $E'|K$ jeweils selbst endliche Galois-Erweiterungen sind. Dann gilt:
(1) Die Erweiterung $E \cdot E'|K$ ist endlich sowie galoissch und die Abbildung $\mathrm{Gal}(E \cdot E'|K) \to \mathrm{Gal}(E'|E \cap E'), \sigma \mapsto \sigma|_{E'}$ ist ein Isomorphismus von Gruppen.
(2) Der Gruppenhomomorphismus

$$\begin{aligned} \mathrm{Gal}(E \cdot E'|K) &\to \mathrm{Gal}(E|K) \times \mathrm{Gal}(E'|K) \\ \sigma &\mapsto (\sigma|_E, \sigma|_{E'}) \end{aligned} \tag{23}$$

ist injektiv. Im Falle $E \cap E' = K$ handelt es sich bei dem obigen Gruppenmonomorphismus sogar um einen Gruppenisomorphismus.

**Rezept (Isomorphie-Typ von Galois-Gruppen)** Sei $L|K$ eine endliche Galois-Erweiterung. Will man den Isomorphietyp von $\mathrm{Gal}(L|K)$ bestimmen, so könnten folgende Schritte hilfreich sein.
(1) Bestimme die Ordnung der Galois-Gruppe. Diese beträgt $[L : K]$.
(2) Welche Gruppen der Ordnung $[L : K]$ gibt es? Für kleine Ordnungen sind dies nicht allzu viele.
(3) Überprüfe charakteristische Merkmale der Gruppen aus (2):
(i) Welche Elementordnungen sind möglich? Gibt es beispielsweise ein Element der Ordnung $[L : K]$ in $\mathrm{Gal}(L|K)$, so muss die Galois-Gruppe zyklisch sein.
(ii) Ist die Gruppe abelsch? Gibt es $\sigma, \tau \in \mathrm{Gal}(L|K)$, sodass $\sigma \circ \tau \neq \tau \circ \sigma$, so kann die Galoisgruppe nicht abelsch sein.
(iii) Welche Normalteiler hat die Gruppe? In einer abelschen Gruppe ist jede Untergruppe ein Normalteiler. Wäre $\mathrm{Gal}(L|K)$ abelsch, dann müsste jede Zwischenerweiterung normal sein.
(iv) Welche Untergruppenstruktur hat die Gruppe? Eine zyklische Gruppe hat bspw. zu jedem Teiler $d$ der Gruppenordnung genau eine Untergruppe vom Index $d$. Laut Hauptsatz der Galoistheorie gibt es also genau einen Erweiterungskörper $M$ mit $[M : K] = d$, falls $textGal(L|K)$ zyklisch ist.

**Lemma (Galoisgruppe und Nullstellen von Polynomen)** Sei $L|K$ eine endliche Galoiserweiterung mit Galois-Gruppe $G = \mathrm{Gal}(L|K)$. Ferner sei $f \in K[x]$ ein nicht notwendigerweise irreduzibles Polynom mit der Eigenschaft, dass $f$ eine Nullstelle $\alpha$ in $L$ hat. Für alle $\sigma \in G$ gilt dann $f(\sigma(\alpha)) = 0 = f(\alpha)$. Umgekehrt gilt auch $f(\sigma^{-1}(\alpha)) = 0 = f(\alpha)$.

**Rezept (Explizite Bestimmung von $K$-Automorphismen)** Sei $L|K$ eine endliche Galois-Erweiterung und seien $\alpha_1, ..., \alpha_n \in L$ dergestalt, dass $L = K(\alpha_1, ..., \alpha_n)$. Will man $\mathrm{Gal}(L|K)$ explizit bestimmen, kann man beispielsweise folgendermaßen vorgehen:
(1) Finde Polynome $f_1, .., f_n$ mit möglichst kleinem Grad, die $\alpha_1, ..., \alpha_n$ als Nullstellen haben.
(2) Nach dem Satz vom primitiven Element gibt es ein $\beta \in L$, sodass $L = K(\beta)$, sodass es genügen würde, das Minimalpolynom von $\beta$ zu bestimmen. Das gestaltet

sich regelmäßig als schwierig.
(3) Die Nullstellen von $f_i$ müssen für jedes $1 \leq i \leq n$ wieder auf Nullstellen des Polynoms abgebildet werden. Dies liefert Bedingungen an die Bilder der $\alpha_1, ..., \alpha_n$ unter den $K$-Automoorphismen.
(4) Jede Relation zwischen den $\alpha_1, ..., \alpha_n$ kann weiterhelfen.
(5) Da $\alpha_1, ..., \alpha_n$ Erzeuger von $L$ als $K$-Vektorraum sind, ist jedes $\sigma \in \mathrm{Gal}(L|K)$ bereits durch $\sigma(\alpha_1), ..., \sigma(\alpha_n)$ eindeutig festgelegt.
(6) Dann bleibt bspw. mittels Fortsetzungssatz zu begründen, dass es zu den soeben erhaltenen Abbildungsvorschriften tatsächlich $K$-Homomorphismen $L \to L$ und damit dann $K$-Automorphismen gibt.

**Definition (Galoisgruppe eines Polynoms)** Sei $f \in K[x]$ ein separables Polynom über $K$ und $L$ sein Zerfällungskörper. Dann ist $L|K$ ebenfalls eine Galoiserweiterung. im Die dazugehörige Galois-Gruppe wird auch als $\mathrm{Gal}(f)$ notiert und *Galoisgruppe von $f$* genannt.

**Satz (Gruppenmonomorphismus zwischen Galoisgruppen von Polynomen und den symmetrischen Gruppen)** Sei $K$ ein Körper, $f \in K[x]$ ein separables Polynom vom Grad $n > 0$ sowie $L$ der Zerfällungskörper von $f$ über $K$. Seien $\alpha_1, ..., \alpha_n \in L$ die Nullstellen von $f$, so definiert $\mathrm{Gal}(L|K) \to \mathrm{Per}(\{\alpha_1, ..., \alpha_n\}) \simeq S_n, \sigma \mapsto \sigma|_{\{\alpha_1,...,\alpha_n\}}$ einen injektiven Gruppenhomomorphismus. Insbesondere lässt sich $\mathrm{Gal}(L|K)$ als Untergruppe der symmetrischen Gruppe $S_n$ auffassen.

## 3.5 Endliche Körper

**Definition (Charakteristik)** Sei $R$ ein Ring mit 1 und $\phi : \mathbb{Z} \to R$ ein Ringhomomorphismus gegeben durch $n \mapsto n \cdot 1$. Die *Charakteristik von $R$* ist definiert als dasjenige $n \in \mathbb{Z}$ mit $\ker \phi = n\mathbb{Z}$ und wir schreiben $n = \mathrm{char}(R)$. Im Falle, dass $R$ ein Integritätsbereich ist, ist $n \in \mathbb{P} \cup \{0\}$.

**Satz (Existenz und Eindeutigkeit endlicher Körper)** (1) Ist $p$ eine Primzahl, $n \in \mathbb{N}$, so gibt es einen Körper der Ordnung $p^n$, der als $\mathbb{F}_{p^n}$ bezeichnet wird.
(2) Ist $K$ ein Körper der Ordnung $|K| = q$ und $p = \mathrm{char}(K)$, so gibt es ein $n \in \mathbb{N}$ mit $q = p^n$ und $K \simeq \mathbb{F}_{p^n}$.

**Proposition (Einheitengruppe)** Sei $p$ eine Primzahl und $q = p^n$ für ein $n \in \mathbb{N}$. Dann ist $\mathbb{F}_q^\times$ eine zyklische Gruppe der Ordnung $q - 1 = p^n - 1$.

**Lemma (Zerfällungskörper-Eigenschaft)** Sei $P_n = X^{p^n} - X \in \mathbb{F}_p[X]$ für ein $n \in \mathbb{N}$ und eine Primzahl $p$. Dann ist $\mathbb{F}_{p^n}$ der Zerfällungskörper von $P_n$ über $\mathbb{F}_p$ und die Erweiterung $\mathbb{F}_{p^n}|\mathbb{F}_p$ ist galoissch.

**Proposition (Frobenius-Homomorphismus)** Sei $p$ eine Primzahl und $n \in \mathbb{N}$. Der *Frobenius-Homomorphismus* ist ein Körper-Homomorphismus, gegeben durch $\mathbb{F}_{p^n} \to \mathbb{F}_{p^n}, a \mapsto a^p$.

**Proposition (Freshman's dream)** Sei $p$ eine Primzahl, $n \in \mathbb{N}$. Für alle $r \in \mathbb{N}$ gilt der sogenannte *freshman's dream*, d.h., $(a+b)^{p^r} = a^{p^r} + b^{p^r}$ für beliebige $a, b \in \mathbb{F}_{p^n}$.

**Proposition (Erweiterungen endlicher Körper)** Es seien $p$ eine Primzahl, $\bar{\mathbb{F}}_p$ ein algebraischer Abschluss von $\mathbb{F}_p$ und $n, m \in \mathbb{N}$. Dann gilt die Äquivalenz $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \Leftrightarrow m|n$. Ferner gilt für die Erweiterung $\mathbb{F}_{p^n}|\mathbb{F}_p$, dass $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$.

**Definition (Primkörper)** Sei $K$ ein Körper und bezeichne $\mathcal{T}$ die Menge aller Teilkörper von $K$. Dann heißt

$$\mathrm{Prim}(K) = \bigcap_{T \in \mathcal{T}} T \tag{24}$$

der *Primkörper von* $K$. Für beliebiges $n \in \mathbb{N}$ und eine Primzahl $p$ gilt also $\mathrm{Prim}(\mathbb{F}_{p^n}) = \mathbb{F}_p$.

**Satz (Galois-Theorie endlicher Körper)** Sei $K$ ein endlicher Körper, der als Ring die Charakteristik $p$ hat, wobei $p$ eine Primzahl bezeichnet. Sei ferner $L|K$ eine endliche Körpererweiterung. Dann ist $L|K$ eine Galois-Erweiterung. Die Galois-Gruppe $\mathrm{Gal}(L|K)$ wird vom Frobenius-Homomorphismus erzeugt, d.h., $\mathrm{Gal}(L|K) = \langle \phi \rangle$, wobei $\phi : L \to L, \alpha \to \alpha^p$. Insbesondere handelt es sich um eine zyklische Gruppe der Ordnung $n$.

## 3.6 Konstruktionen mit Zirkel und Lineal

**Definition (Konstruierbarkeit)** Identifiziere $\mathbb{R}^2 \simeq \mathbb{C}$. Sei $z \in \mathbb{C}$. Er ist *konstruierbar* aus einer Menge $M \subseteq \mathbb{C}$, falls er sich durch Kombination der folgenden drei Konstruktionsschritte mit Zirkel und Lineal aus den Punkten in $M$ konstruieren lässt:
(1) Ziehen einer Verbindungsgerade durch drei Punkte.
(2) Abtragen von Streckenlängen.
(3) Zeichnen eines Kreises um einen vorgegebenen Punkt, dessen Radiuslänge in Form der Entfernung zweier Punkte gegeben ist.
Die Menge aller aus $M$ konstruierbaren Punkte wird als $\mathcal{K}(M)$ bezeichnet.

**Proposition (Körpereigenschaft der Menge aller konstruierbaren Punkte)** Sei $M \subseteq \mathbb{C}$ eine Teilmenge, sodass $\{0, 1\} \subseteq M$. Dann ist $\mathcal{K}(M)$ ein Körper.

**Lemma (Weitere Eigenschaften)** (1) $\mathcal{K}(M)$ ist invariant unter komplexer Konjugation.
(2) $\mathcal{K}(M)$ ist quadratisch abgeschlossen.
(3) Aus $z \in \mathcal{K}(M)$ folgt $\bar{z}, \sqrt{z} \in \mathcal{K}(M)$.
(4) Es gilt $\mathbb{Q}(M \cup \bar{M}) \subseteq \mathcal{K}(M)$.

**Satz (Konstruierbarkeit mit Zirkel und Lineal)** Sei $M \subseteq \mathbb{C}$ und $\{0,1\} \subseteq M$ sowie $z \in \mathbb{C}$ ein Punkt. Dann sind äquivalent:
(1) $z \in \mathcal{K}(M)$.
(2) Es gibt einen Körperturm $\mathbb{Q}(M \cup \bar{M}) = L_0 \subseteq L_1 \subseteq ... \subseteq L_n$, sodass $z \in L_n$ und jeweils $[L_i : L_{i-1}] = 2$ für alle $i \in \{1, ..., n\}$ gilt.
(3) Es gibt eine Galoiserweiterung $L|\mathbb{Q}(M \subseteq \bar{M})$, sodass $z \in L$ und $[L : \mathbb{Q}(M \cup \bar{M})]$ eine Potenz von 2 ist.

**Korollar (Implikation für das Minimalpolynom konstruierbarer Punkte)** Sei $z \in \mathcal{K}(M)$ konstruierbar. Dann gilt für $\mu_{z,\mathbb{Q}(M\cup\bar{M})} \in \mathbb{Q}(M \cup \bar{M})[x]$, dass $\deg(\mu_{z,\mathbb{Q}(M\cup\bar{M})})$ eine Potenz von 2 ist.

# 4 Lineare Algebra

## 4.1 Vektorräume und Basen

**Definition (Vektorraum)** Sei $K$ ein Körper. Sei $(V, +)$ eine nichtleere Mengen versehen mit einer Additionsverknüpfung, so dass $(V, +)$ eine abelsche Gruppe ist. Sei $\cdot : K \times V \to V$ eine zusätzliche Verknüpfung, die sogenannte Skalarmultiplikation, sodass die folgenden Distributivgesetze gelten $\lambda \cdot (\mu \cdot v) = (\lambda \cdot \mu) \cdot v$, $(\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v$, $\lambda \cdot (v + w) = \lambda \cdot v + \lambda \cdot w$, $1 \cdot v = v$. Dann heißt $(V, +, \cdot, K)$ *$K$-Vektorraum.*

**Definition (Basis)** Eine Basis $\mathcal{B}$ existiert für jeden $K$-Vektorraum und ist charakterisiert durch eine der folgenden, äquivalenten Definitionen:
(1) Linear unabhängiges Erzeugendensystem.
(2) Minimales Erzeugendensystem.
(3) Maximale, linear unabhängige Menge.
(4) Jeder Vektor besitzt eine eindeutige Darstellung als Linearkombination von Vektoren aus $\mathcal{B}$.
(2) und (3) gelten nur im Falle, dass die Basis endliche Mächtigkeit hat.

**Definition (Dimension)** Die Mächtigkeit eines Basis heißt *Dimension von $V$*, im Zeichen $\dim_K V$.

**Proposition (Isomorphie von Vektorräumen)** Sei $n \in \mathbb{N}$ und $V$ ein $n$-dimensionaler $K$-Vektorraum. Dann induziert die Koordinatenabbildung einen Isomorphismus $V \simeq K^n$ von $K$-Vektorräumen. Insbesondere sind alle $K$-Vektorräume vorgegebener positiver Dimension paarweise isomorph.

**Proposition (Darstellungsmatrix)** Seien $V, W$ zwei $K$-Vektorräume endlicher aber nicht notwendigerweise gleicher Dimension mit Basen $\mathcal{B}_V = \{v_1, ..., v_n\}$ bzw. $\mathcal{B}_W = \{w_1, ..., w_m\}$. Jede lineare Abbildung $L : V \to W$ ist durch die Bilder der Basisvektoren aus $\mathcal{B}_V$ bereits eindeutig festgelegt, sodass die gesamte Information über die lineare Abbildung in der Matrix $A = (a_{ij})_{1\leq i\leq m, 1\leq j\leq n} \in M(m \times n, K)$

festgelegt ist, wobei $L(v_j) = \sum_{i=1}^{m} a_{ij} w_i$ für alle $j \in \{1, ..., n\}$. Diese Matrix wird als *Darstellungsmatrix von L* bezeichnet und auch als $[L]_{\mathcal{B}_V, \mathcal{B}_W}$ notiert. Umgekehrt erhält man zu einer Matrix $A \in M(m \times n, K)$ durch $\phi_A^{\mathcal{B}_V, \mathcal{B}_W} : V \to W, v \mapsto Av$ eine lineare Abbildung.

**Satz (Matrizen & Lineare Abbildungen)** Die beiden Isomorphismen von $K$-Vektorräumen

$$M(n \times m, K) \to \mathrm{Hom}_K(V, W), A \mapsto \phi_A^{\mathcal{B}_V, \mathcal{B}_W} \tag{25}$$

$$\mathrm{Hom}_K(V, W) \to M(n \times m, K), L \mapsto [L]_{\mathcal{B}_V, \mathcal{B}_W} \tag{26}$$

sind zueinander invers.

**Rezept (Abzählen von Basen)** Desöfteren ist es nötig, die Anzahl der Basen bzw. Untervektorräume über einem endlichen Körper zu bestimmen. Sei dazu $V \simeq \mathbb{F}_q^n$ ein $\mathbb{F}_q$-Vektorraum der Dimension $n$, wobei $q = p^k$ für eine Primzahl $p$ und ein $k \in \mathbb{N}$.
(1) Der erste Vektor $v_1$ ist ein beliebiger Vektor aus $\mathbb{F}_q^n \setminus \{0\}$, denn der Nullvektor ist zu jedem Vektor linear abhängig. Es gibt hier also $|\mathbb{F}_q^n \setminus \{0\}| = q^n - 1$ Möglichkeiten der Wahl.
(2) Ist der $k$-te Basisvektor $v_k$ bereits gewählt, so kann $v_{k+1}$ aus allen Vektoren gewählt werden, die zu den bisher gewählten Basisvektoren linear unabhängig sind, d.h., aus $\mathbb{F}_q^n \setminus \langle v_1, ..., v_k \rangle$. Als Vektorraum über $K$ der Dimension $k$ ist $\langle v_1, ..., v_k \rangle \simeq \mathbb{F}_q^k$ und hat damit $q^k$ Elemente. Wir haben also $q^n - q^k$ Wahlmöglichkeiten für $v_{k+1}$.
(3) Die Anzahl der möglichen Basen ergibt sich durch Produktbildung

$$\#(\text{Basen}) = \prod_{k=0}^{n-1} (q^n - q^k). \tag{27}$$

(4) Um die Anzahl der $m$-dimensionalen ($m \leq n$) Untervektorräume von $V$ zu eruieren, stellen wir fest, dass es $(q^n - 1)(q^n - q) \cdot ... \cdot (q^n - q^{m-1})$ Möglichkeiten gibt, Basen der Länge $m$ zu wählen. Da aber bereits in jedem $m$-dimensionalen Untervektorraum $(q^m - 1)(q^m - q) \cdot ... \cdot (q^m - q^{m-1})$ Möglichkeiten bestehen, eine Basis zu wählen, ist die Gesamtzahl der unterschiedlichen $m$-dimensionalen Untervektorräume von $V$ gegeben durch

$$\#(m\text{-dimensionale Untervektorräume}) = \frac{\prod_{k=0}^{m-1} (q^n - q^k)}{\prod_{k=0}^{m-1} (q^m - q^k)}. \tag{28}$$

## 4.2 Diagonalisierbarkeit

**Definition (Ähnliche Matrizen)** Sei $V$ ein $K$-Vektorraum der Dimension $n$. Zwei Matrizen $A, B \in M(n \times n, K)$ heißen ähnlich, wenn es eine Matrix $T \in \mathrm{GL}_n(K)$ gibt, sodass $A = T^{-1}BT$.

**Definition (Eigenwert & Eigenraum)** Sei $V$ ein $K$-Vektorraum und $A \in M(n \times n, K)$ eine Matrix.
(1) Ein Skalar $\lambda \in K$ heißt *Eigenwert* von $A$, falls es einen Vektor $v \neq 0_V$ gibt, mit der Eigenschaft, dass $Av = \lambda v$. In diesem Fall nennt man $v$ *Eigenvektor von* $A$.
(2) Der Untervektorraum aller Eigenvektoren (zusammen mit dem Nullvektor) zu einem Eigenwert $\lambda \in K$ notieren wir als $\mathrm{Eig}(A, \lambda) = \{v \in V | Av = \lambda v\} \cup \{0_V\}$ und nenne ihn den *Eigenraum* von $A$ zun Eigenwert $\lambda$.

**Definition (Charakteristisches Polynom)** Sei $V$ ein endlich-dimensionaler $K$-Vektorraum und $A \in M(n \times n, K)$ eine Matrix. Dann heißt $\chi_A = \det(A - z \cdot E_n) \in K[z]$ das *charakteristische Polynom* von $A$.

**Satz (Bestimmung von Eigenwerten)** In der Situation der vorangegangenen Definition gilt: $\lambda \in K$ ist Eigenwert von $A$ genau dann wenn $\chi_A(\lambda) = 0$.

**Definition (Diagonalisierbarkeit)** Eine Matrix $A \in M(n \times n, K)$ heißt *diagonalisierbar (über $K$)*, wenn sie ähnlich zu einer Diagonalmatrix ist, d.h., es gibt $\lambda_1, ..., \lambda_n \in K$, sodass es ein $T \in \mathrm{GL}_n(K)$ gibt, mit der Eigenschaft, dass $\mathrm{diag}(\lambda_1, ..., \lambda_n) = T^{-1}AT$.

**Definition (Geometrische, Algebraische Vielfachheit)** Sei $K$ ein Körper, $n \in \mathbb{N}$, $M \in M(n \times n, K)$ und $\lambda_1, ..., \lambda_m \in K$ die verschiedenen Eigenwerte von $M$.
(1) Sei $\chi_M(z) = \prod_{k=1}^{m} (z - \lambda_k)^{\mu_a(M, \lambda_k)}$ eine Zerlegung des charakteristischen Polynoms über $K[z]$ in Linearfaktoren, so heißt $\mu_a(M, \lambda_k)$ die *algebraische Vielfachheit* des Eigenwerts $\lambda_k$. Sie entspricht der Vielfachheit der Nullstelle $\lambda_k$ von $\chi_M$.
(2) Die *geometrische Vielfachheit* $\mu_g(M, \lambda_k)$ des Eigenwerts $\lambda_k$ ist definiert als $\mu_g(\lambda_k, M) = \dim_K \mathrm{Eig}(M, \lambda_k)$ für $1 \leq k \leq m$.

**Lemma (Nützliches über Eigenwerte und Eigenräume)** Sei $K$ ein Körper, $n \in \mathbb{N}$ und $M \in M(n \times n, K)$.
(1) Eigenvektoren zu unterschiedlichen Eigenwerten sind linear unabhängig.
(2) Für jeden Eigenwert $\lambda \in K$ von $M$ gilt $1 \leq \mu_g(M, \lambda) \leq \mu_a(M, \lambda)$.

**Satz (Diagonalisierbarkeitskriterien)** Sei $K$ ein Körper, $n \in \mathbb{N}$ und $M \in M(n \times n, K)$. Dann sind die folgenden Aussagen äquivalent.
(1) $M$ ist diagonalisierbar.
(2) Es gibt eine Basis von $K^n$ aus Eigenvektoren von $M$.
(3) Das charakteristische Polynom $\chi_M$ zerfällt in Linearfaktoren und für jeden Eigenwert $\lambda \in K$ von $M$ gilt $\mu_a(M, \lambda) = \mu_g(M, \lambda)$.

**Rezept (Diagonalisieren von Matrizen)** Sei $M \in M(n \times n, K)$ eine Matrix.
(1) Prüfe, ob Bedingung (3) aus dem Satz "Diagonalisierbarkeitskriterium" erfüllt ist.
(2) Bestimme Basen aller Eigenräume.
(3) Schreibe die Vektoren dieser Basis als Spalten in eine Matrix $T$. Dann ist $T^{-1}AT$ in Diagonalform.

## 4.3 Jordan-Normalform

**Definition (Einsetzungshomomorphismus und Minimalpolynom von Matrizen)** (1) Die Abbildung $\varphi_A : K[x] \to M(n\times n, K), f = \sum_{k=0}^{n} a_k x^k \mapsto \sum_{k=0}^{n} a_k A^k$ ist ein Homomorphismus von Ringen.
(2) Das eindeutig bestimmte Polynom minimalen Grades $\mu_A \in K[x]$ mit der Eigenschaft, dass $(\mu_A) = \ker \varphi_A$ heißt *Minimalpolynom von A*.

**Satz (Cayley-Hamilton)** Sei $n \in \mathbb{N}$, $K$ ein Körper und sei $A \in M(n \times n, K)$ mit charakteristischem Polynom $\chi_A$ und Minimalpolynom $\mu_A$. Dann gilt $\chi_A(A) = 0 = \mu_A(A)$ und $\mu_A | \chi_A$ in $K[x]$.

**Proposition (Eigenwerte und Minimalpolynom)** Unter den Bezeichnungen des Satzes von Cayley-Hamilton ist $\lambda \in K$ genau dann Eigenwert von $A$, wenn gilt $\mu_A(\lambda) = 0$.

**Proposition (Minimalpolynom und Diagonalisierbarkeit)** Sei $K$ ein Körper, $n \in \mathbb{N}$ und $M \in M(n \times n, K)$. Dann sind die folgenden Aussagen gleichwertig: (1) $A$ ist diagonalisierbar und (2) das Minimalpolynom $\mu_A$ von $A$ zerfällt in Linearfaktoren und hat nur einfache Nullstellen.

**Definition (Verallgemeinerter Eigenraum)** Sei $K$ ein Körper, $n \in \mathbb{N}$ und $M \in M(n \times n, K)$. Ist $\lambda \in K$ ein Eigenwert von $A$, so nennen wir $\mathrm{Eig}^i(A, \lambda) = \ker(A - \lambda E_n)^i$ den *verallgemeinerten Eigenraum i-ter Stufe* von $A$ zum Eigenwert $\lambda$.

**Definition (Jordan-Kästchen, Jordan-Normalform)** (1) Eine Matrix

$$J(\lambda, m) = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & & & & \vdots \\ \vdots & & & & \vdots \\ 0 & \cdots & \cdots & 0 & \lambda \end{pmatrix} \in M(m \times m, K). \tag{29}$$

heißt *Jordan-Kästchen der Länge m* zum Eigenwert $\lambda \in K$.
(2) Eine Matrix $A$ liegt in Jordan-Normalform vor, falls $A$ die Form $A = \mathrm{diag}(J(\lambda_1, m_1), ...., J(\lambda_r, m_r))$ besitzt.

**Satz (Hauptsatz der Jordan-Normalform)** Sei $A \in M(n \times n, K)$ eine Matrix deren charakteristisches Polynom in Linearfaktoren zerfällt. Dann ist $A$ ähnlich zu einer Matrix in Jordan-Normalform.

**Proposition (Hilfreiches zur Bestimmung der Jordan-Normalform)** Sei $A \in M(n \times n, K)$ eine Matrix, deren charakteristisches Polynom in Linearfaktoren zerfällt und $T \in \mathrm{GL}_n(K)$ eine Matrix, sodass $B = T^{-1}AT$ in Jordan-Normalform ist.
(1) Die Zahl der Jordan-Kästchen zum Eigenwert $\lambda$ in $B$ entspricht $\dim_K \mathrm{Eig}(A, \lambda)$.

(2) Die Größe des größten Jordan-Kästchens zum Eigenwert $\lambda$ in $B$ entspricht der Vielfachheit der Nullstelle $\lambda$ vom Minimalpolynom $\mu_A$ von $A$.
(3) Die Zahl der Jordan-Kästchen der Größe $m$ zum Eigenwert $\lambda$ in $B$ ist gegeben durch $2\dim_K \mathrm{Eig}^m(A,\lambda) - \dim_K \mathrm{Eig}^{m+1}(A,\lambda) - \dim_K \mathrm{Eig}^{m-1}(A,\lambda)$.

**Rezept (Bestimmung der Jordan-Normalform)** Sei $K$ ein Körper und $A \in M(n \times n, K)$ eine Matrix. Gesucht ist einen Basis $\mathcal{B}$, sodass $A$ bzgl. $\mathcal{B}$ Jordan-Normalform hat.
(1) Prüfe, ob das charakteristische Polynom von $A$ über $K$ in Linearfaktoren zerfällt. In diesem Fall ist es möglich, $A$ auf Jordan-Normalform zu bringen.
(2) Bestimme die Jordan-Normalform, also zu jedem $\lambda_1, ..., \lambda_m$ die Zahl $s(\lambda_i)$ der Jordan-Kästchen sowie deren Länge $k_j(\lambda_i)$ für $1 \leq j \leq s(\lambda_i)$ und $1 \leq i \leq m$.
(3) Frühstücke die Jordan-Kästchen der Reihe nach: Wähle für das erste Kästchen einen Vektor $v_{k_1(\lambda_1)} \in \mathrm{Eig}^{k_1(\lambda_1)}(\lambda_1) \setminus \mathrm{Eig}^{k_1(\lambda_1)-1}(\lambda_1)$.
(4) Arbeite rückwärts, indem man $v_{k_1(\lambda_1)-s} = (A-\lambda_1 E_n)v_{k_1(\lambda_1)-s+1}$ für $s \in \{1, ..., k_1(\lambda_1)-1\}$ setzt.
(5) Arbeite analog für die anderen Jordan-Kästchen zum Eigenwert $\lambda_1$: Wähle einen Vektor $v_{k_1(\lambda_1)+k_2(\lambda_1)} \in \mathrm{Eig}^{k_1(\lambda_1)} \setminus \langle \mathrm{Eig}^{k_1(\lambda_1)-1}(\lambda_1), M\rangle$, wobei $M$ die Menge der schon bestimmten Vektoren ist und setze $v_{k_1(\lambda_1)+k_2(\lambda_1)-s} = (A-\lambda_1 E_n)v_{k_1(\lambda_1)+k_2(\lambda_1)-s+1}$ für $s \in \{1, ..., k_2(\lambda_1)-1\}$ und verfahre analog für gegebenenfalls weitere Jordan-Kästchen.
(6) Gehe zum nächsten Eigenwert, indem die Schritte (3) bis (5) für den neuen Eigenwert durchgeführt werden.
(7) Schreibe die Vektoren $v_1, ..., v_n$ als Spalten in die Transformationsmatrix $T$. Die Matrix $T^{-1}AT$ hat dann Jordan-Normalform.

# 5 Kurs im Wintersemester 18/19

**Aufgabe 1** Sei $G$ Gruppe, $N \trianglelefteq G$ und $U \leq G$. Definiere $UN \equiv \{un \in G | u \in U, n \in N\}$. Da $N \trianglelefteq G$, gilt $UN \leq G$. Zu zeigen ist $U/(U \cap N) \simeq UN/N$. Offenbar ist $N \trianglelefteq UN$. Denn sei $h \in UN$ beliebig. Dann gibt es $u \in U, n \in N$ so dass $h = un$. Sei nun $m \in N$ beliebig. Es gilt $hmh^{-1} = (un)m(un)^{-1} = unmn^{-1}u^{-1}$. Da $N$ Gruppe, ist $n' \equiv nmn^{-1} \in N$ und da $N \trianglelefteq G$, gibt es ferner $n'' \in N$ so dass $n'g = gn''$ für festes $g \in G$, insbesondere also für $g = u^{-1} \in G$. Damit folgt $un'u^{-1} = uu^{-1}n'' = e_g n'' = n'' \in N$. Beliebigkeit von $m \in N$ liefert$hNh^{-1} \subseteq N$ und da $h \in UN$ beliebig war, folgt $hNh^{-1} \subseteq N$ für alle $h \in UN$. Laut Vorlesung ist dies äquivalent zu $N \triangleleft UN$. Mithin erlaubt der kanonische Epimorphismus $\pi : UN \to UN/N, h \mapsto hN$ das Rechnen in der Faktorgruppe $UN/N$. Definiere nun $\Phi : U \to UN/N, u \mapsto [u]$, wobei $[u]$ die Linksnebenklasse $uN \in UN/N$ bezeichnet. Hierbei wurde $U \subseteq UN$ verwendet, denn wegen $N \trianglelefteq G$ gilt $e_G \in N$ und somit $u = u \cdot e_G \in UN$. Als Abbildung ist $\Phi$ somit wohldefiniert. Um den Homomorphiesatz anzuwenden, ist nachzuweisen, dass $\Phi$ Gruppenhomomorphismus (1) ist, der surjektiv (2) ist und $\ker \Phi = U \cap N$ hat. Für (1) sei $u_1, u_2 \in U$ beliebig aber fest. Dann gilt $\Phi(u_1 \cdot u_2) = \Phi(u_1 u_2) = (u_1 u_2)N = (u_1 N) \cdot (u_2 N) = \Phi(u_1)\Phi(u_2)$ nach den Rechenregeln in der Faktorgruppe $UN/N$. Damit ist die Gruppenhomomorphismuseigenschaft von $\Phi$ nachgewiesen. Zum Beweis der Surjektivität (2) sei $R$ Repräsentantensystem von

$UN/N$ und $r \in R$ beliebig. Wegen $R$ Repräsentantensystem, gibt es ein eindeutiges $h = un \in UN$ mit, nicht notwendigerweise eindeutigen $u \in U, n \in N$, so dass $r \in hN = unN = uN$. Hierbei wurde $nN = e_G N$ für $n \in N$ verwendet. Wähle also ein auf diese Weise erhaltenes $u$. Dann gilt $\Phi(u) = [u] = uN$. Wegen $r \in uN$ folgt aus der Repräsentantensystemeigenschaft von $R \ni r$, dass $uN \ni r$. Da $r \in R$ beliebig war, folgt die Surjektivität von $\Phi$. $\Phi$ ist also Epimorphismus. Zu zeigen bleibt $\ker \Phi = U \cap N$, (3). Für $u \in U$ gilt die Äquivalenz $u \in \ker \Phi \Leftrightarrow [u] = [e_G] \Leftrightarrow uN = N \Leftrightarrow \forall n \in N : un \in N \Leftrightarrow \forall n \in N \exists m \in N : un = m \Leftrightarrow \forall n \in N \exists m \in N : u = mn^{-1} \Leftrightarrow u \in N$, weil $N$ als Gruppe abgeschlossen ist. $u \in U$ laut Voraussetzung und nun zusätzlich $u \in N$ ist äquivalent zu $u \in U \cap N$. Damit ist die Gleichheit von Mengen, $\ker \Phi = U \cap N$ nachgewiesen. Laut Homomorphiesatz ist der induzierte Homomorphismus $\bar{\Phi} : U/\ker \Phi = U/(U \cap N) \to UN/N$ Gruppenisomorphismus, d.h., $U/(U \cap N) \simeq UN/N$ wie behauptet. □

**Aufgabe 2** Sei $q = p^r$ mit $p \in \mathbb{P}$ und $r \in \mathbb{N}$. Für beliebiges $n \in \mathbb{N}$, gilt

$$\mathrm{ord}(SL_n(\mathbb{F}_q)) = \frac{\prod_{k=0}^{n-1}(p^{nr} - p^{rk})}{p^r - 1}. \tag{30}$$

Wir zeigen mittels vollständiger Induktion zunächst $\mathrm{ord}(G_n) \equiv \mathrm{ord}(\mathrm{GL}_n(\mathbb{F}_q)) = \prod_{k=0}^{n-1}(p^{nr} - p^{rk})$ für alle $n \in \mathbb{N}$. Für $n = 1$ ist $A = (a) \in G_1 \Leftrightarrow \det(a) \neq 0 \Leftrightarrow a \neq 0 \Leftrightarrow a \in \mathbb{F}_q^\times$ für $a \in \mathbb{F}_q$ einziger Eintrag in der $1 \times 1$-Matrix. Da $\mathbb{F}_q$ endlicher Körper gilt die Äquivalenz $a \neq 0 \Leftrightarrow a \in \mathbb{F}_q^\times$ von oben. Direkt aus den Körperaxiomen folgt aber auch $|\mathbb{F}_q^\times| = q - 1 = p^r - 1 = \prod_{k=0}^{1-1}(p^{nr} - p^{rk})$. Sei nun die Gültigkeit $\mathrm{ord}(G_n) = \prod_{k=0}^{n-1}(p^{nr} - p^{rk})$ vorausegesetzt für festes $n \in \mathbb{N}$. Wir zeigen, dass daraus auch $\mathrm{ord}(G_{n+1}) = \prod_{k=0}^{n}(p^{(n+1)r} - p^{rk})$ folgt. Ein beliebiges $A \in \mathrm{GL}_{n+1}(\mathbb{F}_q)$ hat $n+1$ linear unabhängige Spaltenvektoren aus dem $\mathbb{F}_q$-Vektorraum $\mathbb{F}_q^{n+1}$. Wir schreiben $A = (v_1, ..., v_{n+1})$ und setzen $v_1, ..., v_{n+1} \in \mathbb{F}_q^{n+1}$ als linear unabhängig an. Für $v_1$ gilt $v_1 \neq 0_{\mathbb{F}_q^{n+1}}$, also gibt es $q^{n+1} - 1$ Möglichkeiten, einen Nicht-Null-Vektor $v_1$ zu wählen. Damit die $\{v_i\}_{1 \leq i \leq n+1}$ linear unabhängig sind, muss gelten $[v_2], ..., [v_{n+1}] \in \mathbb{F}_q^{n+1}/\mathrm{lin}_{\mathbb{F}_q}(v_1) \simeq \mathbb{F}_q^n$ linear unabhängig, wobei $v \sim w \Leftrightarrow v - w \in \mathrm{lin}_{\mathbb{F}_q}(v_1)$. Damit wenden wir die Induktionsvoraussetzung auf $[A] \equiv ([v_2], ..., [v_{n+1}])$ an, denn die oben genannte Isomorphie von $\mathbb{F}_q$–Vektorräumen generalisiert spaltenweise auf $GL_n(\mathbb{F}_q^{n+1}/\mathrm{lin}_{\mathbb{F}_q}(v_1)) \simeq GL_n(\mathbb{F}_q^n)$. Zu $[A]$ korrespondiert also in bijektiver Weise ein $B = (w_2, ..., w_n) \in \mathrm{GL}_n(\mathbb{F}_q)$. Infolge der Äquivalenzklassenbildung ist jedes $[v_2], ..., [v_{n+1}]$ nur bis auf Addition von $x \cdot v_1$ mit $x \in \mathbb{F}_q$ bestimmt. Die $\mathrm{ord}(GL_n(\mathbb{F}_q))$ Möglichkeiten, die $[v_2], ..., [v_n]$ zu erhalten sind also noch mit $q^n$ zu multiplizieren, um die Anzahl möglicher $v_2, ..., v_{n+1} \in \mathbb{F}_q^{n+1} \setminus \mathrm{lin}_{\mathbb{F}_q}(v_1)$, die linear unabhängig sind, zu erhalten. Die Anzahl entsprechender Möglichkeiten ist also $q^n \prod_{k=0}^{n-1}(q^n - q^k) = \prod_{k=1}^{n}(q^{n+1} - q^k)$ nach Redefinition des Produktindex. Da bereits $q^{n+1} - 1$Möglichkeiten existieren, $v_1$ den oben genannten Anforderungen an die Matrix $A$ entsprechend zu wählen, gibt es also insgesamt $q^{n+1} - 1 \cdot \prod_{k=1}^{n}(q^{n+1} - q^k)$ das $(n+1)$–Tupel von linear unabhängigen Vektoren $v_1, ..., v_{n+1} \in \mathbb{F}_q^{n+1}$ zu wählen. Einsetzen von $q = p^r$ und Beliebigkeit des gewählten $A \in \mathrm{GL}_n(\mathbb{F}_q)$ liefert nun $\mathrm{ord}(G_{n+1}) = \prod_{k=0}^{n}(p^{(n+1)r} - p^{rk})$. Nach dem Induktionsprinzip ist die Behauptung damit für alle $n \in \mathbb{N}$ bewiesen. Sei nun $n \in \mathbb{N}$ beliebig aber fest. Nach Definition

ist $A \in \mathrm{SL}_n(\mathbb{F}_q)$ genau dann wenn $A \in \mathrm{GL}_n(\mathbb{F}_q)$ und $\det A = 1$. Bekannt ist aus der linearen Algebra, dass $\det : \mathrm{GL}_n(\mathbb{F}_q) \to \mathbb{F}_q^\times, A \mapsto \mathbb{F}_q^\times$ Gruppenhomomorphismus definiert. Für beliebiges $a \in \mathbb{F}_q^\times$ ist die diagonale Matrix $A = \mathrm{diag}(a, 1, ..., 1)$ mit $(n-1)$ Einträgen 1 auf der Diagonalen in $\mathrm{GL}_n(\mathbb{F}_q)$ und es gilt $\det A = a$. Dies zeigt Surjektivität von det. Für beliebiges $A \in \mathrm{GL}_n(\mathbb{F}_q)$ gilt die Äquivalenz $A \in \ker\det \Leftrightarrow \det A = 1 \Leftrightarrow A \in \mathrm{SL}_n(\mathbb{F}_q)$. Beliebigkeit von $A \in \mathrm{GL}_n(\mathbb{F}_q)$ liefert die Gleichheit von Mengen: $\ker\det = \mathrm{SL}_n(\mathbb{F}_q)$. Laut Homomorphiesatz ist der induzierte Homomorphismus von Gruppen, $\bar{\det} : \mathrm{GL}_n(\mathbb{F}_q)/\mathrm{SL}_n(\mathbb{F}_q) \to \mathbb{F}_q^\times$ also ein Isomorphismus von Gruppen. Da isomorphe Gruppen die gleiche Ordnung haben und sowohl $\mathrm{ord}(\mathbb{F}_q^\times) = q - 1$ als auch $\mathrm{ord}(\mathrm{GL}_n(\mathbb{F}_q)) = \prod_{k=0}^{n-1}(q^n - q^k)$ endlich sind, liefert der Satz von Lagrange: $\mathrm{ord}(\mathrm{GL}_n(\mathbb{F}_q)/\mathrm{SL}_n(\mathbb{F}_q)) = \mathrm{ord}(\mathrm{GL}_n(\mathbb{F}_q))/\mathrm{ord}(\mathrm{SL}_n(\mathbb{F}_q))$ und der Isomorphismus $\bar{\det}$ aus dem Homomorphiesatz-Argument von oben die Gleichheit des letztgenannten Quotienten zu$\mathrm{ord}(\mathbb{F}_q^\times)$. Umformen und Einsetzen der entsprechenden bereits vorher hergeleiteten Gruppenordnungen liefert

$$\mathrm{ord}(\mathrm{SL}_n(\mathbb{F}_q)) = \frac{\mathrm{ord}(\mathrm{GL}_n(\mathbb{F}_q))}{\mathrm{ord}(\mathbb{F}_q^\times)} = \frac{\prod_{k=0}^{n-1}(p^{nr} - p^{rk})}{p^r - 1}, \tag{31}$$

was zu beweisen war. □

**Aufgabe 3** Sei $G$ Gruppe, $H \leq G$ und $g \in G$ beliebig. Es ist $\Phi_g : G \to G, h \mapsto ghg^{-1}$ in $\mathrm{Aut}(G)$, insbesondere also Gruppenhomomorphismus. Damit ist $\Phi_g(H) = gHg^{-1} = \{ghg^{-1} | h \in H\}$ insbesondere Untergruppe von $G$ und $H \simeq gHg^{-1}$. Sei nun $R \subseteq G$ Repräsentantensystem von $G/H$. Zu zeigen ist $\Phi_g(R) = gRg^{-1}$ ist Repräsentantensystem von $G/\Phi_g(H)$. Sei also $r \in R$ beliebig. Zu zeigen ist, dass es zu beliebiger Linksnebenklasse $g'gHg^{-1} \in G/\Phi_g(H)$ genau ein $r' \in R'$ gibt, so dass $r' \in g''gHg^{-1}$. Da $\Phi_g$ Automorphismus ist, es also genau ein $g' \in G$ mit $\Phi_g(g') = g''$ gibt, und $r'$ von der Form $grg^{-1}$ für ein eindeutiges $r \in R$ ist, gilt die Äquivalenz $r' \in g''gHg \Leftrightarrow grg^{-1} \in gg'g^{-1}gHg \Leftrightarrow grg^{-1} \in gg'Hg^{-1} \leftrightarrow \exists h \in H : grg^{-1} = gg'hg^{-1} \leftrightarrow \exists h \in Hr = g'h \Leftrightarrow r \in g'H$. Da $R$ Repräsentantensystem von $G/H$ folgt die Existenz eines geeigneten $r' \in R'$. Die Eindeutgkeit des $r'$ ergibt sich ebenfalls aus der Äquivalenz und der eindeutigen Existenz eines $r \in R$ zu vorgegebener Linksnebenklasse $g'H$ mit beliebigen $g' \in G$. □

**Aufgabe 4 - F13T2A1** Sei $x \in \mathbb{Q}$ und sei $[x] = x + \mathbb{Z}$. Zu zeigen ist, dass ein beliebiges $[x] \in \mathbb{Q}/\mathbb{Z}$ endliche Ordnung besitzt. Ein $[x] \in \mathbb{Q}/\mathbb{Z}$ ist von der Form $[x] = m/n + \mathbb{Z}$ für ein $n \in \mathbb{N}$ und nicht–negatives $m$ mit $0 \leq m < n$. Wegen $n \cdot [x] = [x] + ... + [x] = m + \mathbb{Z} = 0 + \mathbb{Z}$, also $n[x] = 0$ in $\mathbb{Q}/\mathbb{Z}$ folgt $\mathrm{ord}([x])|n$. Da $n$ endlich, ist inbesondere $\mathrm{ord}([x]) \leq n$ endlich. Jedes $[x] \in \mathbb{Q}/\mathbb{Z}$ hat also endliche Ordnung. Sei nun die Faktorgruppe $\mathbb{R}/\mathbb{Z}$ unter Betrachtung und dazu $x \in \mathbb{R}$ und $[x] = x + \mathbb{R}$. Sei $[x] \in \mathbb{R}/\mathbb{Z}$ ein Element endlicher Ordnung. Dann gilt $\mathrm{ord}([x]) \cdot [x] \in [0] + \mathbb{Z}$. Es gibt also ein $k \in \mathbb{Z}$ so dass $\mathrm{ord}([x]) \cdot x = k$. Da $\mathrm{ord}(x) \in \mathbb{N}$ insbesondere von 0 verschieden ist, folgt $x = k/\mathrm{ord}(x)$. Damit folgt, dass jedes Element $[x]$ mit endlicher Ordnung aus $\mathbb{R}/\mathbb{Z}$ aus $x \in \mathbb{Q}$ ensteht. Damit sind die Elemente endlicher Ordnung in $\mathbb{R}/\mathbb{Z}$ gerade $[x] \in \mathbb{Q}/\mathbb{Z}$. Sei nun zu $x \in \mathbb{R}$ $[[x]] \in \mathbb{R}/\mathbb{Q}$ gegeben durch $[[x]] = x + \mathbb{Q}$. Offenbar hat $[[0]]$ als Neutralelement der Faktorgruppe die endliche Ordnung 1. Sei also $[[x]] \neq [[0]]$. Dann ist $\mathrm{ord}([[x]]) = \infty$. Denn, angenommen, die Ordnung von

$[[x]]$ wäre endlich, dann gilt $\text{ord}([[x]])[[x]] = [[0]] \Leftrightarrow \exists q \in \mathbb{Q} : \text{ord}([[x]])x = q$ und wegen $\text{ord}([[x]]) \in \mathbb{N}$ also auch $x \in \mathbb{Q}$. Dann ist aber $[[x]] = x + \mathbb{Q} = 0 + \mathbb{Q} = [[0]]$ im Widerspruch zu $[[x]] \neq [[0]]$. Damit hat also nur das Neutralelement $[[0]]$ der Faktorgruppe $\mathbb{R}/\mathbb{Q}$ endliche Ordnung. □

**Aufgabe 5 - H17T3A2** (a) Sei $G$ endliche ablesche Gruppe und $\exp(G) \equiv \min\{n \in \mathbb{N} | na = 0 \forall a \in G\}$. Da $G$ endlich in (a) ist, existiert das Minimum in der Definition des Exponenten von $G$ stets: Für alle $a \in G$ gilt nämlich laut Vorlesung $\text{ord}(a) \leq \text{ord}(G) < \infty$ nach Voraussetzung der Endlichkeit von $G$. Zu zeigen ist, dass $\exp(G) = \max\{\text{ord}(a) | a \in \mathbb{G}\} =: M$. Wir zeigen zuerst $\exp(G) \geq M$. Angenommen, $\exp(G) < M$. Dann gibt es ein $a \in G$ so dass $M = \text{ord}(a) > \exp(G)$. Nach Definition von $\exp(G)$ gilt aber für alle $g \in G$, also insbesondere für $g = a$, $\exp G \cdot a = 0$. Nach Definition ist aber $\text{ord}(a)$ die kleinste natürliche Zahl $m$, die $ma = 0$ erfüllt. Da $\exp G < M = \text{ord}(a)$ kann es also ein Element $a \in G$ mit der geforderten Eigenschaft nicht geben. Daher ist die Annahme falsch gewesen und es gilt $\exp G \geq M$. Wir zeigen nun $M \geq \exp G$. Da $G$ endlich ist, ist $G$ insbesondere durch die Menge seiner Elemente endlich erzeugt. Da ferner $G$ abeslch ist, können wir den Hauptsatz über endlich erzeugte ablesche Gruppen auf $G$ anwenden: Sei dazu $N = \text{ord}(G)$. Ferner sei $I \subseteq \mathbb{N}$ eine endliche Indexmenge und $\{d_i | i \in I\}$ eine Menge natürlicher Zahlen größer 1, so dass $d_1 | G$ und $d_{i+1} | G/d_i$ für alle $i \in I$ und $N = d_1 \cdot ... d_{|I|}$. Der Hauptsatz über endlich erzeugte abelsche Gruppen liefert nun die Existenz eines $I$ wie beschrieben und eines $\{d_i\}_{1 \leq i \leq |I|}$ ebenfalls wie beschrieben, so dass $G \simeq \mathbb{Z}/(d_1\mathbb{Z}) \times ... \times \mathbb{Z}/(d_{|I|})\mathbb{Z} =: H$. Insbesondere hat ein $g \in G$ dieselbe Ordnung wie sein Bild unter dem nach dem Hauptsatz über endlich erzeugte abelsche Gruppen existierenden Isomorphismus $\phi : G \to H$, so dass wir $G = \mathbb{Z}/(d_1\mathbb{Z}) \times ... \times \mathbb{Z}/(d_{|I|}\mathbb{Z})$ für ein $I$ und $\{d_i\}_{1 \leq i \leq |I|}$ annehmen können. Für $n = \text{kgV}(d_1, ..., d_{|I|})$ gilt nun $ng = n(a_1, ..., a_{|I|}) = (na_1, ..., na_{|I|}) = (0, ..., 0)$ für $G \ni g = (a_1, ..., a_{|I|})$ mit $a_i \in \mathbb{Z}/(d_i\mathbb{Z})$ für alle $i \in I$. Also $n \geq \exp(G)$. Andererseits ist durch $g_0 = (b_1, ..., b_{|I|})$ mit $b_i = 1$ für alle $i \in I$ gerade ein Element der Ordnung $n$ in $G$ gegeben. Andernfalls gäbe es ein $d_j$, dass $\text{ord}(g_0)$ nicht teilte, im Widerspruch zu $\text{ord}(g_0)g_0 = e_G = (0, ..., 0)$. Also gilt $\text{ord}(g_0) = n$ und $n \geq \exp(G)$. Nach Definition von $M$, $M \geq n \geq \exp(G)$, also $\exp(G) \leq M$. Zusammen mit $\exp G \geq M$ folgt $\exp G = M$, wie behauptet. □

(b) Wir weisen zuerst nach, dass (laut Voraussetzung: die abelsche Gruppe) $G = \mathbb{Q}/\mathbb{Z}$ Torsionsgruppe ist. Sei dazu $x \in \mathbb{Q}/\mathbb{Z}$ beliebig. Dann gibt es $m \in \mathbb{Z}$ und $n \in \mathbb{N}$, so dass $x = m/n + \mathbb{Z}$. Offenbar gilt $nx = m + \mathbb{Z} = 0 + \mathbb{Z}$. Damit ist $\text{ord}(x) | n$ und insbesondere endlich. Wir zeigen nun, dass $\exp G = \infty$. Angenommen, $\exp G < \infty$. Dann gibt es ein $n \in \mathbb{N}$, so dass $\exp(G) = n$. Sei nun $p \in \mathbb{P}$ die kleinste Primzahl, die echt größer als $n$ ist. Es gilt $n$ teilt $p$ nicht, da $p$ prim, und $p$ teilt $n$ nicht, da $p$ echt größer als $n$. Andererseits gilt offenbar $1/p \notin \mathbb{Z}$ und $1/ı \in \mathbb{Q}$. Wir behaupten $p = \text{ord}([1/p])$: Denn $\text{ord}([1/p])[1/p] = [0] \Leftrightarrow \text{ord}([1/p])1/p \in \mathbb{Z}$. Da $1/p > 0$ und $\text{ord}([1/p])$ wegen der Torsionsgruppeneigenschaft endlich und nach Definition der Ordnung natürlich, also positiv ist, erhalten wir $\text{ord}([1/p])1/p = 1$. Damit gilt $\text{ord}([1/p]) = p > n = \exp G$ nach Wahl von $p$. Damit haben wir den Widerspruch zur Annahme, es gäbe ein endliches $\exp(G)$. □

**Aufgabe 6** Zu zeigen ist, dass die Gruppen $G = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ und $H = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ jeweils versehen mit der komponentenweisen Multiplikation nicht zueinander isomorph sind. Wir nehmen an, $G \simeq H$. Dann gibt es einen Isomorphismus von Gruppen, $\psi : G \to H, g \mapsto \psi(g)$. Für ein Element $g \in G$ gilt, dass $\psi(g) \in G$ dieselbe Ordnung wie $g$ hat. Denn wäre $\mathrm{ord}(g) < \mathrm{ord}(\psi(g))$, so folgte $e_H = \psi(e_G) = \psi(g^{\mathrm{ord}(g)}) = \psi(g)^{\mathrm{ord}(g)} \neq e_H$, da $\mathrm{ord}(\psi(g))$ die kleinste natürliche Zahl mit der Eigenschaft $\psi(g)^{\mathrm{ord}(\psi(g))} = e_H$ ist. Im anderen Falle gilt $\mathrm{ord}(g) > \mathrm{ord}(\psi(g))$. Da Ordnungen von Gruppenelementen natürliche Zahlen sind, und das Neutralelement das eindeutige Element mit Ordnung 1 in der jeweiligen Gruppe ist, folgt $\psi(k(\neq e_G)) \equiv \psi(g^{\mathrm{ord}(\psi(g))}) = (\psi(g))^{\mathrm{ord}(\psi(g))} = e_H$. Da bereits infolge der Homomorphismeneigenschaft $\psi(e_G) = e_H$ gilt und die obenstehende Rechnung auch $\psi(k) = e_H$ für das $k \neq e_G$ liefert, folgt $\ker(\psi) \supseteq \{e_G, k\}$. Dies widerspricht aber der Tatsache, dass $\psi$ Isomorphismus von Gruppen, also insbesondere Gruppenmonomorphismus ist: Letzteres ist vorlesungsgemäß äquivalent zu $\ker(\psi) = \{e_G\}$ im Widerspruch zum oben erhaltenen Ergebnis. Damit ist gezeigt, dass Elemente der Ordnung $k$ aus $G$ auf Elemente der Ordnung $k$ in $H$ vermöge des Isomorphismus $\psi$ abgebildet werden. Da $\psi$ bijektiv ist, folgt ferner, dass zwei verschiedene Elemente $g, g' \in G$ auf zwei verschiedene Elemente $h, h' \in H$ abgebildet werden, wobei $\mathrm{ord}(g) = \mathrm{ord}(h)$ und $\mathrm{ord}(g') = \mathrm{ord}(h')$ gilt. Letzteres Ergebnis impliziert nun, dass die Anzahl der Elemente einer fest vorgegebenen Ordnung in $G$ mit der Anzahl der Elemente derselben Ordnung in $H$ übereinstimmen. Wir zählen für die Spezifikationen von $G$ und $H$ von oben die Elemente in $G$ und $H$ die jeweils die Ordnung 2 haben. In $G$ gibt es in jedem der beiden Faktoren ein Element der Ordnung 1, eines der Ordnung 2 und zwei der Ordnung 4. Im dritten Faktor in der äußeren Prdouktdarstellung von $G$ gibt es ein Element der Ordnung 1 und ein Element der Ordnung 2. Ein Element aus $G$ hat die Form $g = (g_1, g_2, g_3)$, wobei $g_1, g_2 \in \mathbb{Z}/(4\mathbb{Z})$ und $g_3 \in \mathbb{Z}/(2\mathbb{Z})$. Aus der Vorlesung ist bekannt, dass in diesem Fall dann $\mathrm{ord}(g) = \mathrm{kgV}(\mathrm{ord}(g_1), \mathrm{ord}(g_2), \mathrm{ord}(g_3))$. Damit finden wir, dass nur $(\mathrm{ord}(g_1), \mathrm{ord}(g_2), \mathrm{ord}(g_3)) \in \{(1,1,2), (2,1,1), (1,2,1), (2,2,1), (2,1,2), (1,2,2), (2,2,2)\}$ zulässig sind. Insgesamt liefert das $1{\cdot}1{\cdot}1{+}1{\cdot}1{\cdot}1{+}1{\cdot}1{\cdot}1{+}1{\cdot}1{\cdot}1{+}1{\cdot}1{\cdot}1{+}1{\cdot}1{\cdot}1{+}1{\cdot}1{\cdot}1 = 7$ Kombinationen, um ein Element der Ordnung 2 in $G$ zu produzieren. Analog finden wir für die Anzahl der Elemente von Ordnung 2 in $H$, dass es $2^4 - 1 = 15$ solche Elemente gibt: Hierbei haben wir die Anzahl der Kombinationen von Elementen der einzelnen Faktoren zu Elementen der Ordnung $\leq 2$ berechnet ($\to 2^4$) und dann die Anzahl der Elemente der Elemente subtrahiert, deren Ordnung $< 2$ ist. Da nur das Neutralelement in $H$ Ordnung 1 hat, reproduzieren wir die obige Rechnung. Da $7 \neq 15$, folgt der Widerspruch zur Annahme, $\psi : G \to H$ wäre Isomorphismus von Gruppen. Mithin sind $G$ und $H$ nicht isomorph. $\square$

**Aufgabe 7** Gesucht sind bis auf Isomorphietyp alle abelschen Gruppen der Ordnung 500. Es handelt sich also um endliche, insbesondere endlich erzeugte, abelsche Gruppen, die gesucht sind. Nach dem Hauptsatz über endlich erzeugte abelsche Gruppen in der Formulierung für endliche abelsche Gruppen, gibt es also ein $r \in \mathbb{N}$, so dass $G \simeq C_1 \times .... \times C_r$, wobei die Faktoren $C_i$ alle endlich und zyklisch von Primzahlpotenzordnung gewählt werden können (Konsequenz des chinesischen Restklassensatz). Wir bilden also die Primfakorzerlegung von 500: Es gilt $500 = 5^3 \cdot 2^2$. Da

die Ordnung jedes Faktors insbesondere die Ordnung von $G$ teilen muss, finden wir die $3 \cdot 2 = 6$ Optionen

$$G \simeq \mathbb{Z}/(5^3\mathbb{Z}) \times \mathbb{Z}/(2^2\mathbb{Z}) \equiv G_1 \tag{32}$$
$$G \simeq \mathbb{Z}/(5^3\mathbb{Z}) \times (\mathbb{Z}/(2\mathbb{Z}) \times \mathbb{Z}/(2\mathbb{Z})) \equiv G_2 \tag{33}$$
$$G \simeq \mathbb{Z}/(5\mathbb{Z}) \times \mathbb{Z}/(5^2\mathbb{Z}) \times \mathbb{Z}/(2^2\mathbb{Z}) \equiv G_3 \tag{34}$$
$$G \simeq \mathbb{Z}/(5\mathbb{Z}) \times \mathbb{Z}/(5^2\mathbb{Z}) \times (\mathbb{Z}/(2\mathbb{Z}) \times \mathbb{Z}/(2\mathbb{Z})) \equiv G_4 \tag{35}$$
$$G \simeq \mathbb{Z}/(5\mathbb{Z}) \times \mathbb{Z}/(5\mathbb{Z}) \times \mathbb{Z}/(5\mathbb{Z}) \times \mathbb{Z}/(2^2\mathbb{Z}) \equiv G_5 \tag{36}$$
$$G \simeq \mathbb{Z}/(5\mathbb{Z}) \times \mathbb{Z}/(5\mathbb{Z}) \times \mathbb{Z}/(5\mathbb{Z}) \times \mathbb{Z}/(2\mathbb{Z}) \times \mathbb{Z}/(2\mathbb{Z}) \equiv G_6. \tag{37}$$

Zu zeigen verbleibt, dass $G_i \not\simeq G_j$ für $i \neq j$ und $i, j \in \{1, ..., 6\}$ gilt, d.h., dass wir genau sechs verschiedene Isomorphietypen für das $G$ laut Voraussetzung haben. Letzteres folgt aber bereits aus der Tatsache, dass die Gruppen $G' = (\mathbb{Z}/(p\mathbb{Z}))^k$ und $G'' = \mathbb{Z}/(p^k\mathbb{Z})$, für $k \geq 2$ natürlich und $p$ prim, nicht isomorph sind: Wären $G'$ und $G''$ isomorph, so hätten sie insbesondere dieselbe Anzahl an Elementen der Ordnung $p$. In $G'$ gibt es genau $p^k - 1$ Elemente der Ordnung $p$, da jeder Faktor zyklische Gruppe der Ordnung $p \in \mathbb{P}$ ist, und nur das Neutralelement in jedem Faktor Ordnung 1 hat. In $G''$ gibt es hingegen genau $\Phi(p^k) = p^k - p^{k-1}$ Elemente der Ordnung $p^k$, wobei $\Phi$ die Euler'sche $\Phi$-Funktion bezeichnet. Da $G''$-Ordnung $p^k$ hat, folgt für die Anzahl der Elemente, die lediglich Ordnung ungleich $p^k$ und ungleich 1 (Neutralelement) haben, $p^k - (p^k - p^{k-1}) - 1 = p^{k-1} - 1$. Für alle $p \in \mathbb{P}$ und $k \geq 2$ natürlich ist das echt kleiner als die Anzahl $p^k - 1$ der Elemente der Ordnung $p$ in $G'$. Da ferner die Anzahl der Elemente der Ordnung $p$ in $G''$ kleiner oder gleich $p^{k-1} - 1$ ist, folgt der Widerspruch zur Annahme $G' \simeq G''$. Da die Gruppen $G_i$ für $1 \leq i \leq 6$ jeweils zyklische Faktoren von Primzahlpotenzordnung haben, ergibt sich die Behauptung, dass verschiedene $G_i$'s aus der obenstehenden Auflistung nicht isomorph sind. Da der Hauptsatz für endlich erzeugte abelsche Gruppen diese abschließend klassifiziert, gibt es also genau 6 Isomorphietypen für abelsche Gruppen der endlichen Ordnung 500,nämlich gerade die oben Angegebenen. □

**Aufgabe 8** Gesucht sind alle natürlichen $m$, so dass es in der alternierenden Gruppe $A_8$ ein Element der Ordnung $m$ gibt. Da $A_8 \trianglelefteq S_8$, können wir jedes $\sigma \in A_8$ in disjunkte Zykel zerlegen. $A_8$ besteht gerade aus denjenigen Elementen von $S_8$, die gerades Signum besitzen. Wir behandeln das Problem in $S_8$ und schließen hinterher diejenigen Elemente aus, die in der disjunkten Zykel-Zerlegung eine gerade Anzahl von Zykel-Faktoren gerader Länge haben. In $S_8$ gibt es Zykel der Länge $k$ mit $2 \leq k \leq 8$. Sei $\sigma = \rho_1 \odot ... \odot \rho_r$ für $r \in \mathbb{N}_0$ eine Zerlegung von $\sigma$ in disjunkte Zykel. Nach Definition von $A_8$ gilt $+1 = \mathrm{sgn}(\sigma) = \prod_{l=1}^{r} \mathrm{sgn}(\rho_l) = \prod_{l=1}^{r} (-1)^{|\rho_l|-1}$, wobei $|\rho|$ die Länge eines Zykels $\rho \in S_8$ anzeigt. In der Rechnung wurde die Homomorphismus-Eigenschaft des Signums benutzt und, dass ein Zykel $\rho$ Signum $(-1)^{|\rho|-1}$ besitzt. In der disjunkten Zykel-Zerlegung gilt ferner für die Ordnung eines Elements in $S_8$ (und damit auch die Ordnung in $A_8$):

$$\mathrm{ord}(\sigma) = \mathrm{kgV}(\mathrm{ord}(\rho_1), ..., \mathrm{ord}(\rho_r)) \tag{38}$$

wenn $\sigma$ in $r$ disjunkte Zykel zerlegt werden kann. Da für Zykel die Ordnung gerade die Länge des Zykels ist, müssen wir zusätzlich nur noch die Signumsbedingung erfüllen: Das ist gerade die Bedingung

$$\sum_{l=1}^{r} \mathrm{ord}(\rho_l) - r \in 2\mathbb{N}_0. \tag{39}$$

Ferner gilt wegen Disjuktheit der Zykel die Bedingung $2 \leq \sum_{l=1}^{r} \mathrm{ord}(\rho_l) \leq 8$ für die Gesamt-Länge der Träger, wobei wir die Identität $\mathrm{id} \in A_8$ als Element der Ordnung 1 bereits im Vorfeld angeben.

- *Fall $r = 1$:* Dann ist $\mathrm{ord}(\rho_1) \in \{1, 3, 5, 7\}$ und wegen $\sigma = \rho_1$ gibt es also Elemente der Ordnung $3, 5, 7$ in $A_8$, da $\mathrm{ord}(\rho_1) = 1$ nur formal zur Identität korrespondiert und echte Zykel die Länge $\geq 2$ haben.

- *Fall $r = 2$:* Dann ist $\mathrm{ord}(\rho_1) + \mathrm{ord}(\rho_2) \in \{2, 4, 6, 8\}$. Der Fall, dass die Gesamtlänge des Zykels 2 ist, scheidet wegen $r = 2$ aus. Damit finden wir Elemente der Ordnung 2, der Ordnung 3 ($3+3 = 6$), der Ordnung 4, der Ordnung 6, und der Ordnung 15, indem wir alle mögliche Wahlen für natürliche Zahlen $2 \leq \mathrm{ord}(\rho_1) \leq \mathrm{ord}(\rho_2)$ durchspielen, so dass $\mathrm{ord}(\rho_1) + \mathrm{ord}(\rho_2) \in \{4, 6, 8\}$ und von den so erhaltenen Ordnungen dann das $\mathrm{kgV}(\mathrm{ord}(\rho_1), \mathrm{ord}(\rho_2))$ bilden.

- *Fall $r = 3$:* Dann ist $\mathrm{ord}(\rho_1) + \mathrm{ord}(\rho_2) + \mathrm{ord}(\rho_3) \in \{3, 5, 7\}$. Da $r = 3$, ist $\mathrm{ord}(\rho_i)$ für $1 \leq i \leq 3$ jeweils größeroder gleich 2. Also bleibt nur die Möglichkeit $\mathrm{ord}(\rho_1) + \mathrm{ord}(\rho_2) + \mathrm{ord}(\rho_3) = 7$ zu überprüfen. Hier können wir nur (bis auf Reihenfolge) $(\mathrm{ord}(\rho_1), \mathrm{ord}(\rho_2), \mathrm{ord}(\rho_3)) = (2, 2, 3)$ haben. Da $\mathrm{kgV}(\mathrm{ord}(\rho_1), \mathrm{ord}(\rho_2), \mathrm{ord}(\rho_3)) = 2 \cdot 3 = 6$, produzieren wir hier wieder ein Element der Ordnung 6.

- *Fall $r = 4$:* Dann ist $\mathrm{ord}(\rho_1) + \mathrm{ord}(\rho_2) + \mathrm{ord}(\rho_3) + \mathrm{ord}(\rho_4) \in \{4, 6, 8\}$. Wegen $r = 4$ ist $\mathrm{ord}(\rho_i) \geq 2$für alle $1 \leq i \leq 4$, also ist nur eine Zerlegung in 4 disjunkte 2-Zykel möglich. Das liefert uns Elemente der Ordnung $\mathrm{kgV}(2, 2, 2, 2) = 2$ in $A_8$.

Es gibt also Elemente der Ordnung $m \in \{1, 2, 3, 4, 5, 6, 7, 15\}$ in $A_8$. □

**Aufgabe 9** (a) Gesucht ist die Ordnung von

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 10 & 5 & 6 & 7 & 4 & 1 & 2 & 9 & 8 \end{pmatrix} \in S_{10}. \tag{40}$$

Hierzu zerlegen wir $\sigma$ in disjunkte Zykel. Es ist $\sigma = (1357) \odot (2108) \odot (46)$. Laut Vorlesung gilt nun

$$\mathrm{ord}(\sigma) = \mathrm{kgV}(\mathrm{ord}(1357), \mathrm{ord}(2108), \mathrm{ord}(46)) = \mathrm{kgV}(4, 3, 2) = 12, \tag{41}$$

da für einen Zykel der Länge $k$ die Ordnung dieses Zykels gerade $k$ ist.
(b) Gesucht ist die Ordnung von $\sigma = (345) \odot (456) \odot (567) \in S_7$. Offenbar ist $\sigma$ nicht in disjunkte Zykel zerlegt. Es gilt $\sigma = (67) \odot (453)$ in disjunkter Zykel-Zerlegung. Damit lässt sich das Vorgehen zur Ordnungbestimmung aus Teil (a) anwenden: $\mathrm{ord}(\sigma) = \mathrm{kgV}(\mathrm{ord}(67), \mathrm{ord}(453)) = \mathrm{kgV}(2, 3) = 2 \cdot 3 = 6$. □

**Aufgabe 10** Gesucht ist die Anzahl der Elemente vom Zerlegungstyp (33) in $S_6$. Da jedes Element in $S_6$ eine bis auf Reihenfolge eindeutige Zerlegung in disjunkte Zykel erlaubt, erhalten wir die gewünschte Anzahl, indem wir $\sigma = \rho_1 \cdot \rho_2$ darstellen, wobei $\rho_1, \rho_2$ disjunkte 3-Zykel sind. Die Anzahl der gesuchten Elemente ist also die Anzahl aller möglichen Kombinationen disjunkter 3-Zykel (bis auf Reihenfolge). Für die Wahl des ersten 3-Zykels haben wir $(3-1)! \begin{pmatrix} 6 \\ 3 \end{pmatrix} = 2 \cdot 20 = 40$ Möglichkeiten laut eines Vorlesungsresultats. Der Träger des zweiten 2-Zykels liegt nach Wahl des ersten 3-Zykels bereits fest. Also haben wir nur noch $(3-1)! = 2$ Möglichkeiten, den zweiten 3-Zykel zu wählen: Naiv gibt es 3! Möglichkeiten, die verbleibenden 3-Elemente anzuordnen, aber wegen der Zykel-Eigenschaft sind je 3-Möglichkeiten durch zyklische Vertauschung erhalten, definieren also denselben 3-Zykel. Insgesamt haben wir also $2 \cdot 40 = 80$ Möglichkeiten, die beiden 3-Zykel anzuordnen. Da die beiden Zykel disjunkt sind, kommutieren sie, d.h., die Anzahl aller Kombinationen der 3-Zykel, 80, ist durch die Anzahl der Möglichkeiten zu dividieren, die Zykel anzuordnen. Dies sind $2! = 2$. Damit finden wir, dass es $80/2 = 40$ Elemente von Zerlegungstyp (33) in $S_6$ gibt. □

**Aufgabe 11** Gesucht ist die Anzahl der Elemente der Ordnung 2 in $S_8$. Sei $\sigma \in S_8$ beliebiges Element der Ordnung 2. Als Element einer symmetrischen Gruppe, kann $\sigma$ in disjunkte Zykel $\sigma = \rho_1 \odot ... \odot \rho_r$ mit $r \in \mathbb{N}$ zerlegt werden. Für die Ordnung von $\sigma$ gilt dann laut Vorlesung $\text{ord}(\sigma) = \text{kgV}(\text{ord}(\rho_1), ..., \text{ord}(\rho_r))$. Da $\text{ord}(\sigma) = 2 \in \mathbb{P}$, muss $\text{ord}(\rho_i) = 2$ für alle $1 \leq i \leq r$ der $r$ Zykel in derdisjunkten Zykel-Zerlegung von $\sigma$ gelten. Da die Zykel disjunkt sind, ist nur $r \in \{1, 2, 3, 4\}$ möglich. Wir bestimmen also die Anzahlen für jeden möglichen Wert von $r$ separat.

- *Fall $r = 1$:* Laut einem Vorlesungsresultat gibt es $(2-1)! \begin{pmatrix} 8 \\ 2 \end{pmatrix} = 28$ Möglichkeiten, einen 2-Zykel aus $S_8$ zu finden. Da nun $\sigma = \rho_1$ mit dem 2-Zykel $\rho_1$ gilt, haben wir 28 Möglichkeiten, $\sigma \in S_8$ zu finden.

- *Fall $r = 2$:* Dann gilt $\sigma = \rho_1 \odot \rho_2$ mit zwei disjunkten 2-Zykeln $\rho_1, \rho_2 \in S_8$. Für den ersten 2-Zykel gibt es nach Fall 1 28 Möglichkeiten. Für den zweiten 2-Zykel zur Definition des Trägers nur noch 6 Auswahlmöglichkeiten zur Verfügung. Entsprechend gibt es für diesen nur noch $(2-1)! \begin{pmatrix} 6 \\ 2 \end{pmatrix} = 15$ Möglichkeiten. Wir haben $15 \cdot 28$ Möglichkeiten, ein Paar disjunkter 2-Zykel in $S_8$ zu finden. Aus der Vorlesung ist ferner bekannt, da disjunkte Zykel kommutieren. Daher definieren je 2 der $28 \cdot 15$ Möglichkeiten dasselbe $\sigma$. Damit finden wir $28 \cdot 15/2 = 14 \cdot 15 = 210$ verschiedene Möglichkeiten $\sigma$ aus 2-Zykeln aufzubauen.

- *Fall $r = 3$:* Dann gilt $\sigma = \rho_1 \odot \rho_2 \odot \rho_3$ mit paarweise disjunjten 2-Zykeln $\rho_1, \rho_2, \rho_3 \in S_8$. In Fall 2 haben wir bereits gesehen, dass es $28 \cdot 15 = 420$ Möglichkeiten gibt, ein Paar von disjunkten 2-Zykeln $(\rho_1, \rho_2) \in S_8 \times S_8$ zu wählen. Für den Träger des dritten Zykels stehen nun noch $(2-1)! \begin{pmatrix} 4 \\ 2 \end{pmatrix} = 6$ Möglichkeiten zur Verfügung. Somit haben wir $420 \cdot 6$ Möglichkeiten, ein Tripel

paarweise disjunkter 2–Zykel in $S_8 \times S_8 \times S_8$ zu finden. Da die Zykel jeweils paarweise disjunkt sind, kommutieren sie jeweils paarweise. Wir haben $3! = 6$ Möglichkeiten, die drei 2-Zykel anzuordnen und dasselbe $\sigma = \rho_1 \odot \rho_2 \odot \rho_3$ zu produzieren. Damit finden wir $6 \cdot 420/6 = 420$ Möglichkeiten, ein $\sigma \in S_8$ vom Zerlegungstyp $(2, 2, 2)$ zu produzieren.

- *Fall $r = 4$:* Dann gilt $\sigma = \rho_1 \odot \rho_2 \odot \rho_3 \odot \rho_4$ mit paarweise disjunkten 2-Zykeln $\rho_1, \rho_2, \rho_3, \rho_4 \in S_8$. Da durch die Angabe der ersten drei 2-Zykel bereits der Träger des Zykels $\rho_4$ festgelegt ist und weil darüber hinaus $\rho_4$ bereits dadurch als 2-Zykel festgelegt ist, haben wir wie in Fall 3 genau$6 \cdot 420$ Möglichkeiten das Quadrupel $(\rho_1, \rho_2, \rho_3, \rho_4)$ von paarweise disjunkten 2-Zykeln $\rho_1, \rho_2, \rho_3, \rho_4 \in S_8$ zu wählen. Infolge der Disjunktheit der Zykel, kommutieren diese 2-Zykel jeweils paarweise, so dass wir die Anzahl der Möglichkeiten, das obige Quadrupel zu wählen, durch die Anzahl der Möglichkeiten, die Komponenten mit der Komposition $\odot$ in $S_8$ anzuordnen, dividieren müssen. Wir haben $r! = 4!$ Möglichkeiten, dies zu tun. Somit finden wir $6 \cdot 420/4! = 105$ verschiedene $\sigma \in S_8$, die eine Zerlegung in 4 disjunkte 2-Zykel erlauben.

Die Anzahl aller Möglichkeiten, $\sigma \in S_8$ der Ordnung 2 zu erhalten, ergibt sich indem wir die Anzahlen aller Möglichkeiten, $\sigma \in S_8$ der Ordnung 2 und von vorgegebenen Zerlegungstyp gemäß der obigen Fallunterscheidung, addieren. Das liefert $28+210+420+105 = 763$ verschiedene Elemente der Ordnung 2 in der $S_8$. □

**Aufgabe 12 (H15T2A1)** Gesucht sind alle Matrizen $A$ in $\mathrm{GL}_2(\mathbb{C})$, so dass $AB = BA$ für die Matrix

$$B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \tag{42}$$

gilt. Sei dazu die Matrix $A$ in der Form

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \tag{43}$$

mit $a, b, c, d \in \mathbb{C}$ und $\det A = ad - bc \neq 0$, dargestellt. Wir rechnen

$$AB = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix} \tag{44}$$

$$BA = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix}. \tag{45}$$

Wegen $AB = BA$ erhalten wir die Gleichungen $a = a + c$, $a + b = b + d$, $c = c$ und $c + d = d$ durch Gleichsetzen der jeweiligen Einträge in $AB$ und $BA$. Damit finden wir $c = 0$ und $d = a$. Die gesuchten Matrizen sind also von der Form

$$A = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}, \tag{46}$$

wobei die Forderung $A \in \mathrm{GL}_2(\mathbb{C}) \Leftrightarrow \det A = a^2 \neq 0$, also $a \neq 0$ erzwingt. Die Menge $M$ aller Matrizen mit den gewünschten Eigenschaften ist daher

$$M = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in \mathcal{M}(2 \times 2; \mathbb{C}) \,\middle|\, a \in \mathbb{C}^\times, b \in \mathbb{C} \right\}. \tag{47}$$

**Aufgabe 13 (H13T2A5)** Sei $G = S_5$. Wir finden zunächst die Anzahl der Elemente der $S_5$, die Ordnung 4 haben. Sei dazu $\sigma \in G$ Element der Ordnung 4. Als Element einer symmetrischen Gruppe hat $\sigma$ eine Zerlegung in paarweise disjunkte Zykel $\rho_1, ..., \rho_r \in S_5$ für ein $r \in \mathbb{N}_0$, d.h., $\sigma = \rho_1 \odot \rho_2 \odot ...\rho_r$ wenn wir die Verknüpfung auf $G$ mit $\odot$ bezeichnen. Aus der Vorlesung ist bekannt, dass die Ordnung von $\sigma$ und der Faktoren $\rho_1, ..., \rho_r$ in der disjunkten Zykeldarstellung über $\text{ord}(\sigma) = \text{kgV}(\text{ord}(\rho_1), ..., \text{ord}(\rho_r))$ zusammenhängen. Da Zykel in der $S_5$ nur Längen $k \in \{2, 3, 4, 5\}$ haben (Identität bleibt unbeachtlich), können wir $\sigma$ nur durch einen 4-Zykel repräsentieren. Die Möglichkeit, $\sigma$ durch einen 4- und einen dazu disjunkten 2-Zykel darzustellen, scheidet aus, da die Disjunktheit bereits erzwingt, Permutationen der $M_6 = \{1, 2, 3, 4, 5, 6\}$ zu betrachten, wir aber nur in $G = S_5 = \text{Per}(M_5)$ arbeiten. Damit ist $\sigma$ bereits auf den Zerlegungstyp (4) festgelegt. Die Anzahl der verschiedenen 4-Zykel in $S_5$ berechnet sich nach Vorlesungsergebnissen gemäß $(4-1)! \begin{pmatrix} 5 \\ 4 \end{pmatrix} = 5 \cdot 6 = 30$. Also gibt es 30 verschiedene Elemente der Ordnung 4 in $S_5$. In einem zweiten Schritt ist die Anzahl der Untergruppen der $S_5$ zu klären, die die Ordnung 4 haben. Sei $U \leq G$ Untergruppe der Ordnung 4. Da $4 = 2^2$ ein Primzahlquadrat ist, ist $U$ laut Vorlesung abelsche Gruppe. Als endliche abelsche Gruppe ist auf $U$ der Hauptsatz über endlich erzeugte abelsche Gruppen in der Fassung für endliche abelsche Gruppen anwendbar. Dieser liefert nun die Kandidaten $U \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = U_1$ und $U \simeq \mathbb{Z}/4\mathbb{Z} = U_2$ als Isomorphietypen. Diese sind tatsächlich verschiedene Isomorphietypen für 4–elementige Gruppen, da in $U_1$ nur Elemente der Ordnung 2 vorkommen, $U_2$ aber zyklisch von Ordnung 4 ist, also ein Element der Ordnung 4 enthält. Wir unterscheiden also:

- *Fall $U \simeq U_2$:* In diesem Fall wird $U$ von einem 4-Zykel $\sigma \in S_5$ erzeugt. Sei $g \in U$ Element der Ordnung 4. Wegen $\Phi(4) = 2^2 - 2^1 = 2$, gibt es in $U$ genau 2–Elemente der Ordnung 4. Also liegen jeweils zwei (geeignete) 4-Zykel in einer Untergruppe $U \simeq U_2$. Die Anzahl der Untergruppen vom Typ $U_2$ ist also gerade halb so groß wie die Anzahl der 4-Zykel in $S_5$: Damit gibt es $30/2 = 15$ zyklische Untergruppen der Ordnung 4 von $S_5$.

- *Fall $U \simeq U_1$:* In diesem Fall benötigen wir zwei verschiedene Elemente der Ordnung 2, die $U$ erzeugen. Da aber $U \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, also isomorph zu einem äußeren direkten Produkt von Gruppen ist, in dem jeder zyklische Faktor Normalteiler ist, liefert die Isomorphie $\sigma_1\langle\sigma_2\rangle\sigma_1^{-1} = \langle\sigma_2\rangle$ wobei $\sigma_1 \in \langle\sigma_1\rangle$ ein erzeugendes Element ist. Die Elemente der Ordnung 2 in $S_5$ sind Transpositionen und Doppeltranspositionen. Sei zunächst $\sigma_1 = (ij)$ und $\sigma_2 = (kl)$. Falls $k \in \{i, j\}$, ohne Beschränkung der Allgemeinheit $k = i$, gilt $\sigma_1\sigma_2\sigma_1^{-1} = (ij)(il)(ij) = (jil) \notin \langle(il)\rangle$ für $j \neq l$. Falls $j = l$, gilt $\sigma_1 = \sigma_2$ im Widerspruch dazu, dass $\sigma_1 \neq \sigma_2$ gelten muss. Für den Fall von Transposition sind also nur $(ij)$ und $(jk)$ mit paarweise verschiedenen $i, j, k, l \in M_5$ zugelassen. Betrachten wir den Fall, dass $\sigma_1 = (ij)$ Transposition und $\sigma_2 = (kl)(mn)$ Doppeltransposition ist. Einer der Einträge $k, l, m, n$ stimmt mit einem der Einträge $i, j$ überein. Ohne Beschränkung der Allgemeinheit $k = j$. Dann gilt $\sigma_1\sigma_2\sigma_1^{-1} = (ij)(jl)(mn)(ij) = (ilj)(mn)$, was aber im Widerspruch dazu steht, dass es in $U$ kein Element der Ordnung 3 gibt. Also fällt ein wei-

terer Eintrag der Doppeltransposition mit dem Eintrag $i$ der Transposition zusammen. Dann gilt $(kl)(mn) = (ji)(mn)$ oder $(kl)(mn) = (jl)(in)$. Im ersteren Fall gilt $\sigma_1\sigma_2\sigma_1^{-1} = (ij)(ji)(mn)(ij) = (ij)(mn) = \sigma_2 \in \langle\sigma_2\rangle$. Frei wählbar ist also nur $(mn)$ mit $m, n \in M_5$ verschieden und paarweise verschieden von $i, j \in M_5$. Wegen $\sigma\sigma_2 = (mn)$ entspricht dieser Fall aber gerade dem Fall, dass wir zwei Transpositionen $(ij)$ und $(kl)$ mit paarweise verschiedenen $i, j, k, l \in M_5$ wählen. Im zweiten Fall gilt $(ij)(jl)(in)(ij) = (iljn)$, aber es gibt kein Element der Ordnung 4 in $U$ im Falle $U \simeq U_1$. Also können wir uns auf den Fall zurückziehen, dass $U$ von zwei disjunkten Transpositionen erzeugt wird. Für die Wahl eines Paares disjunkter Transpositionen aus $S_5$ haben wir $\begin{pmatrix} 5 \\ 2 \end{pmatrix}\begin{pmatrix} 3 \\ 2 \end{pmatrix} = 30$ Möglichkeiten. Da disjunkte Transpositionen kommutieren, erzeugen gibt also doppelt so viele Möglichkeiten, Paare disjunkter Transpositionen zu bilden wie von ihnen erzeugte, verschiedene Untergruppen. Damit finden wir $30/2 = 15$ verschiedene, von disjunkten Transpositionen in $S_5$ erzeugte Untergruppen. Zuletzt betrachten wir den Fall, dass $\sigma_1$ und $\sigma_2$ Doppeltranspositionen sind. Offenbar muss zusätzlich $\sigma_1 \neq \sigma_2$ gelten. Als Doppeltranspositionen haben $\sigma_1$ und $\sigma_2$ je einen Fixpunkt. Es haben $\sigma_1$ und $\sigma_2$ sogar einen gemeinsamen Fixpunkt: Denn falls $i$ Fixpunkt von $\sigma_2$ aber $i \mapsto j$ unter $\sigma_1$, dann gilt $\sigma_1(\sigma_2(i)) = \sigma_1(i) = j$ aber $\sigma_2(\sigma_1(i)) = \sigma_2(j) \neq i$. Das ist ein Widerspruch zur Normalteiler-Eigenschaft $\langle\sigma_i\rangle \trianglelefteq U$ für $i \in \{1, 2\}$, denn $\sigma_1 \circ \sigma_2\sigma_1^{-1} \in \langle\sigma_2\rangle$ impliziert $\sigma_1\sigma_2\sigma_1 = \mathrm{id}$ oder $\sigma_1\sigma_2\sigma_1 = \sigma_2$, da $\mathrm{ord}(\sigma_1) = 2 = \mathrm{ord}(\sigma_2)$. Ersteres scheidet aus, denn andernfalls folgt $\sigma_1 = \sigma_2$ im Widerspruch dazu, dass $|U| = 4 > 2$. Im zweiten Fall haben wir $\sigma_1\sigma_2 = \sigma_2\sigma_1$, d.h., $\sigma_1$ und $\sigma_2$ kommutieren. Wenn also, im obigen Teil $\sigma_1$ und $\sigma_2$ keinen gemeinsamen Fixpunkt haben, dann kommutieren $\sigma_1$ und $\sigma_2$ also nicht. Da nun $U = \{\mathrm{id}, \sigma_1, \sigma_2, \sigma_1 \circ \sigma_2\}$ und $\sigma_1 \circ \sigma_2$ als Fixpunkt den bereits von $\sigma_1$ und $\sigma_2$ gemeinen Fixpunkt hat, können wir die Anzahlen für den Fall, dass $U$ von zwei Doppeltranspositionen erzeugt wird angand der Anzahlen der möglichen Fixpunkte (aller Gruppelemente) abzählen. Da $|M_5| = 5$, gibt es also genau 5 Möglichkeiten, $U$ aus Doppeltranspositionen zu erzeugen.

Insgesamt haben wir also $15 + 15 + 5 = 35$ Untergruppen der Ordnung 4 in $S_5$.

**Aufgabe 14 (F04T2A1)** Gesucht ist explizit eine Untergruppe der Ordnung 21 von $S_7$. Sei $U$ Untergruppe der Ordnung 21 von $S_7$. Da $|U| = 21 = 3 \cdot 7$ gibt es in $U$ echte Untergruppen nur von Primzahlordnung. Nach dem Satz von Cauchy gibt es ferner in $U$ ein Element der Ordnung 3 und eines der Ordnung 7. Sei $V$ Untergruppe der Ordnung 7 von $U$. Da $(U : V) = 3$ und 3 der kleinste Primteiler von $|U| = 21$ ist, ist die Untergruppe der Ordnung 7 Normalteiler von $U$. Die Elemente der Ordnung 7 in $S_7$ beinhalten die 7-Zykel. Wähle also den 7-Zykel $\sigma = (1234567) \in S_7$ und setze $V = \langle\sigma\rangle$. Wir benötigen nun noch eine Untergruppe der Ordnung 3 von $S_7$. Hierzu wähle z.B. den 3-Zykel $\rho = (123)$, der als 3-Zykel die Ordnung 3 hat. Offenbar ist $\langle\rho\rangle \cap \langle\sigma\rangle = \{\mathrm{id}\}$ in $S_7$, denn jedes Element aus $\langle\rho\rangle$, das nicht die Identität ist, hat die Fixpunktmenge $M_a = \{4, 5, 6, 7\}$, wohingegen jedes von der Identität verschiedene Element aus $\langle\sigma\rangle$ keinen Fixpunkt besitzt. Abgesehen von der Identität können also $\langle\rho\rangle$ und $\langle\tau\rangle$ kein weiteres gemeinsames Element besitzen. Damit ist

das innere semidirekte Produkt $U = \langle\rho\rangle\langle\sigma\rangle$ eine Untergruppe mit den gewünschten Eigenschaften. Die Gleichheit $U = \langle\rho\rangle\langle\sigma\rangle$ folgt dabei daraus, dass $\langle\rho\rangle\langle\sigma\rangle \subset U$ nach Definition des inneren semidirekten Produkts und der Satz von Lagrange liefert nun die Gleichheit der Ordnungen von $U$ und $\langle\rho\rangle\langle\sigma\rangle$, denn $\langle\sigma\rangle \cap \langle\rho\rangle = \{\mathrm{id}\}$ wegen Teilefremdheit der Ordnungen. □

**Aufgabe 15 (H11T3A1)** Zu bestimmen sind für alle $n \geq 5$ natürlich die Normalteiler der symmetrischen Gruppe $S_n$. Dabei ist vorauszusetzen, dass $A_n$ einfach ist, wiederum für alle $n \geq 5$. Sei also $n \geq 5$ natürlich. Als Kern des Signums-Homomorphismus $\mathrm{sign} : S_n \to \{-1, 1\}$, wobei $\{-1, 1\}$ mit der gewöhnliche Multiplikation zu einer Gruppe wird, ist die $A_n$ Normalteiler von $S_n$. Denn $A_n := \{\sigma \in S_n : \mathrm{sign}(\sigma) = 1\}$ per Definition. Laut Vorlesung ist zu einer beliebigen Gruppe $G$ stets die triviale Untergruppe, die nur das Neutralelement enthält, und die Gruppe selbst Normalteiler. Also gilt $\{\mathrm{id}\} \trianglelefteq S_n$ und $S_n \trianglelefteq S_n$, indem wir das Resultat auf $G = S_n$ anwenden. Laut Angabe ist die $A_n$ für $n \geq 5$ einfach. Das bedeutet, die $A_n$ hat genau zwei Normalteiler, nämlich die triviale Untergruppe $\{\mathrm{id}\} \trianglelefteq A_n$ und sich selbst $A_n \trianglelefteq A_n$. Wir behaupten, dass für $n \geq 5$ für einen beliebigen Normalteiler $N$ von $S_n$ gilt $N \in \{\{\mathrm{id}, A_n, S_n\} \equiv \mathcal{N}$. Nachgewiesen wurde schon, dass es sich bei allen Elementen in der angegebenen Menge um Normalteiler handelt. Zu zeigen ist noch, dass die Menge wirklich alle Normalteiler der $S_n$ enthält. Sei dazu $N$ Normalteiler von $S_n$ aber $N \notin \mathcal{N}$. Dann ist $N' \equiv N \cap A_n$ Normalteiler von $A_n$ laut Vorlesung. Falls $N \subseteq A_n$, folgt $N \in \mathcal{N}$, im Widerspruch zur Voraussetzung $N \notin \mathcal{N}$. Falls $N \not\subseteq A_n$, gibt es ein Element $\sigma \in S_n \setminus A_n$, so dass $\sigma \in N$. Da $N' \trianglelefteq A_n$, ist entweder $N'$ die triviale Untergruppe oder ganz $A_n$. Im ersteren Fall ist $\sigma$ ein Element der Ordnung 2 in $S_n$. Da aber aus Gründen der Gruppenordnung gilt $\langle N \cup A_n\rangle = S_n$, liefert der erste Isomorphie-Satz zusammen mit dem Satz von Lagrange den Widerspruch $|A_n/N'| = |A_n| = |S_n|/2 = |S_n/N|$, denn $N$ enthält mit einem Element $\sigma$ der Ordnung 2 auch alle anderen Elemente der Ordnung 2 und vom selben Zerlegungstyp. Für $n \geq 5$ ist dies mehr als eins. Im zweiteren Fall ist $N$ bereits ganz $S_n$ aus Gründen der Gruppenordnung, $\langle N \cup A_n\rangle = S_n$. □

**Aufgabe 16 (H12T3A2)** Sei $n \in \mathbb{N}$ und $G = S_n$. Zu zeigen ist, dass $C_G((12...n)) = \langle(12...n)\rangle$. Sei $\sigma \in C_G((12...n))$. Dann gilt $\sigma(12...n)\sigma^{-1} = \sigma$. Durch die Äquivalenzumformung "Multiplikation mit $\sigma$ von rechts bzgl. der Verknüpfung auf $S_n$" finden wir $\sigma(12....n) = (12...n)\sigma$. "$\supseteq$": Ein beliebiges $\sigma \in \langle(12....n)\rangle$ ist von der Form $\sigma = (12....n)^k$ mit $0 \leq k \leq n-1$. Damit folgt $\sigma(12...n) = (12...n)^k(12...n) = (12...n)^{k+1} = (12...n)^{(k+1)\bmod(n)}$ und $(12...n)\sigma = (12...n)(12...n)^k = (12...n)^{k+1} = (12...n)^{k+1} = (12....n)((k+1)\bmod(n))$, also in der Tat $\sigma(12...n) = (12...n)\sigma$ und damit $\sigma \in C_G((12...n))$. "$\subseteq$". Aus der Vorlesung ist bekannt, dass $|G((12...n))| = (G : C_G((12...n)))$. Wegen $G((12...n)) = \{\sigma' \in S_n : \sigma' = \sigma(12...n)\sigma^{-1}, \sigma \in G\}$, ist $\sigma'$ ein zu $\sigma$ konjugiertes Element und insbesondere vom selben Zerlegungstyp, also ebenfalls ein $n$-Zykel der $S_n$. In $S_n$ gibt es aber $(n-1)!$ $n$-Zykel, so dass $|G((12...n))| = (n-1)!$. Nach dem Satz von Lagrange gilt also $(G : C_G((12...n))) = |G|/|C_G((12...n))| = |G((12...n))|$, d.h., $|C_G((12...n))| = |G|/|G((12....n))| = n!/(n-1)! = n$. Damit ist $C_G((12...n))$ eine Untergruppe der $S_n$ von Ordnung $n$, die die zyklische Gruppe $\langle(12....n)\rangle$, ebenfalls von Ordnung $n$, enthält, wie im ersten Teil des Beweises gezeigt wurde. Also

gilt aus Ordnungsgründen $C_G((12....n)) = \langle (12...n) \rangle$. $\square$

**Aufgabe 17 (H12T1A1)** Sei $p \in \mathbb{P}$ und $q = p^l$ für $l \in \mathbb{N}$ und $G = \mathrm{SL}_2(\mathbb{F}_q)$. Zu zeigen ist zunächst $|\mathrm{SL}_2(\mathbb{F}_q)| = q^2(q^2-1)$. Nach Definition ist die spezielle lineare Gruppe gerade der Kern des Gruppenhomomorphismus $\det : GL_2(\mathbb{F}_q) \to \mathbb{F}_q^\times$ von der allgemeinen linearer Gruppe über $\mathbb{F}_q$ in die Einheitengruppe $\mathbb{F}_q^\times$ von $\mathbb{F}_q$. Der Homomorphiesatz liefert nun eine Isomorphismus $\bar{\det} : \mathrm{GL}_2(\mathbb{F}_q)/(\mathrm{SL}_2(\mathbb{F}_q)) \to \mathbb{F}_q^\times$. Es gilt dann mit dem Satz von Lagrange $|\mathrm{GL}_2(\mathbb{F}_q)^|/|\mathrm{SL}_2(\mathbb{F}_q)| = |\mathbb{F}_q^\times| = q-1$, wobei im letzten Schritt verwendet wurde, dass jedes von $0_{\mathbb{F}_q}$ verschiedene Element von $\mathbb{F}_q$ in der Einheitengruppe $\mathbb{F}_q^\times$ liegt und $\mathbb{F}_q$ der Körper mit $q$ Elementen ist. Durch Umformung ergibt sich nun $|\mathrm{SL}_2(\mathbb{F}_q)| = |\mathrm{GL}_2(\mathbb{F}_q)|/(q-1)$. Aus der linearen Algebra ist bekannt, dass $A \in \mathrm{GL}_2(\mathbb{F}_q)$ äquivalent dazu ist, dass die Spaltenvektoren $v_1, v_2 \in \mathbb{F}_q^2$ linear unabhängig sind. Für $v_1$ können wir einen beliebigen Vektor $v_1 \in \mathbb{F}_q^2 \setminus \{(0_{\mathbb{F}_q}, 0_{\mathbb{F}_q})\}$ wählen. Es gibt also $q^2-1$ Möglichkeiten, $v_1$ zu wählen. Der Vektor $v_2$ kann nun aus $\mathbb{F}_q^2 \setminus \mathrm{lin}_{\mathbb{F}_q}(v_1)$ beliebig gewählt werden: Wir haben also für die Wahl von $v_2$ genau $q^2-q$ Möglichkeiten. Zusammen haben wir also $(q^2-1)(q^2-q)$ Möglichkeiten $v_1, v_2$ linear unabhängig und damit $A \in \mathrm{GL}_2(\mathbb{F}_q)$ zu wählen. Damit ist $|\mathrm{GL}_2(\mathbb{F}_q)| = (q^2-1)(q^2-q)$. Also $|\mathrm{SL}_2(\mathbb{F}_q)| = |\mathrm{GL}_2(\mathbb{F}_q)|/(q-1) = (q^2-1)(q^2-q)(q-1) = q(q^2-1)$. Seien $N^-$ und $B$ wie in der Angabe definiert. Laut Angabe sind $N^- \leq G$ und $B \leq G$. Da $G$ und damit auch die Untergruppen $N^-, B$ von endlicher Ordnung sind, liefert der Satz von Lagrange $|\Omega| = |G|/|B|$. Die Ordnung der Gruppe $B$ lässt sich direkt aus der Definition ablesen: $|B| = (q-1)q$, denn $\mathbb{F}_q^\times$ enthält keine von der 1 verschiedenen Elemente, die zu sich selbst invers sind. Es folgt $|\Omega| = q+1$. Für $N^-$ ergibt sich $|\mathbb{F}_q| = q$. Zu zeigen ist nun, dass die Operation $\odot : N^- \times \Omega \to \Omega, (A, \bar{b}) \mapsto A \cdot \bar{B}$ einen Fixpunkt besitzt. Bezeichne dazu $F$ die Fixpunktmenge der Operation und $R \subseteq B$ ein Repräsentantensystem der Bahnen der Operation, so dass die Bahnen mindestens die Länge 2 haben. Dann gilt die Bahnengleichung:

$$|\Omega| = |F| + \sum_{\bar{B} \in R} (N^- : N^-_{\bar{B}}), \tag{48}$$

wobei $N^-_{\bar{B}}$ den Stabilisator des Elements $\bar{B} \in B$ unter der betrachteten Operation bezeichnet. Da $N^-_{\bar{B}} \leq N^-$ laut Vorlesung und $|N^-| = q$ endlich ist, gilt nach Lagrange $2 \leq (N^- : N^-_{\bar{B}}) = |N^-|/|N^-_{\bar{B}}| = q/|N^-_{\bar{B}}|$. Da $q = p^l$ mit natürlichem $l$, muss $|N^-_{\bar{B}}| \in \{1, ..., p^{l-1}\}$. Wegen $|\Omega| = q+1$ folgt mit der obigen Bahnengleichung

$$p^l + 1 = |F| + \sum_{\bar{B} \in R} \frac{p^l}{p^{k(\bar{B})}} \tag{49}$$

und $k(\bar{B}) \in \{1, ...., l-1\}$. Jeder Beitrag zur Summe über $\bar{B}$ ist durch $p$ teilbar, so dass

$$1 \equiv (p^l + 1) \bmod(p) \equiv |F| \bmod(p), \tag{50}$$

also $|F| = 1 + lp$ mit $l \in \mathbb{N}_0$ gilt, insbesondere also $|F| \geq 1$. Somit hat die betrachtete Operation mindestens einen Fixpunkt. $\square$

**Aufgabe 18** Sei $U \leq S_7$ definiert als $U = \langle (12)(34)(567) \rangle$ und definiere die Abbildung $\alpha : U \times M_7 \to M_7, (\sigma, k) \mapsto \sigma(k)$. Wir zeigen, dass $\alpha$ eine Gruppenoperation ist. Es ist $\alpha(\mathrm{id}, k) = \mathrm{id}(k) = k$ für alle $k \in M_7$. Für $\sigma, \tau \in U$ gilt ferner $\alpha(\sigma(\alpha, \tau(k))) = \alpha(\sigma, (\tau(k))) = \sigma(\tau(k)) = (\sigma \circ \tau)(k) = \alpha(\sigma \circ \tau, k)$ für alle $k \in M_7$. Damit ist $\alpha : U \times M_7 \to M_7$ in der Tat eine Gruppenoperation. Gesucht sind nun die Bahnen $G(k)$ für alle $k \in M_7$. Es gilt $G(1) = \{1, 2\} = G(2)$, $G(3) = \{3, 4\} = G(4)$ und $G(5) = G(6) = G(7) = \{5, 6, 7\}$. Dies sind alle Bahnen, denn $G(1) \uplus G(3) \uplus G(5) = M_7$. Da jede Bahn die Länger $\geq 2$ hat, gilt für die Ordnung des Stabilisators $U_k$, dass $|U_k|||U|$ als echter Teiler (also $|U_k| < |U| = \mathrm{kgV}(2, 2, 3) = 6$). Da die Operation aber nicht-transitiv ist, weil bereits $G(5) \cap G(1) = \emptyset$, gibt es nur die Möglichkeiten $|U_k| \in \{2, 3\}$. Genauer gilt nun mit $\sigma = (12)(34)(567)$, dass $U_k = \{\mathrm{id}, \sigma^2, \sigma^4\} =$ für $k \in \{1, 2, 3, 4\}$ und $U_k = \{\mathrm{id}, \sigma^3\}$ für $k \in \{5, 6, 7\}$. □

**Aufgabe 19** Gesucht sind alle Untergruppen $U$ der Ordnung 4 von $S_5$, so dass $U$ nur die Identität und Doppeltranspositionen enthält. In der $S_5$ gibt es 10 Transpositionen. Ist eine Transposition fixiert, gibt es noch 3 weitere Möglichkeiten eine weitere Transposition mit disjunktem Träger zu wählen. Da die beiden Transpositionen disjunkte Träger haben,kommutieren sie miteinander, so dass wir insgesamt $3 \cdot 10/2! = 15$ Doppeltranspositionen in $S_5$ haben. Sei nun $U$ eine Untergruppe mit den geforderten Eigenschaften und seien $\sigma, \tau$ Doppeltranspositionen in $U$. Da $|\mathrm{supp}(\sigma)| = 4 = |\mathrm{supp}(\tau)| = 4 = 5 - 1$, hat jede Doppeltranspositionen einen Fixpunkt $i = i(\tau) \in M_5$, der von der jeweiligen Doppeltransposition $\tau$ abhängt. Wir zeigen nun, dass für $\sigma, \tau \in U$, die Fixpunkte der beiden Doppeltranspositionen identisch sind. Angenommen, dies ist nicht so. Bezeichne $i \in M_5$ den Fixpunkt von $\sigma$. Dann gilt $\sigma(i) = i$ infolge der Fixpunkteigenschaft von $i$. Nach Annahme gilt $j \equiv \tau(i) \neq i$, da $\tau$ und $\sigma$ verschiedene Fixpunkte haben. Dann gilt $\tau(\sigma(i)) = \tau(i) = j$ aber $\sigma(\tau(i)) = \sigma(j) \neq j$, da $j$ nicht Fixpunt von $\sigma$. Da $|U| = 4 = 2^2$ Primzahlquadrat, ist $U$ abelsch, so dass $\sigma \circ \tau = \tau \circ \sigma$ für $\sigma, \tau \in U$. Insbesondere müsste gelten $(\sigma \circ \tau)(i) = \sigma(j) = j = (\tau \circ \sigma)(i)$ im Widerspruch zu $\sigma(j) \neq j$. Daher war die Annahme falsch und die Doppeltranspositionen in einer Untergruppe $U$ haben jeweils denselben Fixpunkt $i \in M_5$. Wir haben insgesamt 5 Möglichkeiten, diesen Fixpunkt zu wählen, also 5 Untergruppen der Ordnung 4 mit der geforderten Eigenschaft. Explizit:

$$U_1 = \{\mathrm{id}, (23)(45), (24)(35), (25)(34)\}, \tag{51}$$
$$U_2 = \{\mathrm{id}, (13)(45), (14)(35), (15)(34)\}, \tag{52}$$
$$U_3 = \{\mathrm{id}, (21)(45), (24)(15), (25)(14)\}, \tag{53}$$
$$U_4 = \{\mathrm{id}, (23)(15), (21)(35), (25)(31)\}, \tag{54}$$
$$U_5 = \{\mathrm{id}, (23)(41), (24)(31), (21)(34)\}. \tag{55}$$

□

**Aufgabe 20** Gesucht sind zwei Matrizen $A, B \in \mathrm{GL}_n(\mathbb{C})$, so dass gilt: (i) $A$ ist nicht ähnlich zu $B$, (ii) die charakteristischen Polynome $\chi_A, \chi_B \in \mathbb{C}[x]$ stimmen überein, $\chi_A(x) = \chi_B(x)$ für alle $x \in \mathbb{C}$ und (iii) die Minimalpolynome $\mu_A, \mu_B \in \mathbb{C}[x]$ stimmen überein, $\mu_A(x) = \mu_B(x)$ für alle $x \in \mathbb{C}$. $n \in \mathbb{N}$ ist hierbei frei wählbar. Setze

$n = 4$. Es reicht aus, Matrizen $A$ und $B$ mit verschiedenen Jordan-Normalformen anzugeben, in dem Sinne, dass die Jordankästchen in $A$ und $B$ nicht bis auf Reihenfolge übereinstimmen. Da die Jordan-Normalformen nicht übereinstimmen, liefert der Hauptsatz über die Jordan-Normalform, dass die Matrizen $A$ und $B$ nicht ähnlich sind. Sei $\lambda \in \mathbb{C}^\times = \mathbb{C} \setminus \{0_\mathbb{C}\}$ beliebig aber fest. Definiere die Matrizen $A$ und $B$ durch:

$$A = \begin{pmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & 0 & 0 \\ 0 & 0 & \lambda & 1 \\ 0 & 0 & 0 & \lambda \end{pmatrix}, \; B = \begin{pmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & 0 & 0 \\ 0 & 0 & \lambda & 0 \\ 0 & 0 & 0 & \lambda \end{pmatrix}. \tag{56}$$

Offenbar haben die Matrizen $A$ und $B$ eine im oben beschriebenen Sinne verschiedene Jordan-Normalform, sind also nicht ähnlich zueinander (Teil (i)). Die Forderung, $\lambda \in \mathbb{C}^\times$, stellt sicher, dass $\det A = \lambda^4 = \det B$ insbesondere von Null verschieden ist, die Matrizen $A$, $B$ also tatschlich also der Gruppe der invertierbaren $4 \times 4$-Matrizen mit Koeffizienten aus $\mathbb{C}$ stammen. Beide Matrizen liegen in Jordan-Normalform vor, und haben den Eigenwert $\lambda$ mit algebraischer Vielfachheit 4. Mithin gilt für die charakteristischen Polynome $\chi_A(x) = (x - \lambda)^4$ und $\chi_B(x) = (x - \lambda)^4$, insbesondere also $\chi_A = \chi_B$ (Teil (ii)). Sei nun $\mu_A, \mu_B \in \mathbb{C}[x]$ das Minimalpolynom von $A$ bzw. $B$. Laut Hauptsatz über das Minimalpolynom gilt, dass im Falle, dass die Matrix $A$ bzw. $B$ nur einen Eigenwert hat, dieser alleinige Nullstelle von $\mu_A$ bzw $\mu_B$ ist, wobei die Vielfachheit gerade die Länge des größten Jordankästchens zu diesem Eigenwert ist. Da $\lambda$ alleiniger Eigenwert von $A$ bzw. $B$ und das größte Jordan-Kästchen zu $\lambda$ für beide Matrizen Länge 2 hat, liefert der oben angeführte Hauptsatz zusammen mit der Normiertheitsforderung für die Minimalpolynom $\mu_A$, $\mu_B$ also $\mu_A(x) = (x - \lambda)^2$ und $\mu_B(x) = (x - \lambda)^2$, also insbesondere $\mu_A = \mu_B$ (Teil (iii)). Damit sind die beiden Matrizen $A$ und $B$ aus $\mathrm{GL}_n(\mathbb{C})$ mit den gewünschten Eigenschaften (i) bis (iii). □

**Aufgabe 21 (F15T2A4)** (a) Sei $\odot : G \times \Omega \to \Omega, (g, x) \mapsto g \odot x$ eine transititive Gruppenoperation der Gruppe $G$ auf die Menge $\Omega$ mit $|\Omega| > 1$ und der Eigenschaft, dass jedes $g \in G$ einen Fixpunkt besitzt, d.h., es gibt es $x \in \Omega$ zu vorgegebenem $g \in G$, so dass $g \odot x = x$. Zu zeigen ist, dass es ein $U < G$, d.h., eine echte Untergruppe $U$ von $G$ gibt, so dass

$$G = \bigcup_{h \in G} hUh^{-1}. \tag{57}$$

Sei $g' \in G$ beliebig aber nicht das Neutralelement, so dass $a \in \Omega$ Fixpunkt von $g'$. Dies ist möglich, da $G$ transitiv auf eine Menge der Mächtigkeit echt größer als 1 operiert. Bezeichne $G_\alpha = \{g \in G : g \odot \alpha = \alpha\}$ den Stabilisator von $\alpha$ in $G$. Aus der Vorlesung bekannt ist, dass $G_\alpha$ eine Untergruppe von $G$ ist. Da die Operation $\odot$ transitiv ist, gilt $G(\alpha) = \Omega$, also $|G(\alpha)| = |\Omega| > 1$, so dass gilt $G(\alpha) = (G : G_\alpha) > 1$, weswegen bereits $G_\alpha \subsetneq G$ gilt. Es bleibt zu zeigen, dass die angegebene Gleichung stimmt. Klar ist, dass $hUh^{-1} \subseteq G$ für beliebiges $h \in G$, also auch

$$G \supseteq \bigcup_{h \in G} hUh^{-1} \tag{58}$$

gilt. Um zu zeigen, dass auch $G$ in der Vereinigung von Konjugationsklassen enthalten ist, sei $g \in G$ beliebig vorgegeben. Nach Voraussetzung gibt es ein $\beta \in \Omega$, so dass $g \odot \beta = \beta$. Wegen der Transitivität von $\odot$ gibt es ein $k \in G$, so dass $k \odot \alpha = \beta$. Nun gilt $g \in kUk^{-1} \Leftrightarrow k^{-1}gk \in U \Leftrightarrow (k^{-1}gk) \odot \alpha = \alpha$. In der Tat, $k^{-1}(\odot(g \odot (k \odot \alpha))) = k^{-1} \odot (g \odot \beta) = k^{-1} \odot \beta = \alpha$ nach den Rechenregeln für Gruppenoperationen. Also gilt $g \in kUk^{-1}$ und erst recht $g \in \bigcup_{h \in G} hUh^{-1}$. Damit ist die Gleichheit von Mengen nachgewiesen. $\square$

(b) Sei nun $n > 1$ und gesucht ist eine echte Untergruppe von $G = \mathrm{GL}_n(\mathbb{C})$ mit der Eigenschaft, dass $G$ die Vereinigung aller Konjugationsklassen dieser Untergruppe ist. Wir definieren zunächst $\mathcal{U} = \{V \subset \mathbb{C}^n | U \text{ ist Untervektorraum von } \mathbb{C}^n, \dim_{\mathbb{C}} U = 1\}$. Da $n > 1$, sind bereits durch $\mathrm{lin}_{\mathbb{C}}(\hat{e}_1)$, $\mathrm{lin}_{\mathbb{C}}(\hat{e}_2)$ zwei Elemente aus $\mathcal{U}$ gegeben, also $|\mathcal{U}| > 1$. Ferner definieren wir die Abbildung $\odot : G \times \mathcal{U} \to \mathcal{U}$ durch $(A, U) \to A \odot U \equiv A(U)$. Zu überprüfen bleibt, dass hierdurch eine wohldefinierte, transitive Gruppenoperation zustandekommt, so dass zu jedem $A \in G$ ein $U \in \mathcal{U}$ mit $A \odot U = U$ existiert. Zur Wohldefiniertheit. Sei $U \in \mathcal{U}$ beliebig. Da $\dim_{\mathbb{C}} U = 1$, gibt es einen Vektor $v \in \mathbb{C}^n \setminus \{\mathbf{0}\}$, so dass $U = \mathrm{lin}_{\mathbb{C}}(v)$. Sei nun $A \in G$ auch beliebig. Da $A$ invertierbar, ist $Av \neq \mathbf{0}$. Ansonsten wäre $\ker A \neq \{\mathbf{0}\}$, im Widerspruch zur Injektivität des durch $A$ definierten Endomorphismus $\phi_A : \mathbb{C}^n \to \mathbb{C}^n, v \mapsto Av$. Also gibt es ein $w \in \mathbb{C}^n \setminus \{\mathbf{0}\}$ so dass $w = Av$. Es gilt also $w \in A \odot U$. Sei nun $\lambda \in \mathbb{C}$ beliebig, dann gilt $A(\lambda v) = \lambda Av = \lambda w \in A(U)$. Wegen $U = \mathrm{lin}_{\mathbb{C}}(v)$ folgt also sogar bereits $\mathrm{lin}_{\mathbb{C}}(w) = A(\mathrm{lin}_{\mathbb{C}}(v))$. Da $\dim_{\mathbb{C}} \mathrm{lin}_{\mathbb{C}}(w) = 1$, folgt $A(U) \in \mathcal{U}$ für beliebige $A \in G$, $U \in \mathcal{U}$. Mithin ist $\odot$ als Abbildung wohldefiniert. Zur Gruppenoperation: Es gilt für $U \in \mathcal{U}$ beliebig $I_n \odot U = I_n(U) = U$. Für $A, B \in G, U \in \mathcal{U}$ gilt $A \cdot B \in G$ und $A \odot (B \odot U) = A \odot (B(U)) = A(B(U)) = \{w \in \mathbb{C}^n : w = Av \text{ für ein } v \in B(U)\} = \{w \in \mathbb{C}^n : w = Av \text{ für ein } v \in \{w \in \mathbb{C}^n : v = Bu \text{ für ein } u \in U\}\} = \{w \in \mathbb{C}^n : w = (A \cdot B)v \text{ für ein } v \in U\} = (A \cdot B)(U)$. Zur Transitivität: Für den Nachweis der Transitvität reicht es zu zeigen, dass für ein $U \in \mathcal{U}$ gilt $G(U) = \mathcal{U}$. Andernfalls entsteht ein Widerspruch dazu, dass die Bahnen der Operation einer Zerlegung von $\mathcal{U}$ bilden. Sei $V \in \mathcal{U}$ beliebig und setze $U = \mathrm{lin}_{\mathbb{C}}(\hat{e}_1)$. Da $\dim_{\mathbb{C}} V = 1$, gibt es ein $v = v_1 \in \mathbb{C}^n \setminus \{\mathbf{0}\}$, so dass $V = \mathrm{lin}_{\mathbb{C}}(v_1)$. Da $v_1$ Nicht-Nullvektor ist, gibt es nach dem Basisergänzungssatz Vektoren $v_2, ..., v_n \in \mathbb{C}^n \setminus \{\mathbf{0}\}$, so dass $\{v_1, ..., v_n\}$ eine $n$-elementige Menge linear unabhängiger Vektoren in $\mathbb{C}^n$ ist, also eine Basis von $\mathbb{C}^n$. Insbesondere gilt nach einer bekannten Charakterisierung invertierbarer $n \times n$-Matrizen, dass $A = (v_1, ..., v_n)$, bestehend aus den soeben gefundenen Vektoren, in $G$ liegt. Mithin gilt nach Definition der Bahn $G(U) \ni V$. Beliebigkeit von $V \in \mathcal{U}$ impliziert nun zusammen mit der Definition des Bildbereichs der Gruppenopration $\mathcal{U} = G(U)$. Zusammen mit der eingangs gemachten Bemerkung ist das zuletzt genannte Ergebnis gerade die Transitivität der Gruppenoperation $\odot$. Es bleibt zu zeigen, dass es zu fest vorgegebenem $A \in G$ einen Fixpunkt $U \in \mathcal{U}$ der Operation $\odot$ gibt. Sei $A \in G$ also beliebig und bezeichne mit $\chi_A \in \mathbb{C}[x]$ das charaketristische Polynom von $A$. Da $\mathbb{C}$ algebraisch abgeschlossen ist, ist $\mathbb{C}$ Zerfällungskörper von $\chi_A$. Da $A \in G$, also invertierbare $n \times n$-Matrix ist, sind die Eigenwerte von $A$, d.h., die Nullstellen des charakteristischen Polynoms $\chi_A$, alle von $0_{\mathbb{C}}$ verschieden. Ansonsten entsteht ein Widerspruch zur zur Invertierbarkeit äquivalenten Bedingung $\det A \neq 0$. Sei also $\lambda \in \mathbb{C}^{\times}$ Eigenwert von $A$. Dann gilt $Av = \lambda v$ für ein $v \in \mathbb{C}^n \setminus \{0\}$, da die geometrische Vielfachheit eines Eigenwertes stets größer als 1

ist. Da $v \in \mathbb{C}^n \setminus \{\mathbf{0}\}$ ist $\dim_{\mathbb{C}} \mathrm{lin}_{\mathbb{C}}(v) = 1$, also $U \equiv \mathrm{lin}_{\mathbb{C}}(v) \in \mathcal{U}$. Da mit $v \in U$ auch $\lambda^{-1}v \in U$ folgt $A(\lambda^{-1}v) = \lambda\lambda^{-1}v = v \in A \odot U$, so dass $\mathrm{lin}_{\mathbb{C}}(v) \subseteq A \odot U$ und aus Dimensionsgründen $\mathrm{lin}_{\mathbb{C}}(v) = A \odot U$. Also hat $A$ einen Fixpunkt und die Beliebigkeit von $A$ liefert, dass jedes $A \in G$ einen Fixpunkt im obenstehenden Sinne hat. Im Ergebnis liegen alle Voraussetzungen vor, Teil (a) anzuwenden. Dieser liefert die Existenz einer echten Untergruppe $U$ von $G$, so dass $G$ die Vereinigung aller Konjugationsklassen von $U$ in $G$ ist. □

(c) Definiere nun $\bullet : G \times (\mathcal{U} \times \mathcal{U}) \to \mathcal{U} \times \mathcal{U}, (A, (U, V)) \mapsto (A(U), A(V))$. Zu unterstellen ist, dass $\bullet$ eine Gruppenoperation ist. Zu zeigen ist, dass es genau zwei Bahnen gibt. Aus der Vorlesung ist bekannt, dass die Bahnen einen Gruppenoperation eine Zerlegung der Menge ist, auf die die Gruppe operiert. Sei nun $U \in \mathcal{U}$ beliebig. Dann ist $G((U,U)) = \{(V,V) \in \mathcal{U} \times \mathcal{U} | \exists A \in G : V = A(U)\}$. Ferner gilt $\mathcal{U} \times \mathcal{U} \setminus G((U,U)) = \{(V_1, V_2) \in \mathcal{U} \times \mathcal{U} | V_1 \neq V_2\} = \{(V_1, V_2) \in \mathcal{U} \times \mathcal{U} | V_1 \cap V_2 = \{\mathbf{0}\}\}$, wobei für das Gleichheitszeichen verwendet wurde, dass zwei ein-dimensionale Untervektorräume eines Vektorraums $\mathbb{C}^n$ entweder gleich sind oder aber trivialen Schnitt haben. Wir behaupten nun, dass $G(\mathrm{lin}_{\mathbb{C}}(\hat{e}_1), \mathrm{lin}_{\mathbb{C}}(\hat{e}_2)) = \mathcal{U} \times \mathcal{U} \setminus G((U,U)). \subseteq$. Sei $A \in G$ beliebig aber fest. Angenommen, $A \bullet (\mathrm{lin}_{\mathbb{C}}(\hat{e}_1), \mathrm{lin}_{\mathbb{C}}(\hat{e}_2)) \notin \mathcal{U} \times \mathcal{U} \setminus G((U,U))$. Dann gibt es ein $W \in \mathcal{U}$, so dass $A(\mathrm{lin}_{\mathbb{C}}(\hat{e}_1)) = W \,\&\, A(\mathrm{lin}_{\mathbb{C}}(\hat{e}_2)) = W$. Insbesondere gibt es dann Vektoren $w_1, w_2 \in W \setminus \{\mathbf{0}\}$, also insbesondere linear abhängig, so dass $w_1 = A\hat{e}_1$, $w_2 = A\hat{e}_2$. Die lineare Abhängigkeit von $w_1$ und $w_2$ liefert $(\lambda_1, \lambda_2) \in \mathbb{C} \times \mathbb{C} \setminus \{(0_{\mathbb{C}}, 0_{\mathbb{C}})\}$, so dass $\mathbf{0} = \lambda_1 v_1 + \lambda_2 w_2$, also $\mathbf{0} = \lambda_1(A\hat{e}_1) + \lambda_2(A\hat{e}_2) = A(\lambda_1\hat{e}_1 + \lambda_2\hat{e}_2)$ mit $\lambda_1\hat{e}_1 + \lambda_2\hat{e}_2 \neq \mathbf{0}$, im Widerspruch zur aus der Invertierbarkeit von $A$ folgenden Bedingung $\ker A = \{\mathbf{0}\}$. Also gilt $G(\mathrm{lin}_{\mathbb{C}}(\hat{e}_1), \mathrm{lin}_{\mathbb{C}}(\hat{e}_2)) \subseteq \mathcal{U} \times \mathcal{U} \setminus G((U,U))$. $\supseteq$: Sei nun umgekehert $(V_1, V_2) \in \mathcal{U} \times \mathcal{U} \setminus G((U,U))$ gegeben. Zu zeigen ist $(V_1, V_2) \in G(\mathrm{lin}_{\mathbb{C}}(\hat{e}_1), \mathrm{lin}_{\mathbb{C}}(\hat{e}_2))$, also die Existenz eines $A \in G$, so dass $A(\mathrm{lin}_{\mathbb{C}}(\hat{e}_1), \mathrm{lin}_{\mathbb{C}}(\hat{e}_2)) = (V_1, V_2)$. Da $V_1, V_2 \in \mathcal{U}$ gibt es $v_1, v_2 \in \mathbb{C}^n \setminus \{\mathbf{0}\}$, so dass $V_i = \mathrm{lin}_{\mathbb{C}}(v_i)$ für alle $i \in \{1,2\}$. Ferner sind $v_1, v_2$ nach Voraussetzung an $V_1, V_2$, $V_1 \cap V_2 = \{\mathbf{0}\}$, linear unabhängig. Nach dem Basisergänzungssatz finden wir also $(n-2)$ geeignete, paarweise linear unabhängige Vektoren $v_3, ....v_n \in \mathbb{C}^n \setminus \{\mathbf{0}\}$, so dass $\{v_1, v_2, v_3, ..., v_n\}$ $n$-elementige Menge paarweise linear unabhängiger Vektoren in $\mathbb{C}^n$ ist. Da $n < \infty$, bilden sie einen Basis von $\mathbb{C}^n$. Setze nun $A = (v_1, v_2, v_3, ..., v_n)$. Es gilt $A \in G$, denn nach einer bekannten Charakterisierung invertierbarer $n \times n$ Matrizen, ist die Invertiebarkeit äquivalent dazu, dass die Spalten der Matrix $n$ linear unabhängige Vektoren sind. Dann gilt $A(\mathrm{lin}_{\mathbb{C}}(\hat{e}_i)) = \mathrm{lin}_{\mathbb{C}}(v_i) = V_i$ für alle $i \in \{1,2\}$, also $(V_1, V_2) \in G((\mathrm{lin}_{\mathbb{C}}(\hat{e}_2), \mathrm{lin}_{\mathbb{C}}(\hat{e}_2)))$. Beliebigkeit des Paares $(V_1, V_2)$ liefert nun $G(\mathrm{lin}_{\mathbb{C}}(\hat{e}_1), \mathrm{lin}_{\mathbb{C}}(\hat{e}_2)) \supseteq \mathcal{U} \times \mathcal{U} \setminus G((U,U))$. Zusammen mit dem ersten Teil folgt Gleichheit von Mengen. Infolge der Bemerkungen am Anfang des Beweises zur Zerlegungseigenschaft der Bahnen, folgt nun, dass wir zwei Bahnen gefunden haben, die eine Zerlegung von $\mathcal{U} \times \mathcal{U}$ bilden. Da jede Bahn mindestens ein Element beinhaltet, haben wir somit alle Bahnen der Operation $\bullet$ bestimmt – deren Anzahl ist also genau 2. □

**Aufgabe 22 (H14T2A5)** Laut Hauptsatz über die Jordan-Normalform gibt die geometrische Vielfachheit des Eigenwerts $\lambda = 1$ der (speziell hier) Matrix $A = I_6 + N$ mit einer nilpotenten Matrix $N$ mit Nilpotenzindex 3 an, wie viele Jordan-Kästchen es gibt. Die Jordan-Normalform von $A$ besteht also aus 3 Jordan-Kästchen, so dass

die Längen der drei Jordan-Kästchen sich zu 6 addieren. Da $\lambda = 1$ die Vielfachheit 6 hat, ist $\lambda = 1$ auch der einzige Eigenwert der Matrix $A \in \mathrm{M}_6(\mathbb{R})$. Nach dem Hauptsatz über das Minimalpolynom der Matrix $A$ ist also die Vielfachheit der Nullstelle $\lambda = 1$ des Minimalpolynoms gerade der Nilpotenzindex der Matrix $A - \lambda I_6 = A - I_6 = N$. Es gilt $A - I_6 = N$, $(A - I_6)^2 = N^2 \neq 0$ nach Aufgabenstellung, aber $(A - I_6)^3 = N^3 = 0$. Also hat auch $A$ Nilpotenzindex 3. Für das Minimalpolynom $\mu_A$ von $A$ gilt also, dass es die drei-fache Nullstelle 1 hat. Nach einem Zusatz zum Hauptsatz über die Jordan-Normalform ist die Vielfachheit einer Nullstelle $\mu$ des Minimalpolynoms $\mu_A$ gerade die Größe des größten Jordan-Kästchens zum Eigenwert $\mu$ von $A$. Da hier $\lambda = \mu = 1$ einziger Eigenwert, ist das größte Jordan-Kästchen in der Jordan-Normalform von $A$ ein 3-er Jordan-Kästchen. Wir bezeichnen dieses mit $J_1$. Da die Matrix insgesamt 3 Jordan-Kästchen besitzt, verbleiben zwei Jordankästchen $J_2, J_3$ der Länge $l_2, l_3$ respektive. Da für die Summe der Längen aller Jordan-Kästchen gilt $3+l_2+l_3 = 6 \Leftrightarrow l_2+l_3 = 3$, ist entweder $l_2 = 2$ und $l_3 = 1$ oder $l_2 = 1$ und $l_3 = 2$ möglich. Da nach einem Satz über die Eindeutigkeit der Jordan'schen Normalform, diese nur bis auf Reihenfolge der Jordan-Blöcke festgelegt ist, wählen wir ohne Beschränkung der Allgemeinheit $l_2 = 2$, $l_3 = 1$. Zusammen mit der Voraussetzung, dass der Eigenwert $\lambda = 1$ ist, haben wir für die Jordan-Normalform $J[A]$ von $A$:

$$J[A] = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \tag{59}$$

bis auf Reihenfolge der Jordan-Kästchen. □

**Aufgabe 23 (F18T3A1(b))** Sei $\psi : \mathbb{F}_5^3 \to \mathbb{F}_5^2$ surjektive und lineare Abbildung. Zu bestimmen ist $|\ker\psi|$. Da $\psi$ surjektiv ist, und $\mathbb{F}_5^k$ für $k\{2,3\}$ ein $\mathbb{F}_5$-Vektorraum über dem endlichen Körper $\mathbb{F}_5$ ist, liefert der Kern-Bild-Satz für lineare Abbildungen: $\dim\mathrm{im}\psi + \dim\ker\psi = 3$. Da $\psi$ surjektiv ist, $\dim\mathrm{im}\psi = \dim\mathbb{F}_5^2 = 2$, so dass $\dim\ker\psi = 1$, also $\ker\psi \simeq \mathbb{F}_5$ vermöge eines Vektorraum-Isomorphismus. Da dieser eine Bijektion zwischen zwei endlichen Mengen ist, folgt $|\ker\psi| = |\mathbb{F}_5| = 5$. □

**Aufgabe 24 (F18T2A1(d)** Seien $P_1, P_2, ..., P_5 \in \mathbb{R}^2$ von der Form $P_j = (x_j, y_j)$ für $j \in \{1,2,3,4,5\}$. Zu zeigen ist, dass es $(a,b,c,d,e,f) \in \mathbb{R}^6 \setminus \{\mathbf{0}_{\mathbb{R}^6}\}$ gibt, so dass $ax_j^2 + bx_jy_j + cy_j^2 + dx_j + ey_j + f = 0$ für alle $j \in \{1,2,3,4,5\}$. Es gibt $\mathbb{R}^6 \ni (a,b,c,d,e,f) \neq (0,0,0,0,0,0)$ genau dann wenn das lineare Gleichungssystem definiert durch $0 = A_{ij}z_j$ mit $z = \sum_{j=1}^6 z_j\hat{e}_j = (a,b,c,d,e,f)$ und $A = (A_{ij})_{1\leq i\leq 5, 1\leq j\leq 6}$ gegeben durch $A_{i1} = x_i^2$, $A_{i2} = x_iy_i$, $A_{i3} = y_i^2$, $A_{i4} = x_i$, $A_{i5} = y_i$ und $A_{i6} = 1$ eine nicht-triviale Lösung, d.h., einem vom Null-Vektor verschiedene Lösung, hat. Sei $r \equiv \mathrm{rang}(A)$ der Rang der $5 \times 6$-Matrix $A$ über $\mathbb{R}$. Laut Vorlesung ist der Lösungsraum $\mathcal{L} = \{z \in \mathbb{R}^6 : 0_{\mathbb{R}^5} = A \cdot z\}$ des betrachteten linearen Gleichungssystems ein Untervektorraum von $\mathbb{R}^5$ und genauer gilt für die Dimension $\dim\mathcal{L} = \dim_{\mathbb{R}^6} - r$. Als $5 \times 6$-Matrix, kann $A$ maximal Spaltenrang 6 und maximal

Zeilenrang 5 haben, nach der Gleichheit von Zeilen- und Spaltenrang also maximal Rang 5, $0 \leq r \leq 5$. Damit gilt $6 \leq \dim_{\mathbb{R}} \mathcal{L} \geq 1$ und insbesondere gibt es ein nichtverschwindendes $z_0 \in \mathbb{R}^6$, so dass $\mathrm{lin}_{\mathbb{R}} \subseteq \mathcal{L}$. Die Komponenten dieses $z$ erfüllen die Eigenschaften des gesuchten $(a, b, c, d, e, f) \in \mathbb{R}^6 \setminus \{0_{\mathbb{R}^6}\}$. Damit ist gezeigt, dass mindestens ein vom Nullvektor verschiedenes 6-Tupel $(a, b, c, d, e, f) \in \mathbb{R}^6$ mit den gewünschten Eigenschaften existiert. □

**Aufgabe 25** Sei $G$ eine endliche Gruppe, $p$ eine Primzahl, $P$ eine $p$-Sylowgruppe von $G$. Zu zeigen ist $N_G(P) = N_G(N_G(P))$. Sei also $p$ Primzahl und $P$ eine, nicht notwendigerweise die einzige $p$-Sylowgruppe von $G$. Nach Definition ist der Normalisator $N_G(P)$ von $P$ in $G$ die maximale Untergruppe von $G$, die $P$ enthält und in der $P$ ein Normalteiler ist, $N_G(P) \equiv \{g \in G : gPg^{-1} \subseteq P\}$. Wir zeigen zuerst $N_G(P) \subseteq N_G(N_G(P))$. Da $P$ als Gruppe abgeschlossen ist, gilt $P \subseteq N_G(P)$. Da stets $gN_G(P)g^{-1} \subseteq N_G(P)$ für alle $g \in N_G(P)$, folgt automatisch $N_G(P) \subseteq N_G(N_G(P))$. Damit ist die Inklusion $\subseteq$ nachgewiesen. Wir zeigen nun $N_G(N_G(P)) \subseteq N_G(P)$. Zunächst gilt, dass $P \trianglelefteq N_G(P)$ nach Definition des Normalisators, s.o.. Da $N_G(P) \leq G$ und $P$ als $p$-Sylowgruppe insbesondere Untergruppe von $G$ ist, liefert die Inklusion $P \subseteq N_G(P)$ bereits, dass $P$ ebenfalls eine Untergruppe von maximaler $p$-Potenzordnung, also $p$-Sylowgruppe von $N_G(P)$ ist. Da $P \trianglelefteq N_G(P)$, liefert die Folgerung aus dem zweiten Sylowsatz, dass $P$ die einzige $P$-Sylowgruppe von $N_G(P)$ ist. Sei nun $g \in N_G(N_G(P))$ vorgegeben. Dann gilt $gN_G(P)g^{-1} \subseteq N_G(P)$. Sei nun weiter $h \in N_G(P)$ vorgegeben. Dann gilt $ghg^{-1} \in N_G(P)$, also $(ghg^{-1})P(ghg^{-1})^{-1} \subseteq P \Leftrightarrow h(g^{-1}Pg)h^{-1} \in g^{-1}Pg$. Laut dem zweiten Sylowsatz sind je zwei $p$-Sylowgruppen der Gruppe $G$ zueinander konjugiert. Damit ist $Q \equiv g^{-1}Pg$ eine $p$-Sylowgruppe von $G$ und es gilt $h \in N_G(Q = g^{-1}Pg)$. Da $h \in N_G(P)$ beliebig war, folgt $N_G(P) \subseteq N_G(Q)$. Wir oben stellen wir fest, dass $Q \trianglelefteq N_G(Q)$. Ebenso wie $P$ ist auch $Q$ $p$-Sylowuntergruppe von $N_G(Q)$, für $P$ ergibt sich dies daraus, dass $P$ dieselbe maximale $p$-Potenzordnung wie $Q$ hat. Wäre nun $Q \neq P$, dann hätte $N_G(Q)$ zwei verschiedene $p$-Sylowgruppen. Laut Folgerungen aus zweitem Sylowsatz ist aber $Q \trianglelefteq N_G(Q)$ äquivalent dazu, dass es genau eine $p$-Sylowgruppe in $N_G(Q)$ gibt. Das widerspricht der Annahme, $P \neq Q$. Damit ist also $P = Q = g^{-1}Pg \Leftrightarrow gPg^{-1} = P$. Das ist aber äquivalent dazu, dass $g \in N_G(P)$, denn $N_G(P) \leq G$ ist per Definition die größte Untergruppe von $G$ in der $P$ Normalteiler ist. □

**Aufgabe 26 (F11T2A3)** Sei $V = \mathbb{F}_2^2$ und definiere $G = \{v \mapsto Av + b | A \in \mathrm{GL}_2(\mathbb{F}_2), b \in V\}$. Als bereits bewiesen ist zu unterstellen, dass $G$ eine Gruppe ist, die sogenannte Gruppe der affinen Abbildungen von $V$. Wir geben zunächst alle Elemente aus $GL_2(\mathbb{F}_2)$ an. Dies ist die Gruppe der invertierbaren $2 \times 2$-Matrizen mit Einträgen aus dem Körper $\mathbb{F}_2$, so dass die Determinante $\det A \neq 0$ für eine beliebige Matrix $A \in GL_2(\mathbb{F}_2)$. Es gilt für $A \in M_{2\times 2}(\mathbb{F}_2)$

$$A = \begin{pmatrix} c_1 & c_2 \\ c_4 & c_3 \end{pmatrix}, \tag{60}$$

wobei $c_1, c_2, c_3, c_4 \in \mathbb{F}_2$ beliebig. Da $\det : M_{2\times 2}(\mathbb{F}_2) \to \mathbb{F}_2$ und $1 \in \mathbb{F}_2$ das einzige Element in der Einheitengruppe von $\mathbb{F}_2$ ist, muss $\det A = 1$ gelten, damit $A \in$

$\mathrm{GL}_2(\mathbb{F}_2)$. Bekannt aus der Vorlesung ist, dass für die Determinante einer $2 \times 2$-Matrix gilt: $\det A = c_1c_3 - c_1c_2$, wobei hier in $\mathbb{F}_2$ zu rechnen ist. Es gilt also $\det A \neq 0$ genau dann wenn $c_1c_3 \neq c_1c_4$ in $\mathbb{F}_2$. Das gilt für $c_1c_3 \neq 0$, .h., $c_1 = 1 = c_3$ wenn $c_2c_4 = 0$, also $c_2 = 0, c_4 = 1$ oder $c_2 = 1, c_4 = 0$ oder $c_2 = 0, c_4 = 0$. Für $c_2c_4 \neq 0$, also $c_2 = 1 = c_4$ ergibt sich $c_1c_3 = 0$, also $c_1 = 0 = c_3$ oder $c_1 = 0, c_3 = 1$ oder $c_1 = 1, c_3 = 0$. Damit haben wir alle Möglichkeiten durchgetestet, denn sonst wäre $c_1c_3 \neq 0$ und $c_2c_4 \neq 0$, also $c_1c_3 = 1 = c_2c_4$ und somit $\det A = c_1c_3 - c_2c_4 = 1 - 1 = 0$ oder $c_1c_3 = 0$ und $c_2c_4 = 0$ und somit ebenfalls $\det A = c_1c_3 - c_2c_4 = 0 - 0 = 0$, d.h., $A \notin \mathrm{GL}_2(\mathbb{F}_2)$. Es folgt:

$$\mathrm{GL}_2(\mathbb{F}_2) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right. \tag{61}$$

$$\left. \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \right\}. \tag{62}$$

Insbesondere gilt $|\mathrm{GL}_2(\mathbb{F}_2)| = 6$. Nun zeigen wir, dass $G \simeq S_4$. Definiere dazu die Abbildung $\odot : G \times V \to V, ((A, b), v) \mapsto Av + b =: (A, b) \odot v$, wobei wir ein gegebenes Element aus $G$ durch das Tupel $(A, b)$ mit $A$ in $\mathrm{GL}_2(\mathbb{F}_2)$ und $b \in V$ angeben. Wohldefiniertheit ist klar, denn für beliebiges $(A, b) \in G, v \in V$ gilt $(A, b) \odot v = Av + b$, was wegen der $\mathbb{F}_2$-Vektorraumeigenschaft von $V = \mathbb{F}_2^2$ und $A \in \mathrm{GL}_2(\mathbb{F}_2)$ wiederum in $V$ liegt. Wir zeigen, dass $\odot : G \times V \to V$ wie angegeben eine Gruppenoperation ist. Das Neutralelement in $G$ ist offenbar $(I_2, 0)$. Es gilt $(I_2, 0) \odot v = I_2v + 0 = v$ für beliebiges $v \in V$. Ferner gilt für $(A, b), (A', b') \in G$ $(A, b) \odot ((A', b') \odot v) = (A, b) \odot (A'v + b') = A(A'v + b') + b = AA'v + (Ab' + b) = ((A, b) \cdot (A', b')) \odot v$, das heißt die Abbildung $\odot$ ist mit der Komposition affiner Abbildungen als Verknüpfung auf $G$ verträglich. Laut Vorlesung definiert eine Gruppenoperation $\odot : G \times V \to V$ einen Gruppenhomomorphismus $\Phi : G \to \mathrm{Per}(V)$, wobei $\mathrm{Per}(V)$ die Gruppe der bijektiven Abbildung von $V$ nach $V$ bezeichnet. Da $|V| = |\mathbb{F}_2|^2 = 2^2 = 4$, gilt $\mathrm{Per}(V) \simeq S_4$, wobei $S_4$ die Symmetrische Gruppe der Ordnung 4 bezeichnet. Wir müssen zeigen, dass $\Phi$ sogar ein Isomorphismus von Gruppen ist, also bijektiv. Wir zeigen zuerst, dass $\Phi$ injektiv ist. Das Neutralelement in $\mathrm{Per}(V)$ ist die Identität. Es gilt $\ker \Phi = \{(A, b) \in G : (A, b) \odot v = v\}$, also gilt für $(A, b) \in \ker \Phi$, dass $Av + b = v$ für alle $v \in V$. Durch Inspektion der Elemente aus $\mathrm{GL}_2(\mathbb{F}_2)$ aus Teil (a) stellt man fest, dass die vorher genannte Gleichung nur für $A = I_2, b = 0$ erfüllt wird. Damit folgt $g \in \{(I_2, 0)\}$ und $\ker \Phi \subseteq \{(I_2, 0)\}$. Die umgekehrte Inklusion ist trivial nach Definition eines Gruppenhomomorphismus, so dass $\ker \Phi = \{(I_2, 0)\}$. Laut Vorlesung folgt daraus, dass $\Phi$ injektiv ist. Zum Nachweis der Surjektivität sei $\psi \in \mathrm{Per}(V)$ vorgegeben. Wir behaupten, dass $(A = (\psi(e_1) - \psi(0), \psi(e_2) - \psi(0)), b = \psi(0)) \in G$ durch $\Phi$ auf $\psi$ abgebildet wird, wobei $e_1 = (1, 0)^T$ und $e_2 = (0, 1)^T$ und 0 der Nullvektor ist. Das angegebene Element ist in der Tat in $G$, denn $\psi(0) \in V$ ist wegen $\psi \in \mathrm{Per}(V)$ klar, die lineare Unabhängigkeit von $(\psi(e_1) - \psi(0))$ und $(\psi(e_1) - \psi(0))$ In der Tat gilt mit dem soeben definierten $(A, b)$ für beliebiges $v = 0$, dass $(A, b) \odot v = (A0 + \psi(0)) = \psi(0)$, für $v = e_1$, dass $(A, b) \odot v = (\psi(e_1) - \psi(0)) + \psi(0) = \psi(1)$, für $v = e_2$, dass $(A, b) \odot v = (\psi(e_2) - \psi(0)) + \psi(0) = \psi(e_2)$ und somit $(A, b) \odot v = \psi(e_1 + e_2)$, da $(A, b) \odot v$ nicht aus $\{\psi(0), \psi(e_1), \psi(e_2)\}$ und $\psi$ bijektiv. Damit ist $\Phi$ bijektiv, also ein Isomorphismus und es folgt $G \simeq S_4$. Nun müssen wir zeigen, dass $\mathrm{GL}_2(\mathbb{F}_2) \simeq S_3$. Durch Einschränkung der Operation $\odot$ auf $G \geq U := \mathrm{GL}_2(\mathbb{F}_2) \times \{0\} \simeq \mathrm{GL}_2(\mathbb{F}_2)$,

erhalten wir eine Operation $\odot|_U : U \times V \to V, v \mapsto Av + b = Av = (A,0) \odot_U v$. Wir stellen fest, dass $0 \in V$ Fixpunkt der Operation ist, denn für alle $A \in \mathrm{GL}_2(\mathbb{F}_2)$ gilt $A0 = 0$. Damit gilt für die Einschränkung des obigen Gruppenisomorphismus $\Phi|_U : U \to W \leq S_4$, wobei $W$ eine Untergruppe der $S_4$ ist, deren Elemente selbst einen Fixpunkt besitzen, d.h., es gibt es ein $m \in \{1,2,3,4\}$, so dass $\tau(m) = m$ für alle $\tau \in W$. Bezeichnet 0 das zu $m$ gehörige Element,so gilt andernfalls $0 = (A,0)(0) = \psi(0) \neq 0$ für $\psi = \Phi((A,0))$ zu beliebigem $A \in U$, also ein Widerspruch. Als Untergruppe der $S_4$, die einen Fixpunkt besitzt, ist $W \simeq S_3$ und somit vermöge $\Phi_U$: $U \simeq W \simeq S_3$,also $\mathrm{GL}_2(\mathbb{F}_2) \simeq S_3$ wie behauptet. Besser ist vermutlich zu Fuß: Wir definieren $\bullet : U \times W \to W$, wobei $U = \mathrm{GL}_2(\mathbb{F}_2)$ und $W = \mathbb{F}_2^2 \setminus \{0\}$. Diese Abbildung ist wohldefiniert, denn $Av = 0 \Leftrightarrow v = 0$, da $A \in \mathrm{GL}_2(\mathbb{F}_2)$, also $Av \neq 0$ für $v \neq 0$. Wiederum ist $\bullet$ Gruppenoperation, diesmal von $U$ auf $W$, denn für das Neutralelement $I_2 \in U$ gilt: $\bullet(I_2, v) = I_2 v = v$ für alle $v \in W$. Ferner gilt für $A, B \in U$ beliebig $A\bullet(B\bullet v) = A\bullet(Bv) = A(Bv) = (AB)v = (AB)\bullet v$ für alle $v \in W$. Laut Vorlesung gibt es damit einen Gruppenhomomorphismus $\phi : U \to \mathrm{Per}(W)$. Wegen $|W| = 3$ folgt $\mathrm{Per}(W) \simeq S_3$. Wir zeigen nun noch, dass $\phi$ bijektiv ist, also ein Isomorphismus von Gruppen ist. Zur Injektivität: $A \in \ker\phi \Leftrightarrow A \bullet v = \mathrm{id}_W(v) = v \Leftrightarrow A = I_2$, da $\mathrm{id}_W$ das Neutralelement in $\mathrm{Per}(W)$ ist. Zur Surjektivität: Wir bemerken, dass durch $v_1 \mapsto \psi(v_1)$ und $v_2 \mapsto \psi(v_2)$ für zwei verschiedene Elemente $v_1, v_2 \in W$ bereits das Bild des verbleibenden Dritten $v_3 \notin \{v_1, v_2\}$ festgelegt ist, denn $\psi \in \mathrm{Per}(W)$ ist bijektiv. Es gilt $\psi(v_3) \in W \setminus \{\psi(v_1), \psi(v_2)\}$, wobei letzteres eine einelementige Menge ist. Da $e_1 = (1,0)^T \neq (0,1)^T = e_2$ verschiedene Elemente aus $w$ sind, sei zu beliebigem $\psi \in \mathrm{Per}(w)$ $A = (\psi(e_1), \psi(e_2))$. Wir behaupten: $\Phi(A) = \psi$. Sei nämlich $v \in W$, dann gilt $A \bullet e_1 = Ae_1 = \psi(e_1)$, $A \bullet e_2 = Ae_2 = \psi(e_2)$ nach Definition von $A$ und $A \bullet (e_1 + e_2) = A(e_1 + e_2) = Ae_1 + Ae_2 = \psi(e_1) + \psi(e_2) \notin \{\psi(e_1), \psi(e_2)\}$, also $A \bullet (e_1 + e_2) = \psi(e_1 + e_2)$ wegen obenstehender Ausführungen. Damit folgt $A \bullet v = \psi(v)$ für alle $v \in W$, d.h., $\phi(A) = \psi$. Damit ist $\phi$ auch surjektiv. Alternativ bemerkt man, dass $|U| = 6 = |\mathrm{Per}(W)|$, und $|\phi(U)| = 6$ da $\phi$ injektiver Gruppenhomomorphismus. Da $\mathrm{Per}(W)$ die einzige Untergruppe von $\mathrm{Per}(W)$ mit genau 6 Elementen ist, folgt $\phi(U) = \mathrm{Per}(W)$ also die Surjektivität. Insgesamt ist $\phi$ somit bijektiv, also $U \simeq \mathrm{Per}(W) \simeq S_3$, wie behauptet. □

**Aufgabe 27 (H13T2A1)** Sei $G$ Gruppe der Ordnung $750 = 2 \cdot 3 \cdot 5^3$ und sei $\mathrm{Syl}_5$ die Menge der 5-Sylowgruppen von $G$, $n_5 \equiv |\mathrm{Syl}_5|$. (a) Es gilt nach dem dritten Sylow-Satz: $n_5 | 2 \cdot 3$, also $n_5 \in \{1,2,3,6\}$ und $n_5 \equiv 1 \bmod(5)$. Also gilt wegen $2 \not\equiv 1 \bmod(5)$ und $3 \not\equiv 1 \bmod(5)$ sogar $n_5 \in \{1,6\}$. (b) Falls nun $n_5 = 1$ und $P$ die einzige 5-Sylowgruppe von $G$ bezeichnet, dann ist nach einer Folgerung aus dem zweiten Sylow-Satz $P \trianglelefteq G$. Da $|\{e_G\}| = 1 < |P| = 5^3 = 125 < 750 = |G|$, also $\{e_G\} \subsetneq P \subsetneq G$. Damit ist $P$ ein nicht-trivialer Normalteiler, $G$ also nicht einfach. (c) Definiere nun $\odot : G \times \mathrm{Syl}_5 \to \mathrm{Syl}_5, (g,P) \to gPg^{-1}$. Wir sollen zeigen, dass $\odot$ eine Gruppenoperation und transitiv ist. Aus der Vorlesung ist bereits bekannt, dass die Gruppe $G$ von Ordnung $p^r m$ mit $p \not| m$ wie angegeben auf die Menge ihrer $p$-Sylowgruppen operiert. Für die konkrete Gruppenordnung liefert das Resultat, dass $\odot$ eine Gruppenoperation von $G$ der Ordnung 750 auf die Menge ihrer 5-Sylowgruppen darstellt. Wir zeigen noch, dass $\odot$ transitiv ist. Sei dazu $P \in \mathrm{Syl}_5$ beliebig. Wir müssen zeigen, $G(P) = \mathrm{Syl}_5$. Sei nun ein be-

liebiges $Q \in \mathrm{Syl}_5$ weiter vorgegeben. Nach dem zweiten Sylowschen Satz sind je zwei $p$-Sylowgruppen, also 5-Sylowgruppen in unserem Beispiel, zueinander konjugiert. Es gibt also hier ein $g \in G$, so dass $Q = gPg^{-1}$. das bedeutet $Q \in G(P)$. Da $Q$ beliebig ist, folgt $\mathrm{Syl}_5 \subseteq G(P)$. Die Inklusion $G(P) \subseteq \mathrm{Syl}_5$ ist klar nach Definition der Bahn des Elementes$P$ unter der Gruppenoperation $\odot$. Insgesamt also $G(P) = \mathrm{Syl}_5$. Mithin ist $\odot$ einer transitive Gruppenoperation. (d) Wir nehmen nun an, dass $n_5 = 6 > 1$. Zu zeigen ist, dass $G$ nicht einfach ist. Wenn wir also einen nicht-trivialen Normalteiler von $G$ gefunden haben sind wir fertig. Nach dem Satz über den Zusammenhang von Gruppenoperationen und Gruppenhomomorphismen definiert $\odot$ einen Gruppenhomomorphismus $\Phi : G \to \mathrm{Per}(\mathrm{Syl}_5)$. Nach Voraussetzung $n_5 = 6$ gilt $\mathrm{Per}(\mathrm{Syl}_5) \simeq S_6$. Im Falle $\ker\Phi \notin \{\{e_G\}, G\}$ sind wir fertig, da $\ker\Phi \triangleleft G$ nichttrivialer Normalteiler von $G$ ist, $G$ also nicht einfach ist. Sei zunächst also $\ker\Phi = \{e_G\}$. Das heißt, $\Phi$ ist injektiv. Wegen $|G| = 750$ aber $|\mathrm{Per}(\mathrm{Syl}_5)| = |S_6| = 6! = 720 < 750$ haben wir einen Widerspruch, denn $|\Phi(G)|||S_6|$ nach Lagrange. Sei nun $\ker\Phi = G$. Dann gilt $\Phi(G) = \{\mathrm{id}_{\mathrm{Syl}_5}\}$, also $g \odot P = gPg^{-1} = \mathrm{id}_{\mathrm{Syl}_5}(P) = P$ für ein $P \in \mathrm{Syl}_5$ und für alle $g \in G$. Das bedeutet, dass $P$ Normalteiler von $G$ ist. Da $|\{e_G\}| = 1 < |P| = 125 < |G|$, folgt $P \triangleleft G$ als nicht-trivialer Normalteiler. Nach der Folgerung aus dem zweiten Sylowschen Satz gilt dann $n_5 = 1$, was im Widerspruch zu $n_5 = 6$ steht. Damit gilt in der Tat $G \triangleright \ker\Phi \notin \{\{e_G\}, G\}$, $G$ ist mithin nicht einfach. □

**Aufgabe 28 (F15T1A3)** Sei $G$ Gruppe der Ordnung $|G| = 105 = 3 \cdot 5 \cdot 7$. (a) Wir zeigen zunächst, dass $G$ einen Normalteiler der Ordnung 5 oder 7 hat. Sei $\nu_p$ die Anzahl der $p$-Sylowgruppen von $G$. Für $p = 5$ gilt nach dem dritten Sylowsatz $\nu_5|3 \cdot 7$, also $\nu_5 \in \{1, 3, 7, 21\}$. Ferner gilt $\nu_5 \equiv 1 \bmod(5)$. Da $3 \not\equiv 1 \bmod(5)$ und $7 \equiv 2 \bmod(5) \not\equiv 1 \bmod(5)$, aber $4 \cdot 5 + 1 = 21 \equiv 1 \bmod(5)$, folgt $\nu_5 \in \{1, 21\}$. Für $p = 7$ finden wir nach dem dritten Sylowsatz $\nu_7|3{\cdot}5$, also $\nu_7 \in \{1, 3, 5, 15\}$. Ferner gilt $\nu_7 = 1 \bmod(7)$. Wegen $3 \not\equiv 1 \bmod(7)$ und $5 \not\equiv 1 \bmod(7)$ aber $2{\cdot}7{+}1 = 15 \equiv 1 \bmod(7)$ folgt $\nu_7 \in \{1, 15\}$. Dass $G$ einen Normalteiler der Ordnung 5 oder 7 besitzt, ist nach der Folgerung zum zweiten Sylowschen Satz äquivalent dazu, dass $G$ genau eine $p$-Sylowgruppe $P$ zu $p = 5$ bzw. $p = 7$ besitzt. Indem wir also ausschließen, dass es $\nu_5 = 21$ 5-Sylowgruppen und $\nu_7 = 15$ 7-Sylowgruppen von $G$ gibt, zeigen wir, dass $G$ eine $p0-$Sylowgruppe zu $p = 5$ oder $p = 7$ besitzt, nach obenstehender Ausführung also einen Normalteiler der gewünschten Ordnung. Angenommen, $\nu_5 = 21$ und $\nu_7 = 15$. Die 5-Sylowgruppen von $G$ sind von maximaler 5-Potenzordnung, d.h., von Ordnung 5. Da 5 Primzahl, sind die 5-Sylowgruppen zyklisch. Analog sind die 7-Sylowgruppen von $G$ von maximaler 7-Potenzordnung, also von Ordnung 7. Da 7 Primzahl, sind die 7-Sylowgruppen von $G$ ebenfalls alles zyklisch. Laut Vorlesung ist für eine zyklische Gruppe der Ordnung $p$ (prim) die Anzahl der Elemente der Ordnung $p$ gerade $\Phi(p) = p - 1$, wo $\Phi$ die Euler'sche $\Phi$-Funktion ist. Wir haben also in $G$ auf jeden Fall $n_5 \cdot \Phi(5) = 21 \cdot 4 = 84$ Elemente der Ordnung 5, da die 5-Sylowgruppen jeweils paarweise trivialen Schnitt haben. Analog finden wir, dass es in $G$ auf jeden Fall $n_7 \cdot \Phi(7) = 15 \cdot 6 = 90$ Elemente der Ordnung 7 gibt. Da für zwei verschiedene Primzahlen $p, q$ je eine $p$-Sylowgruppe und eine $q$-Sylowgruppe trivialen Schnitt hat, finden wir zusammen mit dem Element der Ordnung 1, dem Neutralelement, dass in $G$ mindestens $n_5 \cdot \Phi(5) + n_7 \cdot \Phi(7) + 1 = 175$ verschiedene

Elemente enthalten sind. Da aber $|G| = 105 < 175$ haben wir einen Widerspruch dazu, dass $G$ genau 105 Elemente enthält. Insofern kann der Fall $n_5 = 21$ und $n_7 = 15$ nicht auftreten. Also gilt $n_5 = 1$ oder $n_7 = 1$. Im ersteren Fall ist, wie oben beschrieben, die einzige 5-Sylowgruppe $P_5$ von $G$ Normalteiler von $G$, im zweiten Fall ist analog die einzige 7-Sylowgruppe $P_7$ von $G$ Normalteiler. In jedem Fall hat $G$ einen Normalteiler der gesuchten Ordnung. (b) Wir zeigen nun, dass $G$ auflösbar ist. Wir halten fest, dass für $N \triangleleft G$ für eine beliebige Gruppe Normalteiler ist, $G$ auflösbar äquivalent dazu ist, dass $G/N$ und $N$ auflösbar sind. Bekannt ist ferner, dass abelsche Gruppen auflösbar sind.

- *Fall $\nu_5 = 1$:* Dann hat $G$ eine Normalteiler der Ordnung 5, nämlich die einzige 5-Sylowgruppe $P_5$. Die Faktorgruppe $H_5 \equiv G/P_5$ hat nach dem Satz von Lagrange die Ordnung 21. Für die Anzahl $\mu_7$ der 7-Sylowgruppen von $H_5$ gilt nach dem dritten Sylowsatz $\mu_7|3$, also $\mu_7 \in \{1, 3\}$. Ebenfalls nach dem dritten Sylowsatz gilt $\mu_7 \equiv 1 \bmod(7)$, so dass wegen $3 \not\equiv 1 \bmod(7)$ nur $\mu_7 = 1$ gelten kann. Nach der Folgerung zum dritten Sylowschen Satz ist also die einzige 7-Sylowgruppe $Q_7$ von $H_5$ ein Normalteiler von $H_5$. Nach dem Satz von Lagrange gilt für die Ordnung der Faktorgruppe $H_5/Q_7$ also $|H_5/Q_7| = 3$. Das ist eine Primzahl, so dass $H_5/Q_7 \simeq \mathbb{Z}/(3\mathbb{Z})$ isomorph zu einer zyklischen, insbesondere also abelschen Gruppe ist, und damit selber abelsch ist. $Q_7$ ist als Gruppen von Primzahlordnung ebenfalls zyklisch und damit abeslch. Zusammen ist also $H_5/Q_7$ und $Q_7$ abelsch, also auflösbar, und damit auch $H_5$ auflösbar. Da $P_5$ von Primzahlordnung 5, damit zyklisch, also abelsch also auflösbar ist, ist $H_5$ und $P_5$ auflösbar, also nach dem eingangs zitierten Satz damit $G$.

- *Fall $\nu_7 = 1$:*Dann hat $G$ einen Normalteiler der Ordnung 7,nämlich die einzige 7-Sylowgruppe $P_7$. Die Faktorgruppe $H_7 \equiv G/P_7$ hat nach dem Satz von Lagrange die Ordnung 15. Für die Anzahl $\kappa_5$ der 5-Sylowgruppen von $H_7$ gilt nach dem dritten Sylowschen Satz $\kappa 5|3$, also $\kappa_5 \in \{1, 3\}$. Wegen $\kappa_5 \equiv 1 \bmod(5)$ auch laut drittem Sylowschen Satz, aber $3 \not\equiv 1 \bmod(5)$, kann nur $\kappa_5 = 1$. Die Folgerung zum zweiten Sylowschen Satz liefert also, dass die einzige 5-Sylowgruppe $Q_5$ von $H_7$ ein Normalteiler von $H_7$ ist. Die Faktorgruppe $H_7/Q_5$ hat nach Lagrange die Ordnung 3. Als Gruppen von Primzahlordnung sind $H_7/Q_5$, $Q_5$ isomorph zu zyklischen Gruppen der respektiven Gruppenordnung, also zu $\mathbb{Z}/(3\mathbb{Z})$ bzw. $\mathbb{Z}/(5\mathbb{Z})$. Diese sind jeweils abelsch, also sind auch $H_7/Q_5$ und $Q_5$ abelsche Gruppen und damit auflösbar. Damit ist dann laut Vorlesung auch $H_7$ auflösbar. Da $P_7 \trianglelefteq G$ Normalteiler von Primzahlordnung 7 ist, ist $P_7 \simeq \mathbb{Z}/(7\mathbb{Z})$ zyklisch und insbesondere abelsch, also auflösbar. Da nun $H_7, P_7$ beide auflösbare Gruppen sind, ist auch $G$ auflösbar.

Insgesamt ergibt sich in beiden Fällen, dass $G$ jeweils auflösbar ist, so dass wir gezeigt haben, dass jede Gruppe $G$ der Ordnung 105 auflösbar ist. □

**Aufgabe 29 (F17T1A3)** Zu zeigen ist, dass es keine einfache Gruppe der Ordnung 300 gibt. Sei $G$ eine Gruppe der Ordnung 300, die einfach ist. Da $300 = 2^2 \cdot 3 \cdot 5^2$ finden wir mit dem dritten Sylowschen für die Anzahl der 5-Sylowgruppen $\nu_5$, dass $\nu_5|12$, also $\nu_5 \in \{1, 2, 6, 12\}$. Da weiter nach dem dritten Sylowschen Satz gilt $\nu_5 \equiv 1 \bmod(5)$ aber $2 \not\equiv 1 \bmod(5)$ und $2 \cdot 5 + 2 = 12 \not\equiv 1 \bmod(5)$, folgt $\nu_5 \in \{1, 6\}$.

- *Fall 1 $\nu_5 = 1$:* In diesem Fall gibt es nur eine 5-Sylowgruppe von $G$, bezeichnet mit $P_5$. Diese ist nach einer Folgerung zum zweiten Sylow-Satz auch ein Normalteiler von $G$. Da $1 < |P_5| = 5^2 < |G| = 300$, gilt somit $\{e_G\} < P_5 < G$, also haben wir mit $P_5$ einen nicht-trivialen Normalteiler von $G$ gefunden, im Widerspruch zur Einfachheit von $G$.

- *Fall 2 $\nu_7 = 6$:* Definiere in diesem Fall die Operation $\odot : G \times \mathrm{Syl}_5 \to \mathrm{Syl}_5$ durch $(g, P) \to gPg^{-1}$, wobei $\mathrm{Syl}_5$ die, nach Voraussetzung 6-elementige, Menge der 5-Sylowgruppen von $G$ bezeichnet. Laut dem Satz über den Zusammenhang von Gruppenoperationen und -homomorphismen ist durch die Operation vermöge $\Phi : G \to \mathrm{Per}(\mathrm{Syl}_5), g \mapsto \odot(g, \heartsuit)$ ein Gruppenhomomorphismus definiert. Aus der Vorlesung ist bekannt, dass der Kern $\ker\Phi$ Normalteiler von $G$ ist. Können wir also ausschließen, dass $\ker\Phi \in \{\{e_G\}, G\}$, haben wir einen nicht-trivialen Normalteiler von $G$, im Widerspruch dazu, dass $G$ als einfach angenommen wurde. $G$ ist dann nicht einfach.

  - *Fall 1.1:* Nehmen wir zunächst an, dass $\ker\Phi = \{e_G\}$. Es gilt dann, dass $\Phi$ Gruppenmomomorphismus, also injektiv ist. Wegen $|\mathrm{Syl}_5| = \nu_5 = 6$, gilt $\mathrm{Per}(\mathrm{Syl}_5) \simeq S_6$, wobei $S_6$ als symmetrische Gruppe Ordnung $|S_6| = 6! = 720$ hat. Da ein Gruppenmonomorphismus stets ein Gruppenisomorphismus auf sein Bild ist, gilt $\Phi(G) \leq \mathrm{Per}(\mathrm{Syl}_5)$ und nach dem Satz von Lagrange $|\Phi(G)||720 = |S_6|$. Allerdings $|\Phi(G)| = |G|$ infolge der Isomorphismuseigenschaft von $\Phi$ auf sein Bild und 300 kein Teiler von 720. Damit haben wir einen Widerspruch dazu, dass $\Phi(G) \leq \mathrm{Per}(\mathrm{Syl}_5)$. Folglich ist $\ker\Phi = \{e_G\}$ nicht möglich.
  - *Fall 2.2:* Nehmen wir nun an, dass $\ker\Phi = G$. Dann gilt $\Phi(G) = \mathrm{id}_{\mathrm{Syl}_5}$, da $\mathrm{id}_{\mathrm{Syl}_5} \in \mathrm{Per}(\mathrm{Syl}_5)$ das Neutralelement ist. Sei weiter $P$ beliebige 5-Sylowgruppe von $G$. Es gilt nun für beliebiges $g \in G$, $\odot(g, P) = gPg^{-1} = \mathrm{id}_{\mathrm{Syl}_5}(P) = P$, also $gPg^{-1} = P$. Damit ist $P$ Normalteiler von $G$. Die Folgerung zum zweiten Sylowschen Satz liefert uns nun, dass dann $\nu_5 = 1$, im Widerspruch zur Voraussetzung $\nu_5 = 6$. Dieser Fall scheidet also aus.

  Insgesamt haben wir also $\ker\Phi \notin \{\{e_G\}, G\}$. Damit ist $\ker\Phi$ ein nicht-trivialer Normalteiler von $G$ im Widerspruch zur Einfachheit von $G$.

In jedem Fall hat $G$ einen nicht-trivialen Normalteiler, ist also nicht-einfach. □

**Aufgabe 30 (H14T3A1)** Sei $G$ eine Gruppe der Ordnung 2014. Zu zeigen ist, dass $G$ einen zyklischen Normalteiler der Ordnung $1007 = 19 \cdot 53$ besitzt. Zunächst gilt für eine Gruppe $G$ der Ordnung 2014, dass $|G| = 2014 = 19 \cdot 53 \cdot 2$. Sei $\nu_p$für eine Primzahl $p$ die Anzahl der $p$-Sylowgruppen von $G$. Nach dem dritten Sylowschen Satz gilt für die Anzahl $\nu_{53}$ der 53-Sylowgruppen von $G$ einmal $\nu_{53}|(2 \cdot 19)$, also $\nu_p \in \{1, 2, 19, 2 \cdot 19 = 38\}$, und weiter $\nu_{53} \equiv 1 \bmod(53)$. Wegen $2 \not\equiv 1 \bmod(53)$ und $19 \not\equiv 1 \bmod(53)$ und $38 \not\equiv 1 \bmod(53)$ ist nur $\nu_{53} = 1$ möglich. Bezeichne also die einzige 53-Sylowgruppe von $G$ mit $P_{53}$. Für die Anzahl $\nu_{19}$ der 19-Sylowgruppen von $G$ gilt $\nu_{19}|2 \cdot 53$, also $\nu_{19} \in \{1, 2, 53, 106\}$ nach dem dritten Sylowschen Satz. Nun gilt weiterhin nach dem dritten Sylowschen Satz $\nu_{19} \equiv 1 \bmod(19)$. Es gilt

$53 = 2 \cdot 19 + 15$, also $53 \equiv 15 \bmod(19) \not\equiv 1 \bmod(19)$ und $106 = 95 + 11 = 5 \cdot 19 + 11$, also $106 \equiv 11 \bmod(19) \not\equiv 1 \bmod(19)$. Zusätzlich ist $2 \not\equiv 1 \bmod(19)$. Folglich ist nur $\nu_{19} = 1$ möglich. Bezeichnet nun $P_{19}$ die einzige 19-Sylowgruppe von $G$, liefert die Folgerung zum zweiten Sylowschen Satz, dass $P_{19}$ ebenfalls ein Normalteiler von $G$ ist. Da $\mathrm{ggT}(|P_{19}|, |P_{53}|) = \mathrm{ggT}(19, 53) = 1$, gilt $P_{19} \cap P_{53} = \{e_G\}$. Definiere nun $U = P_{53} \cdot P_{19}$. Dieses Komplexprodukt ist wegen $P_{53} \cap P_{19} = \{e_G\}$, $P_{53} \trianglelefteq U$ inneres semidirektes Produkt von Gruppen. Da sogar $P_{19} \triangleleft U$, ist $U$ sogar inneres direktes Produkt von Gruppen. Laut Vorlesung gilt nun $U \simeq P_{53} \times P_{19}$. Da $P_{53}$ und $P_{19}$ jeweils von Primzahlordnung sind, sind sie jeweils isomorph zu den zyklischen Gruppen $\mathbb{Z}/(19\mathbb{Z})$ respektive $\mathbb{Z}/(53\mathbb{Z})$. Also gilt zunächst $U \simeq \mathbb{Z}/(19\mathbb{Z}) \times \mathbb{Z}/(53\mathbb{Z})$. Da zudem $\mathrm{ggT}(53, 19) = 1$, liefert der chinesische Restklassensatz $\mathbb{Z}/(19\mathbb{Z}) \times \mathbb{Z}/(53\mathbb{Z}) \simeq \mathbb{Z}/(19 \cdot 53\mathbb{Z}) = \mathbb{Z}/(1007\mathbb{Z})$. Also ist $U$isomorph zur zyklischen Gruppe der Ordnung 1007 und insbesondere selber zyklisch und von Ordnung 1007. Wir müssen nun zeigen, das $U \trianglelefteq G$. Nach dem Satz von Lagrange gilt nun $(G : U) = |G|/|U| = 2014/1007 = 2$. Aus der Vorlesung ist bekannt, das Index 2 Untergruppen Normalteiler sind. Also gilt tatsächlich $U \trianglelefteq G$ und $U$ ist zyklisch von Ordnung 1007, wie zu zeigen war. □

**Aufgabe 31 (H17T3A1)** Sei $G$ Gruppe der Ordnung $992 = 2^5 \cdot 31$ ($2^5 = 32$), $n_p$ sei für eine beliebige Primzahl $p$ die Anzahl der $p$-Sylowgruppen von $G$. Wir bestimmen zunächst $n_2$ und $n_3 1$. Laut drittem Sylowsatz gilt $n_2 | 31$ und $n_2 \equiv 1 \bmod(2)$. Da 31 Primzahl ist, folgt $n_2 \in \{1, 31\}$. Die zweite Bedingung liefert nichts Neues, da beide Möglichkeiten für $n_2$ bereits ungerade Zahlen sind. Der dritte Sylowsatz liefert für $n_{31}$ die zwei Bedingungen $n_{31} \in \{1, 2, 2^2 = 4, 2^3 = 8, 2^4 = 6, 2^5 = 32\}$ und $n_{31} \equiv 1 \bmod(31)$. Da $2 \equiv 2 \bmod(31) \not\equiv 1 \bmod(31)$, $2^2 = 4 \bmod(31) \not\equiv 1 \bmod(31)$, $2^3 = 8 \bmod(31) \not\equiv 1 \bmod(31)$ und $2^4 \equiv 16 \bmod(31) \not\equiv 1 \bmod(31)$ aber $32 = 1 \cdot 31 + 1 \equiv 1 \bmod(31)$ gibt es die zwei Möglichkeiten $n_{31} \in \{1, 32\}$. Wir müssen nun zeigen, dass $G$ auflösbar ist. Dazu wiederholen wir aus der Vorlesung, dass für eine gegebene Gruppe $G$ und einen Normalteiler $N \trianglelefteq G$ die Gruppe $G$ genau dann auflösbar ist, wenn $G/N$ und $N$ beide auflösbar sind. Ferner ist bekannt, dass abelsche Gruppe stets auflösbar sind. Um den zuerst genannten Satz anzuwenden, benötigen wir einen Normalteiler der für die Aufgabe relevanten Gruppe $G$. Sei $p$ beliebiger Primteiler von $|G|$. Laut einer Folgerung zum zweiten Sylowschen Satz ist für eine $p$-Sylowgruppe die Normalteilereigenschaft äquivalent dazu, dass diese $p$-Sylowgruppe die einzige $p$-Sylowgruppe von $G$ ist. Wir schließen also den Fall, dass $n_{31} = 32$ und $n_{32} = 31$ durch Elemente-Zählen aus. Sei $P_{31}$ eine beliebige 31-Sylowgruppe von $G$. Dann ist $P_{31}$ von Primzahlordnung, also zyklisch von der Ordnung 31. Laut Vorlesung gibt es dann in $P_{31}$ genau $\Phi(31) = 31 - 1 = 30$ Elemente der Ordnung 31, wobei $\Phi$ die Euler'sche $\Phi$-Funktion bezeichnet. Da nach Voraussetzung $32 = n_{31}$ verschiedene 31-Sylowgruppen existieren, liefert der zweite Sylowsatz, d.h., je zwei verschiedene 31-Sylowgruppen sind zueinander konjugiert und haben somit im Falle von Primzahlordnung trivialen Schnitt, dass es in $G$ $n_{31} \cdot \Phi(31) = 32 \cdot 30 = 960$ Elemente der Ordnung 31 gibt. Da $\mathrm{ggT}(32, 31) = 1$, ist je eine $2-$Sylowgruppe $P_2$ von $G$ zu jeder 31-Sylowgruppe von $P_{31}$ so, dass der Schnitt $P_{31} \cap P_2 = \{e_G\}$ trivial ist. Seien also $P_2, P_2'$ zwei verschiedene 2-Sylowgruppen von $G$. Bezeichne mit $\mathrm{Syl}_{31}$ die Menge der 31-Sylowgruppen von $G$. Diese Menge ist 32-elementig nach Voraussetzung, dass $n_{31} = 32$. Wegen $P_2 \cap P_{31} = \{e_G\}$ gilt $\left| P_2 \setminus \{e_G\} \cup \bigcup_{P_{31} \in \mathrm{Syl}_{31}} \bigcup_{g \in P_{31}, \mathrm{ord}(g) = 31} \{g\} \right| =$

$(32-1)+30\cdot 32 = 991$. Da $P_2$ von $P_2'$ verschieden ist, existiert ein Element $g(\neq e_G)$ in $P_2'$, so dass $g \notin P_2$. Da $1 < \mathrm{ord}(g)|32$, also gerade ist, gilt $\mathrm{ord}(g) \not| 31$, also $g \notin P_{31}$. Da $g \in G$ und zusätzlich für das Neutralelement gilt $e_G \in G$, haben wir zwei weitere Elemente gefunden, die noch nicht gezählt wurden, aber in $G$ liegen. Also gilt $|G| \geq 991 + |\{e_G, g\}| = 991 + 2 = 993 > 992 = |G|$. Das ist ein Widerspruch. Folglich kann der Fall $n_2 = 31$ und $n_{31} = 32$ nicht auftreten. Nach Aufgabenteil (a) ist demnach $n_2 = 1$ oder $n_{31} = 1$. Also hat, nach der besprochenen Folgerung zum zweiten Sylowsatz, $G$ einen Normalteiler der Ordnung $2^5 = 32$ oder einen Normalteiler der Ordnung 31.

- *Fall 1, $n_2 = 1$:* Dann hat $G$ auf jeden Fall einen Normalteiler der Ordnung $32 = 2^5$, nämlich die einzige 2-Sylowgruppe $P_2$. Für die Ordnung der Faktorgruppe $G/P_2$ gilt nach dem Satz für Lagrange $|G/P_2| = |G|/|P_2| = 31$. Da 31 eine Primzahl ist, ist $G/P_{31}$ eine zyklische Gruppe der Ordnung 31, insbesondere also abelsch und damit auflösbar. Zu zeigen ist noch, dass $P_2$ auflösbar ist. Aus der Vorlesung ist bekannt, dass Gruppen von $p$-Potenzordung stets auflösbar sind. Also ist für $p = 2$ auch $P_2$ auflösbar. Die Auflösbarkeit von $P_2$ und $G/P_2$ ist nach dem eingangs zitierten Satz gerade äquivalent zur Auflösbarkeit von $G$. Damit ist $G$ auflösbar.

- *Fall 2, $n_{31} = 1$:* Dann hat $G$ auf jeden Fall einen Normalteiler der Ordnung 31, nämlich die einzige 31-Sylowgruppe $P_{31}$. Für die Ordnung der Faktorgruppe $G/P_{31}$ gilt nach dem Satz für Lagrange $|G/P_{31}| = |G|/|P_{31}| = 32 = 2^5$. Da 32 eine Primzahlpotenz ist, ist $G/P_{31}$ laut Vorlesung auflösbar. Zusammen mit der Auflösbarkeit von $P_{31}$ ist auch $G$ auflösbar.

In jedem Fall ist $G$ auflösbar. □

**Aufgabe 32 (F15T3A2)** Seien $p, q, r$ Primzahlen so dass $p < q < r$ und $pq < r + 1$. Sei $G$ eine Gruppe der Ordnung $pqr$. Zu zeigen ist, das $G$ auflösbar ist. Wir bestimmen zuerst die Anzahlen der $r$-Sylowgruppen von $G$, bezeichnet mit $\nu_p$, $\nu_q$, $\nu_r$ respektive. Nach dem dritten Sylowsatz gilt $\nu_r | pq$ und $\nu_r = 1 \bmod(r)$, also $\nu_r \in \{1, p, q, pq\}$, aber wegen $p \not\equiv 1 \bmod(r)$, da $1 < p < r$ und wegen $q \not\equiv 1 \bmod(r)$, da $1 < q < r$ und $pq \not\equiv \bmod(r)$, da $1 < p < pq < r + 1$, ist nur $\nu_r = 1$ möglich. Nach einer Folgerung zum zweiten Sylowschen Satz ist dann die einzige $r$-Sylowgruppe $P_r$ von $G$ Normalteiler von $G$. Da $r$ Primzahl ist, ist $P_r$ insbesondere zyklische Gruppe der Ordnung $r$, also abelsch, also auflösbar. Betrachte nun die Faktorgruppe $G/P_r$ ($P_r \lhd G$ nichttrivial wegen $1 < |P_r| = r < pqr = |G|$). Nach dem Satz von Lagrange ist $|G/P_r| = |G|/|P_r| = pqr/r = pq$. Bezeichne mit $\mu_q$ die Anzahl der $q$-Sylowuntergruppen von $G/P_r$. Es gilt nach dem dritten Sylowschen Satz $\mu_q | p$, also $\mu_q \in \{1, p\}$. Weiter gilt nach dem dritten Sylowschen Satz $\mu_q \equiv 1 \bmod(q)$. Wegen $p < q$, gilt $p \equiv p \bmod(q) \neq 1 \bmod(q)$. Also ist nur $\mu_q = 1$ möglich. Die einzige $q$-Sylowgruppe von $G/P_r$, bezeichnet mit $Q_q$, ist also Normalteiler von $G/P_r$, $Q_q \trianglelefteq G/P_r$. Wegen $1 < p < q = |Q_q| < pq = |G/P_r|$ ist $Q_q$ nichttrivialer Normalteiler von $G/P_r$. Da $|Q_q| = q$ eine Primzahl ist, ist $Q_q$ zyklisch von Ordnung $q$, insbesondere also abelsch und damit auflösbar. Für die Faktorgruppe $(G/P_r)/Q_q$ gilt nach dem Satz von Lagrange $|(G/P_r)/Q_q| = |G/P_r|/|Q_q| = pq/q = p$. Also hat $(G/P_r)/Q_q$ ebenfalls Primzahlordnung, ist somit zyklisch, also abelsch, also

auflösbar. Da $Q_q \triangleleft G/P_r$ und $Q_q$ sowie $(G/P_r)/Q_q$ auflösbar sind, ist laut Vorlesung auch $G/P_r$ auflösbar. Da $P_r \triangleleft G$ und $G/P_r$ sowie $P_r$ auflösbar sind, ist laut Vorlesung auch $G$ auflösbar. $\square$

**Aufgabe 33** Sei $n \in \mathbb{N}$, $V = \mathbb{C}^n$, $G = \mathrm{GL}_n(\mathbb{C})$ und $\mathcal{U}$ die Menge aller Untervektorräume von $V$. Sei $\odot : G \times \mathcal{U} \to \mathcal{U}, (A, U) \mapsto A \odot U := A(U)$ die angegebene Operation von $G$ auf $\mathcal{U}$. Gesucht ist die Anzahl $N$ der Bahnen der Operation. Wir behaupten zu diesem Zwecke, dass $R = \{\{0\}, \mathrm{lin}_{\mathbb{C}}(\hat{e}_1), \mathrm{lin}_{\mathbb{C}}(\hat{e}_1, \hat{e}_2), ...., \mathrm{lin}_{\mathbb{C}}(\hat{e}_1, \hat{e}_2, ..., \hat{e}_n)\}$ ein Repräsentantensystem der Bahnen der Operation ist. $\hat{e}_k$ bezeichnet hierbei den $k$-ten Einheitsvektor der Standardbasis des $n$-dimensionalen $\mathbb{C}$-Vektorraums $V$. Ist der Nachweis der Repräsentantensystemeigenschaft erbracht, so gilt $N = |R|$, da die in Rede stehenden Bahnen einen disjunkte Zerlegung von $\mathcal{U}$ bilden. Zum Nachweis der Repräsentantensystemeigenschaft sei $U \in \mathcal{U}$ ein beliebiger Untervektorraum von $V$ und $G(U)$ die Bahn von $U$ unter der Operation von oben.Zu zeigen ist (i), dass mindestens ein $X \in R$ in $G(U)$ enthalten ist und dass (ii) höchstens ein $X \in R$ in $G(U)$ enthalten ist.

- *Fall 1:* $\dim U = 0$ Laut Vorlesung ist dann der einzige Untervektorraum von $V$ mit Dimension 0 der triviale Untervektorraum $\{0\}$. Es gilt $\emptyset \in R$. Damit enthält die Bahn $G(U)$ tatsächlich ein Element aus $R$ Angenommen, es gäbe nun noch ein weiteres $X \in R$ mit $X \neq \{0\}$, so dass $X \in G(\{0\})$. Dann gilt ebenfalls $\{0\} \in G(X)$ nach der Zerlegungseigenschaft der Bahnen einer Gruppenoperation. Dann gibt es ein $A \in G$, so dass $\{0\} = A(X)$. Betrachte nun, die durch $A$ definierte lineare Abbildung $\Phi_A : X \to \mathbb{C}^n, v \mapsto Av$. Wegen $X \neq \{0\}$, ist $X$ mindestens ein-dimensionaler Untervektorraum von $V$. Nach der Dimensionsformel gilt $\dim \ker \Phi_A + \dim \mathrm{im}\Phi_A = \dim X \geq 1$. Da $A$ invertierbar ist, ist $\Phi_A$ zumindest injektiv, also $\ker \Phi_A = \{0\}$. Damit folgt $1 \leq \dim X = \dim \mathrm{im}\Phi_A$. Allerdings gilt $\mathrm{im}\Phi_A = \{0\}$, so dass der Widerspruch $1 \leq \dim X = 0$ entsteht. Also war die Annahme, es gäbe $X \neq \{0\}$ mit den beschriebenen Eigenschaften, falsch. Also enthält die Bahn $G(U)$ höchstens ein Element. Zusammen haben wir gezeigt, dass für $U \in \mathcal{U}$ mit $\dim U = 0$ die Bahn $G(U)$ genau ein $X \in R$ enthält.

- *Fall 2:* $1 \leq \dim U = k \leq n$ Dann gilt $U \neq \{0\}$. Weegen der Zerlegungseigenschaft der Bahnen gilt $X \in G(U) \leftrightarrow U \in G(X)$. Sei $k = \dim U$. Aus der Vorlesung ist bekannt, dass es dann linear unabhängige Vektoren $v_1, ..., v_k \in U$ gibt, so dass $U = \mathrm{lin}_{\mathbb{C}}(v_1, ..., v_k)$. Mit dem Basis-Ergänzungssatz finden wir Vektoren $w_{k+1}, ..., w_n \in V \setminus U$, so dass $v_1, ..., v_k, w_{k+1}, ..., w_n$ genau $n$ linear unabhängige Vektoren in $V$ sind. Nach dem Satz über Basen endlich dimensionaler Vektorräume gilt dann, dass $v_1, ..., v_k, w_{k+1}, ..., w_n$ eine Basis von $V$ sind. Definiere nun die Matrix $A = (v_1, ..., v_k, w_{k+1}, ..., w_n)$, indem die Vektoren von gerade eben als Spalten eingetragen werden. Da $v_1, ..., v_k, w_{k+1}, ..., w_n$ linear unabängig sind, ist $A$ eine invertierbare Matrix, d.h., $A \in G$. Ferner gilt $A(X_k) = U$ für $X_k = \mathrm{lin}_{\mathbb{C}}(\hat{e}_1, ..., \hat{e}_k)$. Denn $U \ni v = \sum_{l=1} \lambda_l v_l = \sum_{l=1}^k \lambda_l A(\hat{e}_l) = \sum_{l=1}^k A(\lambda_l \hat{e}_l) = A(\sum_{l=1}^k \lambda_l \hat{e}_l) =: Aw$ mit $w = \sum_{l=1}^k \lambda_l \hat{e}_l \in X_k$ und nach obiger Rechnung eindeutig festgelegt. Damit haben wir gezeigt $U \in G(X_k)$, also nach der Bemerkung am Anfang $X_k \in G(U)$. Also enthält jede

Bahn mindestens ein Element aus $R$. Um zu zeigen, dass die Bahn $G(U)$ auch nur höchstens ein Element aus $R$ enhält, bemerken wir, dass für paarweise verschiedene Elemente $X_k, X_{k'} \in R$ gilt $\dim X_k \neq \dim X_{k'}$. Angenommen, es gäbe $U \in \mathcal{U}$, so dass $X_k, X_{k'} \in G(U)$ mit $k \neq k'$ gilt, d.h., $X_k \neq X_{k'}$. Dann gbt es $B_1, B_2 \in G$, so dass $X_{k'} = B_1(U)$, $X_k = B_2^{-1}(U)$ bzw. $U = B_2(X_k)$. Wegen der Verträglichkeit der Operation $\odot$ mit der Verknüpfung aus $\mathcal{U}$, gilt für $A \equiv B_1 \cdot B_2 \in G$ also $X_{k'} = A(X_k)$. Definiere nun die lineare Abbildung $\Phi_A : X_k \to V \supseteq X_{k'}$ durch $v \mapsto Av$. Nach der Dimensionsformel der linearen Algebra gilt also $\dim X_k = \dim \ker \Phi_A + \dim \mathrm{im} \Phi_A$. Da $A \in G$ invertierbar ist, ist $\Phi_A$ auf $X_k \subseteq V$ zumindest injektiv, d.h., $\dim \ker \Phi_A = \dim\{0\} = 0$. Also gilt $\dim X_k = \dim \mathrm{im} \Phi_A$. Wegen $\Phi_A(X_k) = A(X_k) = X_{k'}$ gilt aber $\dim \mathrm{im} \Phi_A = \dim X_{k'}$. Also $\dim X_k = \dim X_{k'}$. Nach Voraussetzung gilt aber $X_k \neq X_{k'}$, so dass nach der Beobachtung oben $\dim X_k = k \neq k' = \dim X_{k'}$. Das ist ein Widerspruch zum vorherigen Ergebnis. Also war die Annahme, es gäbe $U \in \mathcal{U}$, so dass $X_k, X_{k'} \in R$ mit $X_k \neq X_{k'}$ existieren aber $X_k, X_{k'} \in G(U)$, falsch. Also enthält jede Bahn $G(U)$ höchstens ein Element aus $R$. Zusammen mit dem ersten teil des Beweises folgt, dass jede Bahn $G(U)$ für $U \in \mathcal{U}$ mit $1 \leq \dim U \leq n$ genau ein $X_k \in R$ enthält.

Insgesamt ist damit der Nachweis der Repräsentantensystemeigenschaft erbracht. Es gilt für $|R|$ ferner $|R| = \sum_{k=0}^{n} 1 = n + 1$. Also gibt es genau $n + 1$ Bahnen der Operation. □

**Aufgabe 34 (H16T2A2)** Seien $A, B$ abelsche Gruppen, $\phi : B \to \mathrm{Aut}(A)$ Gruppenhomomorphismus. Definiere das semidirekte Produkt $A \rtimes_\phi B := \{(a, b) | a \in A, b \in B\}$. Dies ist nach Aufgabenstellung eine Gruppe bzgl. der Verknüpfung definiert durch $(a_1, b_1) * (a_2, b_2) \equiv (a_1 \phi(b_1)(a_2), b_1 b_2)$.
(a) Zu zeigen ist, dass $A \rtimes_\phi B$ genau dann abelsch ist, wenn $\phi : B \to \mathrm{Aut}(A), b \mapsto \mathrm{id}_A$. Wir zeigen zuerst "⇐". Sei also $\phi(b) = \mathrm{id}_A$ für alle $b \in B$. Dann gilt für $(a_1, b_1) \in A \rtimes_\phi B$, dass $(a_1, b_1) * (a_2, b_2) = (a_1 \phi(b_1) a_2, b_1 b_2) = (a_1 \mathrm{id}_A(a_2), b_1 b_2) = (a_1 a_2, b_1 b_2) = (a_2 a_1, b_2 b_1)$, da $A, B$ jeweils abelesch nach Voraussetzung. Andererseits gilt aber auch $(a_2, b_2) * (a_1, b_1) = (a_2 \phi(b_2)(a_1), b_2 b_1) = (a_2 \mathrm{id}_A(a_1) b_2 b_1) = (a_2 a_1, b_2 b_1)$. Zusammen mit dem vorherigen Ergebnis finden wir $(a_1, b_1) * (a_2, b_2) = (a_2, b_2) * (a_1, b_1)$. Beliebigkeit von $(a_1, b_1), (a_2, b_2) \in A \rtimes_\phi B$ impliziert nun, dass $A \rtimes_\phi B$ abelsch ist. Für die umgekehrte Richtung "⇒" müssen wir zeigen, dass die Kommutativität der Gruppe $\phi(b) = \mathrm{id}_A$ für alle $b \in B$ festlegt. Es gilt zunächst $(a, b) * (c, e_B) = (a\phi(b)(c), b e_B) = (a\phi(b)(c), b)$. Dies ist wegen der vorausgesetzten Kommutativität gleich $(c, e_B) * (a, b) = (c\phi(e_B)(a), b e_B) = (c \mathrm{id}_A(a), b) = (ca, b)$, denn die Gruppenhomomorphismus-Eigenschaft zusammen mit der Neutralelement-Eigenschaft von $\mathrm{id}_A \in \mathrm{Aut}(A)$ impliziert $\mathrm{id}_A = \phi(e_B)$. Also gilt $a\phi(b)(c) = ca$ mit $a, c \in A$ und $b \in B$ beliebig. Da $A$ kommutativ ist, gilt $a\phi(b)(c) = ac$ und da $a^{-1} \in A$ liefert Multiplikation der vorangegangenen Gleichung von links mit $a^{-1}$, dass $\phi(b)(c) = c$ für alle $c \in A$ und $b \in B$. Also gilt $\phi(b) = \mathrm{id}_A$ für alle $b \in B$. Damit ist die Äquivalenz bewiesen.
(b) Gesucht ist nun explizit eine nicht-abelsche Gruppe der Ordnung 2015. Durch Primfaktorzerlegung finden wir $2015 = 5 \cdot 403 = 5 \cdot 13 \cdot 31$. Die zyklischen Gruppen $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/13\mathbb{Z}$, $\mathbb{Z}/31\mathbb{Z}$ sind insbesondere abelsch und von teilerfremder Ordnung. Wir

konstruieren zunächst eine nicht-abelsche Gruppe $H$ der Ordnung $5 \cdot 31$. Das äußere direkte Produkt von $H$ und $\mathbb{Z}/13\mathbb{Z}$ ist dann nicht-abeslch, weil einer der Faktoren, nämlich $H$, nicht-abelsch ist. Wir müssen also einen nicht-trivialen Gruppenhomomorphismus $\phi : \mathbb{Z}/5\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/31\mathbb{Z})$ finden. Die Kontraposition von Teil (a) liefert uns dann, dass $\mathbb{Z}/31\mathbb{Z} \rtimes_\phi \mathbb{Z}/5\mathbb{Z} =: H$ nicht-abeslche Gruppe ist und die Teilerfremdheit der Ordnung der zyklischen "Faktoren" liefert, dass $|H| = 5 \cdot 31$. Da 31 Primzahl ist, gilt die Isomorphie $\Psi : \mathrm{Aut}(\mathbb{Z}/31\mathbb{Z}) \to (\mathbb{Z}/31\mathbb{Z})^\times = \mathbb{Z}/((31-1)\mathbb{Z}) = \mathbb{Z}/30\mathbb{Z}$. Sei $\bar{1}$ das erzeugende Element der $\mathbb{Z}/5\mathbb{Z}$. Dann ist vermöge $\phi(\bar{1}) = \Psi^{-1}(6 \cdot \bar{1})$ ein nicht-trivialer Gruppenhomomorphismus $\phi : \mathbb{Z}/5\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/31\mathbb{Z})$ erklärt. Die Homomorphismuseigenschaft ist klar: Denn, $\bar{1}$ hat Ordnung 5 in $\mathbb{Z}/5\mathbb{Z}$ und wird auf das Element $6 \cdot \bar{1} = \bar{6}$ vermöge $\Psi \circ \phi$ in $\mathbb{Z}/30\mathbb{Z}$ abgebildet. Da $\mathrm{ord}_{\mathbb{Z}/30\mathbb{Z}} = 30/\mathrm{ggT}(6, 30) = 5 | 5 = \mathrm{ord}_{\mathbb{Z}/5\mathbb{Z}}(\bar{1})$ handelt es sich bei $\Psi \circ \psi$, somit also auch bei $\Psi^{-1} \circ \Psi \circ \phi = \phi$, um einen Gruppenhomomorphismus. Da $\Psi \circ \phi(\bar{1}) = \bar{6} \neq \bar{0}$ ist auch $\phi$ nicht-trivial. Spezialisiere nun das soeben erhaltene $\phi$ und setze $H = \mathbb{Z}/31\mathbb{Z} \rtimes \mathbb{Z}/5\mathbb{Z}$ als semidirektes äußeres Produkt. Nach Kontraposition von Teil (a) ist dieses nicht-abelsch und hat die geforderte Ordnung $5 \cdot 31$. Nach den eingangs gemachten Ausführungen ist also

$$G := \mathbb{Z}/13\mathbb{Z} \times H = \mathbb{Z}/13\mathbb{Z} \times (\mathbb{Z}/31\mathbb{Z} \rtimes_\phi \mathbb{Z}/5\mathbb{Z}) \tag{63}$$

mit dem oben gefundenen $\phi$ und der Verknüpfung $\odot$definiert durch $(a_1, b_1, c_1) \odot (a_2, b_2, c_2) = (a_1 a_2, b_1 \phi(c_1)(b_2), c_1 c_2)$ eine nicht-abelsche Gruppe. Teilefremdheit der Ordnungen der Faktoren im direkten äußeren Produkt impliziert, dass $|G| = 13 \cdot (5 \cdot 31) = 2015$, wie gefordert. □

**Aufgabe 35 (F13T3A1)** Gesucht ist eine nicht-abelsche Gruppe der Ordnung 2013. Es gilt $2013 = 3 \cdot 671 = 3 \cdot 11 \cdot 61 = 3 \cdot 11 \cdot 4 \cdot 17$. Aus der Vorlesung ist bekannt, dass für zwei abelsche Gruppen $A, B$ und einen nicht-trivialen Gruppenhomomorphismus $\phi : B \to \mathrm{Aut}(A), b \mapsto \phi(b) \in \mathrm{Aut}(A)$ das äußere semi-direkte Produkt $A \rtimes_\phi B = \{(a, b) \in A \times B\}$ zusammen mit der Verknüpfung definiert durch $(a_1, b_1) * (a_2, b_2) = (a_1 \phi(b_1)(a_2), b_1 b_2)$ für alle $(a_1, b_1), (a_2, b_2) \in A \rtimes_\phi B$ eine nicht-abelsche Gruppe ist. Definiere zunächst die zyklischen, also abelschen Gruppen $H_1 = \mathbb{Z}/3\mathbb{Z}, H_2 = \mathbb{Z}/11\mathbb{Z}$, $H_3 = \mathbb{Z}/4\mathbb{Z}$ und $H_4 = \mathbb{Z}/17\mathbb{Z}$. Wir konstruieren zunächst ein nicht-abelsches äußeres semidirektes Produkt von $H_3, H_4$. Es gilt $\mathrm{Aut}(H_4) \simeq (\mathbb{Z}/17\mathbb{Z})^\times \simeq \mathbb{Z}/((17-1)\mathbb{Z}) = \mathbb{Z}/16\mathbb{Z} =: H_5$, da 17 Primzahl ist, und die Vorlesungsresultate zur Struktur der Einheitengruppe der Restklassenringe verwendet wurden. Da Komposition mit Isomorphismen die Nicht-Triviliatät von $\phi$ nicht ändert, reicht es, einen nicht-trivialen Gruppenhomomorphismus $\psi : H_3 \to H_5$ zwischen den zyklischen Gruppen $H_3$ und $H_5$ zu finden. Dieser ist wegen Zyklizität von $H_3$ bereits durch die Spezifikation des Bildes eines Erzeugers festgelegt. Sei $\bar{1}$ das erzeugende Element der $H_3$. Dann gilt $\phi(\bar{1}) = 4 \cdot \bar{1} = \bar{4} \in H_5$ ist ein Element der Ordnung 4 in $H_5$. Dies ist ein Teiler der Ordnung 4 des Erzeugers $\bar{1}$ von $H_3$. Also erhalten wir durch die Zuweisung $\psi(\bar{1}) = \bar{4}$ tatsächlich einen Gruppenhomomorphismus. Wegen $\bar{4} \neq \bar{0}$ in $H_5$, ist dieser auch nicht-trivial. Bezeichne den aus $\psi$, vermöge Komposition mit den oben beschriebenen Isomorphismen von Gruppen entstehenden, Homomorphismus von Gruppen $H_3 \to H_4$mit $\phi$. Es gilt nun nach den eingangs gemachten Bemerkungen, dass $H_4 \rtimes_\phi H_3$ eine nicht-abelsche Gruppe ist. Da $\mathrm{ggT}(|H_3|, |H_4|) = \mathrm{ggT}(4, 17) = 1$, gilt insbesondere

$|H_4 \rtimes_\phi H_3| = |H_3 \times H_4| = |H_3||H_4| = 4 \cdot 17$, wie gewünscht. Aus der Vorlesung ist nun bekannt, dass ein aus endlich vielen Faktoren bestehendes äußeres direktes Produkt von Gruppen eine Gruppe ist. Sie ist abeslch genau dann wenn jeder der Faktoren im äußeren direkten Produkt abelsch ist. Wir setzen nun wieder die Restklassen explizit statt der $H$-Gruppen ein:

$$G = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z} \times (\mathbb{Z}/17\mathbb{Z} \rtimes_\phi \mathbb{Z}/4\mathbb{Z})\,. \tag{64}$$

Da der dritte Faktor nicht-abelsch ist, liefert das oben zitierte Resultat die Nicht-Kommutativität von $G$. Teilerfremdheit der jeweiligen Ordnungen der Faktoren des äußeren direkten Produkts liefert ferner $|G| = 3 \cdot 11 \cdot (4 \cdot 17) = 2013$. Damit haben wir eine nicht-abelsche Gruppe der Ordnung 2013 konstruiert. □

**Aufgabe 36 (F16T1A3)** Sei $H$ Gruppe und $N \trianglelefteq H$ Normalteiler vom Index 2. Zu zeigen ist, falls $x, y \in H \setminus N$, dann ist $xy \in N$. Sei $H/N$ die Faktorgruppe. Da $x, y \in H \setminus N$ und es wegen $(H : N) = 2$ genau zwei Linksnebenklassen gibt, ist $|H/N| = (H : N) = 2$ Gruppe der Ordnung 2 und $[x] = [y]$, vom Neutralelement $[e_H]$ verschieden. Da die $H/N$ endlich ist, ist $1 \neq \mathrm{ord}([x]) = \mathrm{ord}([y])|2$, also $\mathrm{ord}([x]) = \mathrm{ord}([x]) = 2$. Damit gilt $[x][y] = [e_H]$, oder aber, mit Linksnebenklassen formuliert, $(xN)(yN) = (xyN) = N$ nach den Rechenregeln für Faktorgruppen. Insbesondere gilt dann für alle $n \in N$, dass $xyn \in N \Leftrightarrow xy \in n^{-1}N \Leftrightarrow xy \in N$. Sei nun $\cdot$ die Verknüpfung auf $H$ und $(A, +)$ eine abelsche Gruppe. Zu zeigen ist, dass die auf der Menge $A \times H$ definierte Verknüpfung, $(a_1, h_1) * (a_2, h_2) = (a_1 + a_2, h_1h_2)$ falls $h_1 \in N$ und $(a_1, h_1) * (a_2, h_2) = (a_1 - a_2, h_1h_2)$ falls $h_1 \notin N$, assoziativ ist. Seien dazu $(a_1, h_1), (a_2, h_2), (a_3, h_3) \in A \times H$ beliebig vorgegeben. Wir führen eine Fallunterscheidung durch, je nachdem ob $(h_1, h_2) \in \{N \times N, H \setminus N \times N, N \times H \setminus N, H \setminus N \times H \setminus N\}$.

- *Fall 1* $(h_1, h_2) \in N \times N$. Dann gilt $h_1h_2 \in N$ und wir rechnen nach:

$$\begin{aligned}(a_1, h_1) * ((a_2, h_2) * (a_3, h_3)) &= (a_1, h_1) * (a_2 + a_3, h_2h_3)\\ &= (a_1 + a_2 + a_3, h_1h_2h_3)\\ &= (a_1 + a_2, h_1h_2) * (a_3, h_3)\\ &= ((a_1, h_1) * (a_2, h_2)) * (a_3, h_3)\end{aligned}$$

- *Fall 2* $(h_1, h_2) \in H \setminus N \times N$. Dann gilt $h_1h_2 \in H \setminus N$ und wir rechnen nach:

$$\begin{aligned}(a_1, h_1) * ((a_2, h_2) * (a_3, h_3)) &= (a_1, h_1) * (a_2 + a_3, h_2h_3)\\ &= (a_1 - a_2 - a_3, h_1h_2h_3)\\ &= (a_1 - a_2, h_1h_2) * (a_3, h_3)\\ &= ((a_1, h_1) * (a_2, h_2)) * (a_3, h_3)\end{aligned}$$

- *Fall 3* $(h_1, h_2) \in N \times H \setminus N$. Dann gilt $h_1h_2 \in H \setminus N$ und wir rechnen nach:

$$\begin{aligned}(a_1, h_1) * ((a_2, h_2) * (a_3, h_3)) &= (a_1, h_1) * ((a_2 - a_3, h_2h_3))\\ &= (a_1 + a_2 - a_3, h_1h_2h_3)\\ &= (a_1 + a_2, h_1h_2) * (a_3, h_3)\\ &= ((a_1, h_1) * (a_2, h_2)) * (a_3, h_3).\end{aligned}$$

- *Fall 3* $(h_1, h_2) \in H \setminus N \times H \setminus N$. Dann gilt $h_1 h_2 \in N$ und wir rechnen nach:

$$\begin{aligned}(a_1, h_1) * ((a_2, h_2) * (a_3, h_3)) &= (a_1, h_1) * ((a_2 - a_3, h_2 h_3)) \\ &= (a_1 - a_2 + a_3, h_1 h_2 h_3) \\ &= (a_1 - a_2, h_1 h_2) * (a_3, h_3) \\ &= ((a_1, h_1) * (a_2, h_2)) * (a_3, h_3).\end{aligned}$$

In jedem der vier Fälle gilt also das Assoziativgesetz. Die Verknüpfung $*$, wie in der Aufgabenstellung definiert, ist also assoziativ. Im Folgenden ist laut Aufgabenstellung als gegeben anzunehmen, dass $A \times H$ mit der Verknüpfung $*$ eine Gruppe mit Neutralelement $(0_A, 1_H)$ ist. Zu zeigen ist, dass falls $h \in H \setminus N$ Element der Ordnung 2 ist, also $h^2 = e_H$ gilt, dann hat für beliebiges $a \in A$ das Element $(a, h) \in A \times H$ die Ordnung 2. Da $h \in H \setminus N$, ist $[h] = hN \neq N$. Sei $a \in A$ beliebig. Es gilt $(a, h) * (a, h) = (a - a, h^2) = (0_A, 1_H)$. Da $h \neq 1_H$, da $1_H \in N$, aber $h \notin N$, ist $(a, h) \neq (0_A, 1_H)$. Daher gilt nicht nur $\mathrm{ord}((a, h))|2$, sondern sogar $\mathrm{ord}((a, h)) = 2$. Als konkrete Anwendung geben wir explizit eine Gruppe der Ordnung $42 = 6 \cdot 7 = 2 \cdot 21$ an, die kein Element der Ordnung 6 oder 14 enthält. Setze $A = \mathbb{Z}/21\mathbb{Z}$ und $H = \{\pm 1\}$. Eindeutiger Normalteiler ist $\{1\}^{\triangleleft} \neq H$, der auch Index 2 hat. Es gilt, dass $A \times H$, ausgestattet mit der Verknüpfung $*$, Gruppe der Ordnung $|A \times H| = |A||H| = 21 \cdot 2 = 42$ ist. Sei nun $(a, h) \in A \times H$ vorgegeben.

- *Fall 1* $h = -1$. Dann gilt $h \in H \setminus N$. Nach dem vorangegangenen Teil hat dann $(a, -1)$ für beliebiges $a \in A$ die Ordnung 2.

- *Fall 2* $h = 1$. Dann gilt $h \in N$. Wir finden also für $n \in \mathbb{N}$ beliebig und beliebiges $a \in A$, dass $(a, 1)^n = (na, 1^n) = (na, 1)$. Damit folgt $\mathrm{ord}_{A \times N}((a, 1)) = \mathrm{ord}_A(a)$. Da $\mathrm{ord}_A(a)||A| = 21$, ist nur $a \in \{1, 3, 7, 21\}$ möglich.

Insgesamt hat die angegebene Gruppe nur Elemente der Ordnung $1, 2, 3, 7, 21$, und keine der Ordnung 6 oder 14. □

**Aufgabe 37** Zu zeigen ist, dass kein Ringhomomorphismus $\phi : \mathbb{Q} \to \mathbb{Z}$ existiert. Angenommen, es gäbe einen Ringhomomorphismus $\phi : \mathbb{Q} \to \mathbb{Z}$. Dann gilt $\phi(1_\mathbb{Q}) = 1_\mathbb{Z}$. Wir behaupten $\phi(n \cdot 1_\mathbb{Q}) = n$ für alle $n \in \mathbb{Z}$. Für $n = 1$ ist das klar nach Definition des Ringhomomorphismus. Für $n = -1$ finden wir $\phi(-1_\mathbb{Q}) + \phi(1_\mathbb{Q}) = -\phi(1_\mathbb{Q}) + \phi(1_\mathbb{Q}) = -1_\mathbb{Z} + 1_\mathbb{Z} = 0_\mathbb{Z}$, so dass $\phi(-1_\mathbb{Q}) = -\phi(1_\mathbb{Q}) = -1_\mathbb{Z}$. Da $\phi$auf $(\mathbb{Q}, +), (\mathbb{Z}, +)$ Gruppenhomomorphismus zwischen abelschen Gruppen ist, gilt insbesondere $\phi(0_\mathbb{Q}) = \phi(0_\mathbb{Z})$. Sei nun $n \in \mathbb{N}$ beliebig und nimm an, dass $\phi(n \cdot 1_\mathbb{Q}) = n \cdot 1_\mathbb{Z} = n$. Dann gilt $\phi((n+1) \cdot 1_\mathbb{Q}) = \phi(n \cdot 1_\mathbb{Q} + 1_\mathbb{Q}) = \phi(n \cdot 1_\mathbb{Q}) + \phi(1_\mathbb{Q}) = n \cdot 1_\mathbb{Z} + 1_\mathbb{Z} = (n+1) \cdot 1_\mathbb{Z} = n + 1$. Nach dem Induktionsprinzip gilt die Aussage also für beliebige $n \in \mathbb{N}$. Wegen $\phi(-n) + \phi(n) = \phi((-n) \cdot 1_\mathbb{Q} + n \cdot 1_\mathbb{Q}) = \phi(0_\mathbb{Q}) = 0_\mathbb{Z}$ finden wir nun $\phi(-n) = -\phi(n) = -n$ für alle $n \in \mathbb{N}$. Insgesamt haben wir also bisher gezeigt $\phi(n \cdot 1_\mathbb{Q}) = n \cdot 1_\mathbb{Z}$ für $n \in \mathbb{Z}$. Sei nun $q \in \mathbb{Q} \setminus \mathbb{Z}$. Da insbesondere $q \neq 0$, gibt es $m \in \mathbb{Z} \setminus \{0\}$ und $n \in \mathbb{N}$, so dass $\phi(q) = m\phi(1/n)$ mit analoger Argumentation zu oben für $\phi(1/n) \in \mathbb{Z}$ anstelle von $1_\mathbb{Z}$. Setze nun $n > 1$ voraus. Wir setzen nun $m = n$, betrachten also $= m/n = n/n = 1$. Dann finden wir $n \cdot \phi(1/n) = 1_\mathbb{Z}$. Die Gleichung bedeutet, dass $n > 1$ eine Einheit in $\mathbb{Z}$ ist. Andererseits ist aus der

Vorlesung bekannt, dass $\mathbb{Z}^\times = \{\pm 1\}$. Wegen $n > 1$ gilt aber $n \neq -1$ und $n \neq +1$, also $n \notin \mathbb{Z}^\times$. Das ist ein Widerspruch zur Annahme, es existierte ein Ringhomomorphismus $\phi : \mathbb{Q} \to \mathbb{Z}$. Damit war die Annahme falsch, und es existiert kein solcher Ringhomomorphismus. □

**Aufgabe 38 (F13T3A3)** Sei $R$ ein endlicher Integritätsbereich. Zu zeigen ist, dass $R$ dann bereits Körper ist. Aus der Vorlesung ist bekannt, dass für jedes $r \in R$ dann infolge Endlichkeit gilt, dass $r$ Einheit oder Nullteiler ist. Da $R$ Integritätsbereich, können wir das Vorlesungsresultat anwenden, dass Einheiten in $R$ keine Nullteiler sind und dass ebenso Nullteiler keine Einheiten sind. Für endliche Integritätsbereiche $R$ gilt dann $R^\times = R \setminus \{0_R\}$. Das bedeutet aber gerade, dass $R$ Körper ist. □

**Aufgabe 39** Sei $R$ ein endlicher Ring, d.h., $n := |R| < \infty$. Sei $r \in R$ beliebig. Zu zeigen ist, dass $r$ Nullteiler oder Einheit ist. Sei $k \in \mathbb{N}$ beliebig. Wir behaupten, dass $M = \{r^k | k \in \mathbb{N}\}$ Teilmenge von $R$ ist, also insbesondere gilt $|M| \leq n < \infty$. Da $R$ Ring ist, gilt insbesondere für $r \in R$, $r^2 = r \cdot r \in R$. Durch Induktion sieht man leicht $r^k \in R$ für beliebiges $k \in \mathbb{N}_0$. Damit gilt für alle $x \in M$, dass $x \in R$, also $M \subseteq R$. Insbesondere ist dann $|M| \leq |R| = n < \infty$. Also gibt es $K \in \mathbb{N}$ so dass gilt $r^K = r$. Andernfalls wären alle Elemente $r^k$, d.h., für alle $k \in \mathbb{N}$, paarweise verschieden, im Widerspruch zur Endlichkeit von $M$. Die obenstehende Gleichung ist nun äquivalent zu $(r^{K-1} - 1_R) \cdot r = 0_R$. Dann gilt entweder $r^{K-1} - 1_R \neq 0_R$ oder $r^{K-1} - 1_R = 0_R$. Im ersten Fall ist $r$ ein Nullteiler, denn wir haben das von $0_R$ verschiedene Ringelement $s := r^{K-1} - 1_R$ gefunden, so dass $s \cdot r = 0_R$. Im zweiten Fall gilt $r^{K-2} \cdot r = r^{K-1} = 1_R$. Da $1_R \in R^\times$ einziges Element der Ordnung 1 in der Einheitengruppe des Rings ist, können wir uns auf den Fall $K \geq 3$ beschränken. Dann gilt $r \in R^\times$, denn $t := r^{K-2}$ erfüllt die Gleichung $t \cdot r = 1_R = r \cdot t$. Damit ist gezeigt, dass für einen endlichen Ring beliebiges $r \in R$ Einheit oder Nullteiler ist.□

**Aufgabe 40** *Bemerkung:* Sei $R = \mathbb{Z}[\sqrt{-d}]$ mit $d \in \mathbb{N}$. Für beliebiges $\alpha \in R \setminus \{0\}$ gilt $|R/(\alpha)|N(\alpha)$, wobei $N : R \to \mathbb{N}$ die Norm-Funktion bezeichnet.
Zu bestimmen ist die Mächtigkeit von $\mathbb{Z}[i]/(2+i)$. Wir zeigen, $|\mathbb{Z}[i]/(2+i)| = 5$. Wir behaupten, dass $\mathcal{R} = \{0, 1, 2, 3, 4\}$ ein Repräsentanten-System des Faktor-Rings ist. Hierzu ist zu zeigen, dass für jedes $r \in \mathcal{R}$ ein $l \in \mathcal{R}$ existiert, sodass $r - l \in (2+i)$. Das ist äquivalent dazu, dass jede Nebenklasse mindestens einen Repräsentanten aus $\mathcal{R}$ enthält. Zunächst beobachten wir, dass wegen $2 + i \in (2+i)$ gilt $-2 + (2+i) = i + (2+i)$. Sei nun $r \in \mathbb{Z}[i]$ beliebig vorgegeben. Dann gilt $r = \alpha + \beta i$ mit $\alpha, \beta \in \mathbb{Z}$. Da $R$ euklidischer Ring ist, finden wir $p, q \in R$, so dass $r = p(2+i) + q$ gilt, wobei $0 \leq N(q) < N(2+i)$ nach dem Euklidischen Algorithmus gilt. Da $0 \leq N(q) < N(2+i) = 5$, gilt also $N(q) \in \{0, 1, 2, 3, 4\}$. Damit finden wir $r + (2+i) = q + (2+i)$, da $2 + i + (2+i) = 0 + (2+i)$. Nun gilt für obiges $q \in \mathbb{Z}[i]$ beliebig $q = q_1 + iq_2$ mit $q_1^2 + q_2^2 \leq 4$. Wir behaupten, dass es nun möglich ist, $q_2 = 0$ zu wählen. Nämlich $q + (2+i) = q_1 + iq_2 + (2+i) = (q_1 - 2\cot q_2) + (2+i)$. Wegen $N(2+i) = (2-i) \cdot (2+i) \in (2+i)$können wir uns hier auf den Fall beschränken, dass $0 \leq (q_1 - 2q_2) \leq 4$, wobei wir den Euklidischen Algorithmus wiederum verwenden, aber nun in $\mathbb{Z}$: Ist $q_1 - 2_q 2 \geq 5$ oder $q_1 - 2q_2 \leq 0$, dann finden finden wir nach dem

Euklidischen Algorithmus in $\mathbb{Z}$ ein $l \in \{0,1,2,3,4\}$, so dass $5|(q_1-2q_2-l)$. Dann gilt $q_1-2q_2+(2+i) = l+(2+i)$. Da die Elemente von $\mathcal{R}$ gerade die Form $l \in \{0,1,2,3,4\}$ haben, haben wir gezeigt, dass für beliebiges $r \in \mathcal{R}$ gilt $r+(2+i) = l+(2+i)$ für ein $l \in \mathcal{R}$. Damit gilt $r - l \in (2+i)$, also enthält eine beliebige Nebenklasse $r + (2+i)$ mindestens ein $l \in \mathcal{R}$. Wir müssen nun noch zeigen, dass für zwei beliebige $l, l' \in \mathcal{R}$ gilt: $l - l' \in (2+i) \Rightarrow l = l'$. Seien dazu $l, l' \in \mathcal{R}$ beliebig vorgegeben und ohne Beschränkung der Allgemeinheit dürfen wir annehmen, dass $l \geq l'$. Aus $l-l' \in (2+i)$ folgt, dass es ein $x \in R$ gibt, so dass $(l-l') = x\cot(2+i)$. Angenommen, $l \neq l'$. Dann ist $x \neq 0$. Nun gilt für alle $x \in R \setminus \{0\}$, dass $N(x) \in \mathbb{N}$ also echt positiv ist. Also $N(l-l') = N(x(2+i)) = N(x)N(2+i) \geq N(2+i) = 5$. Da $l, l' \in \{0,1,2,3,4\}$ und $l, l'$ folgt $0 \leq l-l' \leq 4$ und ebenso $0 \leq N(l-l') \leq 4$ im Widerspruch zu $N(l-l') \geq 5$! Damit ist die Annahme, $l \neq l'$ also falsch gewesen und es gilt $l = l'$. Mithin enthält jede Nebenklasse also genau ein $l \in \mathcal{R}$. Damit ist der Nachweis der Repräsentanten-System-Eigenschaft abgeschlossen. Wegen $|\mathbb{Z}[i]/(2+i)| = |\mathcal{R}| = |\{0,1,2,3,4\}| = 5$ folgt die Behauptung. □

**Aufgabe 41** Sei $K$ Körper und $R = K[x,y]$ und $I = (x-y-1)$ Ideal in $R$. Zu zeigen ist $R/I = \{f + I | f \in K[x]\} =: M$. "$\supseteq$": Das ist klar nach Definition, denn ein beliebiges $f \in K[x]$ erfüllt auch $f \in K[x,y]$. Der Faktorring $R/I$ enthält nun gerade Elemente der Form $g + I$ wobei $g \in K[x,y]$ beliebig. Insbesondere enthält er ebenfalls $f + I$. "$\subseteq$": Sei $\bar{f} \in R/I$ beliebig. Dann gibt es ein $f \in R$, so dass $f$ Urbild von $\bar{f}$ unter dem Kanonischen Epimorphismus $\pi : R \to R/I$ ist. Wir zeigen zuerst per Induktion, dass für beliebiges $k \in \mathbb{N}$ gilt $\overline{y^k} = \overline{(x-1)^k}$ in $R/I$. Für $k = 1$ gilt nämlich $\overline{y} = y + (x-y-1) = y + [x-y-1] + (x-y-1) = x - 1 + (x-y-1) = \overline{x-1}$. Sei nun $k \in \mathbb{N}$ beliebig aber fest. Wir nehmen an, dass $\overline{y^k} = \overline{(x-1)^k}$. Zu zeigen ist nun, dass dann auch $\overline{y^{k+1}} = \overline{(x-1)^{k+1}}$. In der Tat $\overline{y^{k+1}} = \overline{y^k} \cdot \overline{y} = \left(y^k + (x-y-1)\right)(y + (x-y-1)) = ((x-1)^k + (x-y-1))(x-1+(x-y-1)) = \overline{(x-1)^k}\overline{x-1} = \overline{(x-1)^{k+1}}$ nach Induktionsvoraussetzung und -anfang im dritten Schritt und den Rechenregeln in Faktorringen im ersten und letzten Schritt. Damit ist die Hilfsbehauptung bewiesen. Das $f$ vom Anfang des Beweises hat die Form

$$f(x,y) = \sum_{k=0}^{n} \sum_{l=0}^{m} a_{kl} x^k y^l, \tag{65}$$

wobei $a_{kl} \in K$ für alle $0 \leq k \leq n, 0 \leq l \leq m$. Wir finden nun

$$\begin{aligned}
\overline{f} &= \overline{\sum_{k=0}^{n}\sum_{l=0}^{m} a_{kl}x^k y^l} \\
&= \sum_{k=0}^{n}\sum_{l=0}^{m} \overline{a_{kl}x^k y^l} \\
&= \sum_{k=0}^{n}\sum_{l=0}^{m} \overline{a_{kl}}\,\overline{x^k y^l} \\
&= \sum_{k=0}^{n}\sum_{l=0}^{m} \overline{a_{kl}}\,\overline{x^k (x-1)^l} \\
&= \sum_{q=0}^{m+n} \overline{b_q x^q} \\
&= \overline{\sum_{q=0}^{m+n} b_q x^q},
\end{aligned}$$

wobei mit $X_q(K) \equiv \{(k,l) \in \mathbb{N}_0^2 | 0 \leq k \leq n, 0 \leq l \leq K, k+l = q\}$

$$b_q \equiv \sum_{K=0}^{m} \sum_{(k,l)\in X_q(K)} a_{kl} \left( \begin{array}{c} K \\ l \end{array} \right) (-1)^{K-l} \tag{66}$$

nach dem Binomi'schen Lehrsatz gesetzt wurde. In der obenstehenden rechten Gleichung ist $\tilde{f} \equiv \sum_{q=0}^{m+n} b_q x^q \in K[x]$, also $\tilde{f} + I = \overline{\sum_{q=0}^{m+n} b_q x^q} \in M$. Damit ist $R/I \subseteq M$ nachgewiesen. □

**Aufgabe 42** Zu zeigen ist, dass $\mathbb{Z}[i]/(2+i) \simeq \mathbb{Z}/5\mathbb{Z}$. Hierzu definieren wir die Abbildungen $\phi : \mathbb{Z}[i] \to \mathbb{Z}/5\mathbb{Z}, (x+iy) \mapsto (x-2y) \bmod(5)$. Es ist klar, dass für $z_1, z_2 \in \mathbb{Z}[i]$ gilt $\phi(z_1+z_2) = \phi(z_1)+\phi(z_2)$. Ferner gilt $\phi(1_{\mathbb{Z}[i]}) = 1-2\cdot 0 = 1 = 1_{\mathbb{Z}/5\mathbb{Z}}$. Ferner gilt für $z_1, z_2 \in \mathbb{Z}[i]$ der Form $z_1 = x_1+iy_1, z_2 = x_2+iy_2$ mit $x_1, x_2, y_1, y_2 \in \mathbb{Z}$, dass $z_1 z_2 = (x_1x_2 - y_1y_2) + i(x_1y_2 + x_2y_1)$. Nun $\phi(z_1z_2) = x_1x_2 - y_1y_2 - 2(x_1y_2 + x_2y_1)$ und $\phi(z_1)\phi(z_2) = (x_1-2y_1)(x_2-2y_2) = x_1x_2 + 4y_1y_2 - 2(x_1y_2+x_2y_1) = x_1x_2 - y_1y_2 - 2(x_1y_2 + x_2y_1)$ in $\mathbb{Z}/5\mathbb{Z}$, da für alle $y_1, y_2 \in \mathbb{Z}$ gilt $4y_1y_2 \equiv -y_1y_2 \bmod(5)$. Mithin haben wir einen Ringhomomorphismus gefunden. Da $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\} = \mathbb{Z}/5\mathbb{Z}$ finden wir unter dem Kanonischen Epimorphismus $\pi : \mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$ zu jedem $\bar{x} \in \mathbb{Z}/5\mathbb{Z}$ ein $x \in \mathbb{Z}$,so dass $\pi(x) = \bar{x}$. Da insbesondere $\mathbb{Z} \subset \mathbb{Z}[i]$ Teilring, ist $x \in \mathbb{Z}[i]$. Beliebigkeit von $\bar{x} \in \mathbb{Z}/5\mathbb{Z}$ impliziert nun die Surjektivität von $\phi$. Wir haben nun gefunden, dass $\phi$ ein surjektiver Ringhomomorphismus ist. Der Homomorphiesatz für Ringe liefert nun den Isomorphismus $\mathbb{Z}[i]/\ker\phi \simeq \mathbb{Z}/5\mathbb{Z}$. Zu zeigen verbleibt lediglich $(2+i) = \ker\phi$. Um zu zeigen, dass $(2+i) \in \ker\phi$ langt es wegen der Idealeigenschaft von Kernen von Ringhomomorphismen $2+i \in \ker\phi$ zu zeigen. Es gilt in der Tat $\phi(2+i) = 2 - 2\cdot 1 = 2-2 = 0$, also $2+i \in \ker\phi$. Damit folgt $(2+i) \subseteq \ker\phi$ als Teilideal. Wir müssen noch $\ker\phi \subset (2+i)$ zeigen. Sei also $z = x+iy \in \ker\phi$ beliebig. Dann gilt $x - 2y = 0 \bmod(5)$. Damit gibt es

ein $k \in \mathbb{Z}$, sodass $x - 2y = 5k \Leftrightarrow x = 5k + 2y$. Also gilt $z = 5k + 2y + iy$. Nun gilt $2y + iy = y \cdot (2 + i) \in (2 + i)$ und $5k = (2 - i)k \cdot (2 + i) \in (2 + i)$. Also ist auch $z = 5k + 2y + iy = (2k + y - ik) \cdot (2 + i) \in (2 + i)$. Damit ist gezeigt, dass $z \in \ker \phi$ $z \in (2 + i)$ impliziert. Beliebigkeit von $z \in \ker \phi$ liefert also $\ker \phi \subseteq (2 + i)$. Im Ergebnis gilt also $\ker \phi = (2 + i)$. Insgesamt finden wir also $\mathbb{Z}[i]/\ker \phi = \mathbb{Z}[i]/(2 + i) \simeq \mathbb{Z}/5\mathbb{Z}$. □

**Aufgabe 43** Zu zeigen ist, dass (a) $\mathbb{Z}[x]$ und (b) $K[x, y]$ für einen Körper $K$ jeweils keine Hauptidealringe sind. Zu (a): Angenommen, $\mathbb{Z}[x]$ wäre Hauptidealring. Dann gibt es zu jedem Ideal $I$ in $\mathbb{Z}[x]$ ein $\alpha \in \mathbb{Z}[x]$, so dass $I = (\alpha)$. Betrachte nun das Ideal $(2, x) \subset \mathbb{Z}[x]$. Angenommen, es gäbe $\alpha \in \mathbb{Z}[x]$, so dass $(\alpha) = (2, x)$. Dann gilt $2 \in (\alpha)$ und $x \in (\alpha)$. Also gibt es $p, q \in \mathbb{Z}[x]$, so dass $2 = \alpha \cdot p$ und $x = \alpha \cdot q$. Da $\mathbb{Z}[x]$ euklidischer Ring mit der Gradfunktion als Höhenfunktion, gilt $\deg(2) = \deg(\alpha p) = \deg(\alpha) \deg(p)$ und $\deg(x) = \deg(\alpha \cdot q) = \deg(\alpha) \deg(q)$. Aus der letzten Aussage folgt $\deg(\alpha) = 1 = \deg(x)$, da 1 die einzige positive Einheit in $\mathbb{Z}$. Also gilt $\alpha = ax + b$ mit $a, b \in \mathbb{Z}$ und $a \neq 0$. Andererseits ist $0 = \deg(2)$, weswegen wegen $\deg \alpha = 1 \neq 0$, auch $\deg p = 0$. Also gibt es ein $c \in \mathbb{Z}$, so dass $2 = \alpha \cdot c$. Da $\mathbb{Z}[x]$ Integritätsbereich, scheidet, wegen $\alpha \neq 0$ aus Gradgründen, auch $c = 0$ aus. Also gilt $c \neq 0$. Dann gilt $\alpha \cdot c = ac \cdot x + b \cdot c$. Das ist aber wegen $a, c \neq 0$ ein Polynom ersten Grades! Widerspruch zur Annahme, es existiere ein $\alpha$ mit der gewünschten Eigenschaft. Da $(2, x)$ kein von einer ein-elementigen Menge erzeugtes Ideal ist, ist $\mathbb{Z}[x]$ kein Hauptidealring. Zu (b) Angenommen, $K[x, y]$ wäre Hauptidealring. Dann gibt es zu jeden Ideal $I$ ein $\alpha \in K[x, y]$, so dass $I = (\alpha)$. Betrachte das Ideal $I = (x, y) \neq (0)$. Also $\alpha \neq 0$. Da $K[x, y]$ laut Annahme Hauptidealring, gibt es ein $\alpha \in K[x, y]$ sodass $(x, y) = (\alpha)$. Also gibt es $p_x, p_y \in K[x, y]$ so dass $p_x \cdot \alpha = x$ und $p_y \cdot \alpha = y$. Es gilt auch $yp_x\alpha = xy = xp_y\alpha$ und durch Umformen finden wir $(xp_y - yp_x)\alpha = 0$. Da $\alpha \neq 0$ muss $xp_y = yp_x$, sonst Widerspruch zur Eigenschaft von $K[x, y]$, Integritätsbereich zu sein. Expansion von $p_x, p_y$, d.h., Einsetze von $p_x = \sum_{k_x=0}^{n_x} \sum_{l_x=0}^{m_x} a_{k_x l_x} x^{k_x} y^{k_x}$ und $p_y = \sum_{k_y=0}^{n_y} \sum_{l_y=0}^{m_y} b_{k_y l_y} x^{k_y} y^{k_y}$ mit $a_{k_x l_x}, b_{k_y l_y} \in K$ für alle $k_x, l_x, k_y, l_y$ liefert nun nach Koeffizienten-Vergleich in der jeweils niedrigsten Ordnung in $x^k y^l$ $x = 0$ und $y = 0$ also $x = y$, was im Widerspruch zu $x \neq y$ für den multivariaten Polynomring $K[x, y]$ steht. □

**Aufgabe 44** Wir zeigen, dass $\mathbb{Q}[x, y]/(x - 1, y^2 - 2)$ ein Körper ist. Wir beweisen zunächst die Hilfsbehauptung $Q[x, y]/(x - 1, y^2 - 2) \simeq \mathbb{Q}[y]/(y^2 - 2)$. Betrachte dazu die Abbildung $\phi : \mathbb{Q}[x, y] \to \mathbb{Q}[y]/(y^2 - 2), f(x, y) \mapsto f(1, y) \bmod (y^2 - 2)$. Als Komposition von Einsetzungshomorphismus für $y \to 1$ und kanonischem Epimorphismus $\mathbb{Q}[y] \to \mathbb{Q}[y]/(y^2 - 2)$ ist $\phi$ Homomorphismus. Da der Einsetzungshomomorphismus $x \to 1$ surjektiv ist und der kanonische Epimorphismus $\mathbb{Q}[y] \to \mathbb{Q}[y]/(y^2 - 2)$ ebenfalls surjektiv ist, ist auch $\phi$ als Komposition zweier surjektiver Ringhomomorphismen surjektiv. Nach dem Homomorphiesatz für Ring gilt also $\mathbb{Q}[x, y]/\ker \phi \simeq \mathbb{Q}[y]/(y^2 - 2)$. Zu zeigen ist nun $\ker \phi = (x - 1, y^2 - 2)$. "$\supseteq$": Es reicht zu zeigen, dass $x - 1, y^2 - 2 \in \ker \phi$. Einerseits gilt $\phi(x - 1) = (1 - 1) \bmod (y^2 - 2) = 0 \bmod (y^2 - 2)$, andererseits gilt $\phi(y^2 - 2) = (y^2 - 2) \bmod (y^2 - 2) = 0 \bmod (y^2 - 2)$, also ist $x - 1, y^2 - 2 \in \ker \phi$. Da der Kern eines Ringhomomorphismus stets Ideal ist, gilt auch $(x - 1, y^2 - 2) \subseteq \ker \phi$ infolge der Minimalitätseigenschaft von $(x - 1, y^2 - 2)$

das kleinste Ideal zu sein, das $x-1$ und $y^2-2$ enthält. "$\subseteq$": Um zu zeigen, dass $\ker\phi \subseteq (x-1, y^2-2)$, sei $f \in \ker\phi$ vorgegeben. Es gilt $f = \sum_{k=0}^{n}\sum_{l=0}^{m} a_{kl}x^k y^l$ mit $a_{kl} \in \mathbb{Q}$ für alle $0 \leq k \leq n, 0 \leq l \leq m$. Aus $f \in \ker\phi$ folgt $f(1,y) = 0 \bmod (y^2-2)$, also $f(1,y) = p(y)(y^2-2)$ mit einem Polynom $p \in \mathbb{Q}[y] \subseteq \mathbb{Q}[x,y]$. Andererseits gilt

$$\begin{aligned}
f(x,y) &= f(x,y) - f(1,y) + f(1,y) \\
&= \left[\sum_{k=0}^{n}\sum_{l=0}^{m} a_{kl}x^k y^l - \sum_{k=0}^{n}\sum_{l=0}^{m} a_{kl}1^k y^l\right] + p(y)(y^2-2) \\
&= \sum_{k=1}^{n}\sum_{l=0}^{m} a_{kl}(x^k-1)y^l + p(y)(y^2-2) \\
&= \left(\sum_{k=1}^{n}\sum_{l=0}^{m} a_{kl}\left(\sum_{s=0}^{k-1} x^s\right)y^l\right)(x-1) + p(y)(y^2-2) \\
&= q(x,y)(x-1) + p(y)(y^2-2),
\end{aligned}$$

wobei die Teleskopsumme für $k \in \mathbb{N}$

$$x^k - 1 = (x-1)\sum_{l=0}^{k-1} x^k \tag{67}$$

verwendet und $q(x,y) \equiv \sum_{k=1}^{n}\sum_{l=0}^{m} a_{kl}\left(\sum_{s=0}^{k-1} x^s\right)y^l$ gesetzt wurde. Da $q, p \in \mathbb{Q}[x,y]$ ist also $f \in \ker\phi$ von der Form $f = q\cdot(x-1) + p\cdot(y^2-2)$. Wegen $(x-1, y^2-2) = \{r\cdot(x-1) + s\cdot(y^2-2) | r, s \in \mathbb{Q}[x,y]\}$, folgt $f \in (x-1, y^2-2)$, wie zu zeigen war. Die Beliebigkeit von $f \in \ker\phi$ liefert nun $\ker\phi \subseteq (x-1, y^2-2)$. Insgesamt finden wir also $\ker\phi = (x-1, y^2-2)$. Damit ist die eingangs aufgestellte Behauptung bewiesen, denn $\mathbb{Q}[x,y]/(x-1, y^2-2)\mathbb{Q}[x,y]/\ker\phi \simeq \mathbb{Q}[y]/(y^2-2)$. Zu zeigen ist nur noch, dass $\mathbb{Q}[y]/(y^2-2)$ Körper ist. Reduktion modulo 3 liefert zunächst, dass $y^2-2$ in $\mathbb{Q}[y]$ irreduzibel ist. Für das ganzzahliges Polynom reicht es Irreduzibilität in $\mathbb{Z}[x]$ zu zeigen. Diese ist leicht eingesehen, denn $\overline{y^2-2} = \bar{y}^2 + \bar{1} \in \mathbb{Z}/3\mathbb{Z}[x]$ hat keine Nullstellen, $\bar{0}^2 + \bar{1} = \bar{1} \neq \bar{0}$, $\bar{1}^2 + \bar{1} = 2 \neq \bar{0}$ und $\bar{2}^2 + \bar{1} = \bar{5} = \bar{2} \neq \bar{0}$. Als Polynom vom Grad 2 ist somit $\bar{y}^2 + \bar{1}$ in $\mathbb{Z}/3\mathbb{Z}[x]$ irreduzibel, nach dem Reduktionskriterium also $y^2-2$ in $\mathbb{Z}[x]$ und nach einem aus der Vorlesung bekannten Satz also auch im Polynomring $\mathbb{Q}[x]$ über dem Quotientenkörper $\mathbb{Q}$ von $\mathbb{Z}$ als faktoriellem Ring. Da $\mathbb{Q}$ Körper, ist $\mathbb{Q}[x]$ Hauptidealring und die Irreduzibilität von $y^2-2$ über $\mathbb{Q}$ ist äquivalent dazu, dass $(y^2-2)$ maximales Ideal in $\mathbb{Q}[y]$. Damit ist laut Vorlesung $\mathbb{Q}[y]/(y^2-2)$ ein Körper. Damit ist wiederum der zu $\mathbb{Q}[y]/(y^2-2)$ isomorphe Faktorring $\mathbb{Q}[x,y]/(x-1, y^2-2)$ ein Körper. □

**Aufgabe 45** Sei $K$ ein Körper und $R = K[x]$, $f \in R$ Polynom vom Grad $n \geq 1$. Zu zeigen ist, dass $M := \{g \in R | g = 0 \,\text{oder}\, g \neq 0, \deg(g) < \deg f\}$ ein Repräsentantensystem des Faktorrings $R/(f)$ ist. Sei $p \in K[x]$ Polynom und $p+I$ die dazugehörige Nebenklasse. Zu zeigen ist $p+I$ enthält genau ein Element aus $M$. Zunächst zeigen wir, dass $p+I$ mindestens ein Element aus $M$ enthält.

- *Fall 1:* $0 \leq \deg p < \deg f$. Dann ist $p \in p+I$ und nach Definition von $M$ ebenfalls $p \in M$. Somit enthält $p+I$ ein Element aus $M$, nämlich $p$ selbst.

- *Fall 2:* $\deg p \geq \deg f$. Da $K$ Körper, ist $K[x]$ mit der Gradfunktion deg euklidischen Ring. Wegen $\deg f > 0$ gibt es also $q, r \in K[x]$, so dass $p = qf + r$, wobei $\deg r < \deg f$. Nun gilt $qf \in (f) = I$, also $p + I = r + I$. Da $r \in K[x]$ Polynom vom Grad $< \deg f = n$, ist $r \in M$. Damit enthält $p + I$ auch in diesem Fall ein Element aus $M$, nämlich $r$.

Insgesamt ist somit gezeigt, dass in jedem Fall $p + I$ für beliebiges $p \in K[x]$ ein Element aus $M$ enthält. Wir müssen nun zeigen, dass $p + I$ auch nur höchstens ein Element aus $M$ enthält. Angenommen, $r_1, r_2 \in M$ sind verschieden aber $p + I \ni r_1, r_2$. Dann gibt es Polynome $q_1, q_2 \in K[x]$, so dass $p + q_1 f = r_1$ und $p + q_2 f = r_2$. Das können wir umformen zu $p = r_1 - q_1 f$. Damit finden wir $r_1 - q_1 f + q_2 f = r_2$ bzw. $r_1 - r_2 = (q_1 - q_2)f$ also $r_1 - r_2 \in (f)$. Falls $r_1 - r_2 = 0 \in (f)$, haben wir einen Widerspruch dazu, dass $r_1, \neq r_2$ laut Annahme. Falls $r_1 - r_2 \neq 0$ aber $r_1 - r_2 \in (f)$, dann gibt es ein Polynom $0 \neq \chi \in K[x]$, sodass $r_1 - r_2 = \chi f$. Da $K$ Körper ist, gilt insbesondere $n > \deg(r_1 - r_2) = \deg f + \deg \chi \geq n$. Das ist ebenfalls ein Widerspruch. Insgesamt war also die Annahme falsch, und es gilt $r_1 = r_2$. Damit ist gezeigt, dass jede Nebenklasse $p + I \in R/I$ höchstens ein Element aus $M$ enthält. Zusammen mit dem ersten Teil haben wir also gezeigt, dass jede Nebenklasse genau ein Element aus $M$ beinhaltet. □

**Aufgabe 46** Zu bestimmen ist die Anzahl der Elemente im Faktorring $\mathbb{F}_2[x, y]/(y-1, x^3+x+1)$. Wir behaupten $|\mathbb{F}_2[x, y]/(y-1, x^3+x+1)| = 8$. Der Beweis verläuft in zwei Schritten. Zuerst zeigen wir, dass $\mathbb{F}_2[x, y]/(y_1, x^3 + x + 1) \simeq \mathbb{F}_2[x]/(x^3 + x + 1)$ und dann wenden wir die Aussage von Aufgabe 45 auf den Faktorring des univariaten Polynomrings an. Für den ersten Schritt verwenden wir den Homomorphiesatz: Wir erinnern uns an den Einsetzungshomomorphismus $\phi : \mathbb{F}_2[x, y] \to \mathbb{F}[x], f(x, y) \mapsto f(x, 1)$. Er ist surjektiv. Wir erinnern uns ferner an den kanonischen Epimorphismus $\pi : \mathbb{F}_2[x] \to \mathbb{F}_2[x]/(x^3 + x + 1), f \mapsto \bar{f} = f \bmod (x^3 + x + 1)$. Dieser ist ebenfalls surjektiv. Als Komposition zweier surjektiver Ringhomomorphismen ist $\psi : \mathbb{F}_2[x, y] \to \mathbb{F}_2[x]/(x^3 + x + 1), f \mapsto (\pi \circ \phi)(f)$ ebenfalls surjektiver Ringhomomorphismus. Der Homomorphiesatz für Ringe liefert uns nun, die Isomorphie $\mathbb{F}_2[x, y]/\ker \psi = \mathbb{F}_2[x]/(x^3 + x + 1)$. Es verbleibt also zu zeigen, dass $\ker \phi = (y - 1, x^3 + x + 1)$. "$\supseteq$": Da Kerne von Ringhomomorphismen stets Ideale sind und $(y-1, x^3+x+1)$ das kleinste Ideal in $\mathbb{F}_2[x, y]$ ist, das $y-1$ und $x^3+x+1$ enthält, langt es zu zeigen, $y-1, x^3+x+1 \in \ker \psi$. Da $\phi(y-1) = 0$ bereits in $\mathbb{F}_2[x]$, folgt $\psi(x - 1) = 0$ aus der Homomorphismus-Eigenschaft des kanonischen Epimorphismus. Da $\pi(x^3+x+1) = (x^3+x+1) = 0_{\mathbb{F}_2[x]/(x^3+x+1)}$ und $\phi(x^3+x+1) = x^3+x+1$, ist $\psi(x^3 + x + 1) = 0_{\mathbb{F}_2[x]/(x^3+x+1)}$. Also gilt auch $x^3 + x + 1 \in \ker \psi$. Die Bemerkung am Anfang des Nachweises von "$\supseteq$" liefert nun $(y - 1, x^3 + x + 1) \subseteq \ker \psi$. "$\subseteq$". Um umgekehrt zu zeigen, dass $\ker \psi \subseteq (y - 1, x^3 + x + 1)$, sei $p \in \mathbb{F}_2[x, y]$ beliebig mit $p \in \ker \psi$. Dann gilt insbesondere $p(x, 1) = 0 \bmod (x^3 + x + 1)$. Also gibt es ein Polynom $q_1$ in $\mathbb{F}_2[x]$ mit der Eigenschaft, dass $p(x, 1) = q_1(x) \cdot (x^3 + x + 1)$. Nun berechnen wir analog zu Aufgabe 44, dass für $p(x, y) = \sum_{k=0}^{n} \sum_{l=0}^{m} a_{kl} x^k y^l$ mit

$a_{kl} \in \mathbb{F}_2$ für alle $0 \leq k \leq n$, $0 \leq l \leq m$

$$\begin{aligned}
p(x,y) &= (p(x,y) - p(x,1)) + p(x,1) \\
&= \left[\sum_{k=0}^{n}\sum_{l=0}^{m} a_{kl}x^k y^l - \sum_{k=0}^{n}\sum_{l=0}^{m} a_{kl}x^k 1^l\right] + q_1(x)(x^3+x+1) \\
&= \sum_{k=0}^{n}\sum_{l=1}^{m} a_{kl}(y^l - 1)x^k + q_1(x)(x^3+x+1) \\
&= \left(\sum_{k=0}^{n}\sum_{l=1}^{m} a_{kl}\left(\sum_{s=0}^{l-1} y^s\right)x^k\right)(y-1) + q_1(x)(x^3+x+1) \\
&= q_2(x,y)(y-1) + q_1(x)(x^3+x+1),
\end{aligned}$$

wobei die Teleskopsumme für $l \in \mathbb{N}$

$$y^k - 1 = (y-1)\sum_{l=0}^{k-1} y^k \tag{68}$$

verwendet und $q_2(x,y) \equiv \sum_{k=0}^{n}\sum_{l=1}^{m} a_{kl}\left(\sum_{s=0}^{l-1} y^s\right)x^k$ gesetzt wurde. Da $q_1, q_2 \in \mathbb{F}_2[x,y]$ und ferner $(y-1, x^3+x+1) = \{r_1\cdot(x^2+x+1)+r_2\cdot(y-1)|r_1, r_1 \in \mathbb{F}_2[x,y]\}$, folgt $p = q_2\cdot(y-1) + q_1\cdot(x^3+x+1) \in (y-1, x^3+x+1)$. Da $p \in \ker\psi$ als beliebig vorausgesetzt war, folgt $\ker\psi \subseteq (y-1, x^3+x+1)$. Im Ergebnis haben wir also $\ker\psi = (y-1, x^3+x+1)$ verifiziert. Nunmehr finden wir zusammen mit dem Resultat der Überlegungen auf Basis des Homomorphiesatzes für Ringe, $\mathbb{F}_2[x,y]/(x^3+x+1, y-1) = \mathbb{F}_2[x,y]/\ker\psi \simeq \mathbb{F}_2[x]/(x^3+x+1)$. Damit ist der erste Schritt abgeschlossen. Wir wenden nun Aufgabe 45 an. Es ist $\deg(x^3+x+1) = 3$ in $\mathbb{F}_2[x]$. Besagte Aufgabe liefert nun, dass ein Repräsentantensystem $M$ von $\mathbb{F}_2[x]/(x^3+x+1)$ gegeben ist durch

$$M = \{p \in \mathbb{F}_2[x] | p = 0 \,\text{oder}\, p \neq 0, \deg p < 3\}. \tag{69}$$

Da $p = \sum_{k=0}^{2} a_k x^k$ mit $a_0, a_1, a_2 \in \mathbb{F}_2$ zulässig ohne weitere Einschränkung ist, haben wir genau $|\mathbb{F}_2|^3 = 2^3 = 8$ Möglichkeiten, verschiedene $p \in M$ anzugeben. Insbesondere ist dann auch $\mathbb{F}_2[x]/(x^3+x+1)$ endlich und von Mächtigkeit $|M| = 8$. Infolge der Isomorphie $\mathbb{F}_2[x]/(x^3+x+1) \simeq \mathbb{F}_2[x,y]/(y-1, x^3+x+1)$ aus dem ersten Schritt ist also auch $\mathbb{F}_2[x,y]/(y-1, x^3+x+1)$ endlich und von Mächtigkeit $|M| = 8$. Damit ist die Behauptung bewiesen. □

**Aufgabe 47** Gesucht ist $\bar{37}^{-1}$ in $\mathbb{Z}/100\mathbb{Z}$. Hierzu berechnen wir im euklidischen Ring $(\mathbb{Z}, +, \cdot)$ mit Höhenfunktion $H : \mathbb{Z}\setminus\{0\} \to \mathbb{N}_0, x \mapsto |x|$ den größten gemeinsamen Teiler von $a = 37$ und $b = 100$ mittels erweitertem euklidischen Algorithmus. Dieser liefert uns dann $x, y \in \mathbb{Z}$, so dass $\mathrm{ggT}(37, 100) = 1 = x\cdot 100 + y\cdot 37$. Reduktion modulo 100 liefert dann in $\mathbb{Z}/100\mathbb{Z}$, $1 + 100\mathbb{Z} = (y + 100\mathbb{Z})(37 + 100\mathbb{Z})$, sodass

$\bar{y} = y + 100\mathbb{Z} = (37 + 100\mathbb{Z})^{-1} = \bar{37}^{-1}$.

| | | | |
|---|---|---|---|
| $-$ | 100 | 1 | 0 |
| $-$ | 37 | 0 | 1 |
| 2 | 26 | 1 | $-2$ |
| 1 | 11 | $-1$ | 3 |
| 2 | 4 | 3 | $-8$ |
| 2 | 3 | $-7$ | 19 |
| 1 | 1 | 10 | $-27$ |
| 3 | 0 | $-$ | $-$ |

Damit finden wir $100 \cdot (10) + (-27) \cdot 37 = 1000 - 999 = 1$, somit $x = 10$, $y = -27$. Damit finden wir $\bar{37}^{-1} = (37 + 100\mathbb{Z})^{-1} = (-27 + 100\mathbb{Z}) = (73 + 100\mathbb{Z}) = \bar{73}$. Das Inverse von $\bar{37}$ in $\mathbb{Z}/100\mathbb{Z}$ ist also $\bar{73}$. □

**Aufgabe 48** Zu zeigen ist, dass $\mathbb{Q}[x]/J$ mit $J = (x^3 - 7)$ ein Körper ist. Betrachte $R = \mathbb{Q}(\sqrt[3]{7})$. Dies ist der kleinste Körper, sodass $\mathbb{Q} \subseteq R$ und $\sqrt[3]{7} \in R$. Insbesondere ist $R$ auch ein Ring. Wir definieren die Abbildung $\Phi : \mathbb{Q}[x] \to \mathbb{Q}(\sqrt[3]{7}), f(x) \mapsto f(\sqrt[3]{7})$. $\Phi$ ist also gerade der Einsetzungshomomorphismus, wobei anstelle $x$ nun $\sqrt[3]{7} \in \mathbb{Q}(\sqrt[3]{7})$ als Argument von $f \in \mathbb{Q}[x]$ verwendet wird. Die Homomorphismeneigenschaft ist klar, für $f, g \in \mathbb{Q}[x]$ folgt $f + g \in \mathbb{Q}[x]$ und mit $\mathbb{Q}, \{\sqrt[3]{7}\} \subset \mathbb{Q}(\sqrt[3]{7})$ folgt auch $f(\sqrt[3]{7}), g([3]7) \in \mathbb{Q}(\sqrt[3]{7})$. Ist $f = \sum_{k=0}^{\deg f} a_k x^k$, $g = \sum_{k=0}^{\deg g} b_k x^k$, so gilt

$$\Phi(f) = \sum_{k=0}^{\deg f} a_k (\sqrt[3]{7})^k \, , \, \Phi(g) = \sum_{k=0}^{\deg g} b_k (\sqrt[3]{7})^k.$$

ObdA $\deg f \leq \deg g$, sonst vertausche Rollen von $f, g$, und setze $a_{\deg f + 1} = ... = a_{\deg g} = 0$. Dann gilt

$$f = \sum_{k=0}^{\deg g} a_k x^k \, , g = \sum_{k=0}^{\deg g} b_k x^k \, , \, f + g = \sum_{k=0}^{\deg g} (a_k + b_k) x^k$$

$$\Phi(f) = \sum_{k=0}^{\deg g} a_k (\sqrt[3]{7})^k \, , \, \Phi(g) = \sum_{k=0}^{\deg g} b_k (\sqrt[3]{7})^k \, , \, \Phi(f+g) = \sum_{k=0}^{\deg g} (a_k + b_k)(\sqrt[3]{7})^k.$$

Damit sehen wir durch Umordnung einer endlichen Summe in $\mathbb{Q}(\sqrt[3]{7})$, dass in der Tat $\Phi(f + g) = \Phi(f) + \Phi(g)$. Ferner gilt $\Phi(1) = 1$ trivialerweise. Für $f, g \in \mathbb{Q}[x]$ wie oben gilt

$$f \cdot g = \sum_{k=0}^{\deg f \deg g} c_k x^k,$$

wobei $c_k = \sum_{l=0}^{k} a_l b_{k-l}$ mit $a_{\deg f+1} = ... = a_{\deg f \deg g} = 0 = b_{\deg g+1} = ... = b_{\deg f+\deg g}$. Nun gilt

$$\begin{aligned}
\Phi(f) &= \sum_{k=0}^{\deg f} a_k(\sqrt[3]{7})^k\,,\ \Phi(g) = \sum_{k=0}^{\deg g} b_k(\sqrt[3]{7})^k \\
\Rightarrow \Phi(f)\cdot\Phi(g) &= \left(\sum_{k=0}^{\deg f} a_k(\sqrt[3]{7})^k\right)\left(\sum_{k=0}^{\deg g} b_k(\sqrt[3]{7})^k\right) \\
&= \sum_{k=0}^{\deg f}\sum_{l=0}^{\deg g} a_k b_l(\sqrt[3]{7})^k(\sqrt[3]{7})^l \\
&= \sum_{k=0}^{\deg f \deg g}\left(\sum_{l=0}^{k} a_l b_{k-l}\right)(\sqrt[3]{7})^k \\
&= \sum_{k=0}^{\deg f \deg g} c_k(\sqrt[3]{7})^k \\
&= \Phi(f\cdot g)
\end{aligned}$$

Damit haben wir insgesamt die Ring-Homomorphismus-Eigenschaft nachgerechnet. Zur Surjektivität. Da $\sqrt[3]{7}^3 = 7$ und $x^3-7$ nach Eisenstein zu $p=7$ irreduzibel ist, ist $x^3-7$ Minimalpolynom von $\sqrt[3]{7}$. Also ist $[\mathbb{Q}(\sqrt[3]{7}):\mathbb{Q}] = 3$ und jedes $y \in \mathbb{Q}(\sqrt[3]{7})$ von der Form $y = q_1+q_2\sqrt[3]{7}+q_3\sqrt[3]{7}^2$ mit $q_1,q_2,q_3 \in \mathbb{Q}$. Das Polynom $p_y := q_1+q_2x+q_3x^2$ erfüllt nun $\Phi(p_y) = q_1+q_2\sqrt[3]{7}+q_3\sqrt[3]{7}^2 = y$. Beliebigkeit von $y$ impliziert nun die Surjektivität von $\Phi$. Damit ist $\Phi$ also ein surjektiver Ring-Homomorphismus und der Homomorphiesatz für Ringe liefert den Isomorphismus

$$\bar{\Phi} : \mathbb{Q}[x]/\ker\Phi \to \mathbb{Q}(\sqrt[3]{7}). \tag{70}$$

Es bleibt zu zeigen, $\ker\Phi = (x^3-7)$. Da $(x^3-7)$ Hauptideal, also insbesondere endlich erzeugt, ist, reicht es für $(x^3-7) \subseteq \ker\Phi$ nachzuweisen, dass $x^3-7 \in \ker\Phi$. Da $\sqrt[3]{7}^3 = 7 \leftrightarrow \sqrt[3]{7}^3-7 = 0$ ist in der Tat $\Phi(x^3-7) = 0$, also $x^3-7 \in \ker\Phi$. Die Idealeigenschaft von Kernen von Ringhomomorphismen zusammen mit der Minimalitätseigenschaft von $(x^3-7)$ liefert nun $(x^3-7) \subseteq \ker\Phi$. Für die Umkehrung sei $f \in \ker\Phi$ vorgegeben. Dann gilt $\Phi(f) = 0$ bzw. $f(\sqrt[3]{7}) = 0$. Also ist $\sqrt[3]{7}$ eine Nullstelle des Polynoms $f$. Da $x^3-7$ Minimalpolynom von $\sqrt[3]{7}$, gilt $x^3-7|f$. Also gibt es ein $g \in \mathbb{Q}[x]$, sodass $f = g\cdot(x^3-7)$. Damit folgt aber $f \in (x^3-7) = \{p\cdot(x^3-7)|p \in \mathbb{Q}[x]\}$. Beliebigkeit von $f \in \ker\Phi$ liefert nun $\ker\Phi \subseteq (x^3-7)$. Damit ist gezeigt, dass $\ker\Phi = (x^3-7)$ und wir haben insgesamt die Isomorphie

$$\mathbb{Q}[x]/(x^3-7) \simeq \mathbb{Q}(\sqrt[3]{7}) \tag{71}$$

bewiesen. Da $\mathbb{Q}[x]/(x^3-7)$ Urbild eines Körpers unter einem injektiven Ringhomomorphismus, ist $\mathbb{Q}[x]/(x^3-7)$ selbst Körper. □

**Aufgabe 49** Sei $R = \mathbb{Q}[x]$ und $J$ das Ideal $J = (x^2+x+1)$. Gesucht ist die Menge der Kehrwerte von $2x+3+J$ in $R/J$. Als Hauptidealring ist $R$ insbesondere

faktoriell. Es ist $x^2+x+1 \in \mathbb{Q}[x]$ irreduzibel, wie man durch Reduktion zu $p=2$ einsieht. Da $R$ faktorieller Ring ist, ist $(x^2+x+1)$ Primideal in $R$. Da $R$ sogar Hauptidealring, ist $J=(x^2+x+1)$ insbesondere maximales Ideal. Laut eines Satzes aus der Vorlesung folgt daraus, dass der Faktorring $R/J$ sogar ein Körper ist. Da $0 \leq \deg(2x+3)=1<\deg(x^2+x+1)=2$ und $2x+3 \neq 0$, ist $\overline{2x+3} \neq \bar{0}$ in $R/J$, wegen der Körpereigenschaft gilt also $\overline{2x+3} \in (R/J)^\times$, so dass es zu $\overline{2x+3}$ genau ein $\bar{f} \in R/J$ gibt, sodass $\bar{f}$ Kehrwert zu $\overline{2x+3}$ in $R/J$. Wir bestimmen dieses durch Verwendung der weiteren Eigenschaft von $\mathbb{Q}[x]$ zusammen mit der Grad-Funktion $\deg : \mathbb{Q}[x] \setminus \{0\} \to \mathbb{N}, f \mapsto \deg f$ euklidischer Ring zu sein, mit deg als Höhenfunktion. Für beliebiges $\bar{f} \in R/J$ gibt esnämlich ein $f \in \mathbb{Q}[x]$ sodass $\bar{f}=f+J$. In $\mathbb{Q}[x]$ können wir $q=\mathrm{ggT}(2x+3, x^2+x+1)$ bestimmen indem wir den Euklidischen Algorithmus anwenden. Dieser liefert zudem Koeffizienten $f,g \in \mathbb{Q}[x]$, so dass $\mathrm{ggT}(2x+3, x^2+x^2+1) = f\cdot(2x+3)+g\cdot(x^2+x+1)$. Die Irreduzibilität von $f$ und die Beobachtung, dass, wegen $\deg(2x+3) < \deg(x^2+x+1)$, auch $x^2+x^2+1 \not| 2x+3$, liefern nun $\mathrm{ggT}(2x+3, x^2+x+1)=1$, was das multiplikative Neutralelement in $R$ ist. Insofern finden wir $1=f\cdot(2x+3)+g\cdot(x^2+x+1)$. Reduktion modulo $x^2+x+1$ liefert dann zusammen mit den Rechenregeln für Faktorringe $\bar{1} = (f+\mathrm{mod}(J))(2x+3+\mathrm{mod}(J)) = \bar{f}\cdot\overline{x^2+x+1}$, da $\overline{x^2+x+1} = \bar{0}$ und $\bar{g}\cdot\bar{0}=\bar{0}$. Also ist das über den Euklidischen Algorithmus gefundene $f$ Repräsentant von $\bar{f}=(\overline{2x+3})^{-1}$ und es gilt $\bar{f}=f+J$, wie gewünscht. Zur Bestimmung von $f$:

| | | | |
|---|---|---|---|
| $-$ | $x^2+x+1$ | $1$ | $0$ |
| $-$ | $2x+3$ | $0$ | $1$ |
| $x/2-1/4$ | $7/4$ | $1$ | $-x/2+1/4$ |
| $(7/4)^{-1}(2x+3)$ | $0$ | $-$ | $-$ |

Damit finden wir $7/4=(-x/2+1/4)(2x+3)+1\cdot(x^2+x+1)$, also $1=(-2x/7+1/7)(2x+3)+4/7\cdot(x^2+x+1)$. Reduktion modulo $J$ liefert nun wegen $x^2+x+1+J = 0+J$, $1+J=(-2x/7+1/7+J)(2x+3+J)$. Damit ist $f=-2x/7+1/7 \in \mathbb{Q}[x]$ ein Polynom mit den oben beschriebenen Eigenschaften. Insbesondere gilt für alle $h \in f+J$, dass $h\cdot(2x+3) \equiv 1 \,\mathrm{mod}(J)$. Der gesuchte Kehrwert von $2x+3+J$ in $R/J$ ist also $-2/7x+1/7+J$. □

**Aufgabe 50** Sei $R=\mathbb{Z}[x]/(2,x^2+x+1)$. Gesucht ist ein Inverses $g$ in $\mathbb{Z}[x]$, sodass $g+(2,x^2+x+1)$ invers zu $3x+5+(x^2+x+1)$ in $R$ ist. Wir definieren hierfür zuerst die folgende Abbildung

$$\Phi : \mathbb{Z}[x] \to \mathbb{F}_2[x]/(x^2+x+1), f \mapsto \bar{f}, \tag{72}$$

wobei $\bar{f}$ die jeweilige Restklasse vom Polynom $f$ nach Reduktion der Koeffizienten modulo 2 bzgl. des Ideals $(x^2+x+1)$ ist. Mit anderen Worten, $\Phi$ ist die Komposition des surjektiven Reduktionshomomorphismus $\mathrm{mod}(2) : \mathbb{Z}[x] \to \mathbb{F}_2[x]$ und dem kanonischen Epimorphismus $\pi : \mathbb{F}_2[x]/(x^2+x+1)$. Da es sich bei beiden Abbildungen laut Vorlesung um surjektive Ringhomomorphismen handelt ist auch $\Phi = \pi \circ \mathrm{mod}(2)$ ein surjektiver Ringhomomorphismus. Der Homomorphiesatz in der Formulierung für Ringe liefert nun die Isomorphie $\mathbb{Z}[x]/\ker\Phi \simeq \mathbb{F}_2[x]/(x^2+x+1)$ von Ringen, denn $\mathbb{F}_2=\mathbb{Z}/2\mathbb{Z}$ und die Menge rechts ist ein endlicher Integritätsbereich,

also bereits Körper. Wir zeigen nun noch, dass $J := (2, x^2 + x + 1) = \ker \Phi$. Da $J$ von der endlichen Menge $S := \{2, x^2 + x + 1\} \subset J \subset \mathbb{Z}[x]$ erzeugt wird, reicht es, zu zeigen, $2 \in \ker \Phi, x^2 + x + 1 + \in \ker \Phi$. Dann ist zumindest die Inklusion $(2, x^2+x+1) \subset \ker \Phi$ infolge der Minimalitätseigenschaft von $J = (S)$ nachgewiesen. $2 \in \ker \Phi$ ist klar, denn $2 \in \ker \mathrm{mod}(2)$ und infolge der Homorphismuseigenschaft von $\pi$ gilt $\Phi(2) = \pi(\bar{0}) = \bar{0}$. Für $x^2 + x + 1$ gilt $x^2 + x + 1 \equiv x^2 + x + 1 \,\mathrm{mod}(2)$, sodass $\Phi(x^2 + x + 1) = \pi(\bar{x}^2 + \bar{x} + \bar{1}) = \bar{0}$, da $x^2 + x + 1 \in (x^2 + x + 1)$. Um zu zeigen, dass $\ker \Phi \subseteq J$, sei $f \in \ker \Phi$ beliebig vorgegeben. $f \in \ker \Phi$ liefert $\Phi(f) = 0$, also $\bar{f} = 0 \,\mathrm{mod}(\bar{x}^2 + \bar{x} + \bar{1})$. Daher gilt $\bar{x}^2 + \bar{x} + \bar{1} | \bar{f}$ in $\mathbb{F}_2[x]$. Also gibt es ein $g \in \mathbb{F}_2[x]$, sodass $\bar{f} = (\bar{x}^2 + \bar{x} + \bar{1})\bar{g}$. Da $\mathbb{F}_2[x] \simeq \mathbb{Z}[x]/(2)$ vermöge des Reduktionshomomorphismus laut Vorlesung, ist letztgenannte Gleichung gleichbedeutend mit $f + (2) = (x^2 + x + 1 + (2))(g + (2)) = (x^2 + x + 1)g + (2)$, wo $g \in \mathbb{Z}[x]$ mit der Eigenschaft $g + (2) = \bar{g}$ in $\mathbb{Z}[x]/(2) \simeq \mathbb{F}_2[x]$ gewählt sei. Aus der Gleichung in $\mathbb{Z}[x]/(2)$ folgt $2|[f - (x^2 + x + 1) \cdot g]$ in $\mathbb{Z}[x]$. D.h., es gibt $h \in \mathbb{Z}[x]$ sodass $2 \cdot h = f - g \cdot (x^2 + x + 1)$ bzw. $f = g \cdot (x^2 + x + 1) + h \cdot 2$. Wegen $J = (2, x^2 + x + 1) = \{g_1 \cdot 2 + g_2 \cdot (x^2 + x + 1) | g_1, g_2 \in \mathbb{Z}[x]\}$, haben wir also die Implikation $f \in \ker \Phi \Rightarrow f \in J$ verifiziert. Initiale Beliebigkeit von $f$ liefert nun $\ker \Phi \subseteq J$. Insgesamt haben wir somit $J = \ker \Phi$ und wir erhalten in der Tat den Isomorphismus

$$\mathbb{Z}[x]/J \simeq \mathbb{F}_2[x]/(x^2 + x + 1), \tag{73}$$

bezeichnet mit $\bar{\Phi}$. Nun nehmen wir das Polynom $p = 3x + 5$ und wenden $\bar{\Phi}$ auf dieses an: Das liefert uns zunächst $\bar{\Phi}(3x + 5) = \bar{x} + \bar{1} + (\bar{x}^2 + \bar{x} + \bar{1})$. Wir bestimmen nun zunächst ein Inverses dieses Elements mittels Euklidischem Algorithmus in $\mathbb{F}_2[x]/(x^2 + x + 1)$. Dieser ist anwendbar, da $\mathbb{F}_2[x]$ als Polynomring über einem Körper insbesondere Euklidisch ist, mit Höhenfunktion gegeben durch die Grad-Funktion. Hierzu beachten, wir dass $\bar{x}^2 + \bar{x} + \bar{1}$ durch Einsetzen als nullstellenfrei, wegen $\deg(\bar{x}^2 + \bar{x} + \bar{1}) = 2$ und Normiertheit also al irreduzibel befunden wird (in $\mathbb{F}_2[x]$). Wegen Normierheit und $\deg(\bar{x} + \bar{1}) = 1$ ist $\bar{x} + \bar{1}$ ebenfalls in $\mathbb{F}_2[x]$ irreduzibel. Insbesondere gilt dann $\mathrm{ggT}(\bar{x} + \bar{1}, \bar{x}^2 + \bar{x} + \bar{1}) = \bar{1}$. Der Euklidische Algorithmus, angewendet im Polynomring $\mathbb{F}_2[x]$,lieferte uns nun $\bar{f}, \bar{g} \in \mathbb{F}_2[x]$, sodass $f \cdot (\bar{x} + \bar{1}) + g \cdot (\bar{x}^2 + \bar{x} + \bar{1}) = \bar{1}$. In der Tat finden wir bereits durch bloßes Inspizieren der Polynome $(\bar{x}) \cdot (\bar{x} + \bar{1}) + \bar{1} \cdot (\bar{x} + \bar{x} + \bar{1}) = \bar{1}$. Damit gilt modulo $(\bar{x}^2 + \bar{x} + \bar{1}) =: I$, dass $\bar{1} + I = (\bar{x} + I)(\bar{x} + \bar{1} + I)$, also $(\bar{x} + I) = (\bar{x} + \bar{1} + I)^{-1}$ in $\mathbb{F}_2[x]/I$. Wegen $\mathrm{ggT}(2, x^2 + x + 1) = 1$ in $\mathbb{Z}[x]$ gilt also $(x + J) = (x + 1 + J)^{-1}$ bzw. $1 + J = (x + J)(x + 1 + J)$ in $R/J$. Insbesondere gilt für $3x + 5 = x + 1 + 2 \cdot x + 2 \cdot 2 \in x + 1 + J$ also $3x + 5 + (2, x^2 + x + 1) = x + 1 + (2, x^2 + x + 1)$, dass $x + J$ ebenfalls Inverses zu $3x + 5 + (x^2 + x + 1) \subseteq 3x + 5 + J$ in $R$ ist. □

**Aufgabe 51 (F14T3A2)** Gegeben sei ein kommutativer Ring $R$. Für $a, b, c, d \in R$ schreiben wir $a \equiv b \,\mathrm{mod}(c)$ genau dann wenn $a - b = c \cdot d$.
(a) Wir zeigen, dass es sich hierbei um eine Äquivalenzrelation handelt. Die Relationseigenschaft ist hierbei klar. Sei $c \in R$ beliebig aber fest vorgegeben und $a.b \in R$beliebig. Wir zeigen zunächst Reflexitvität. Es gilt $a - a = a + (-a) = 0_R$. Da in einem Ring stets $0_R \cdot c = 0_R$ gilt, liefert die Kommutativität $a \equiv a \,\mathrm{mod}(c)$ denn $a - a = c \cdot 0_R$. Wir zeigen Symmetrie. Es gilt $a - b = -b + a = -(b - a)$. Sei

$a \equiv b \bmod(c)$ vorausgesetzt. Dann gibt es nun $d \in R$, so dass $a - b = c \cdot d$, so gilt $b-a = -(a-b) = -c \cdot d = c \cdot (-d)$. $-d \in R$ liefert nun $b \equiv a \bmod(c)$. Für die Umkehrung vertausche man ein einfach die Rollen von $a$ und $b$ und verfahre analog. Für die Trantivität seien $a_1, a_2, a_3 \in R$ vorgegeben, so dass $a_1 \equiv a_2 \bmod(c)$, $a_2 \equiv a_3 \bmod(c)$. Zu zeigen ist $a_1 \equiv a_3 \bmod(c)$. Wegen $a_1 \equiv a_2 \bmod(c)$ finden wir zunächst ein $d_1 \in R$, so dass $a_1 - a_2 = c \cdot d_1$. Analog finden wir infolge $a_2 \equiv a_3 \bmod(c)$ ein $d_2 \in R$, sodass $a_2 - a_3 = c \cdot d_2$. Addition liefert nun $a_1 - a_3 = (a_1 - a_2) + (a_2 - a_3) = c \cdot d_1 + c \cdot d_2 = d_1 \cdot c + d_2 \cdot c = (d_1 + d_2) \cdot c$. Wegen $d_1 + d_2 \in R$ gilt also $a_1 \equiv a_3 \bmod(c)$. Damit ist die Relation $\bmod(c)$ für beliebiges $c \in R$ eine Äquivalenzrelation.
(b) Im Spezialfall $R = \mathbb{Z}$ sind nun alle Lösungen $y \in R$ der Kongruenz $51y = 34 \bmod(85)$ gesucht. Da $51 = 3 \cdot 17$ und $85 = 5 \cdot 17$ sind 51 und 85 nicht teilerfremd. Wir sehen, dass sogar $\mathrm{ggT}(34, 85, 51) = 17$. Nach den Rechenregeln für Kongruenzen können wir also äquivalent vereinfachen $3y = 2 \bmod(5)$. Da 3 und 5 teilerfremd sind, suchen wir nach Lösungen des Kongruenzensystems $z = 2 \bmod(5)$ und $z = 0 \, textmod(3)$. Wir sehen leicht, dass dann $y = z/3$ eine Lösung der Ausgangskongruenz ist und umgekehrt jedes $y \in \mathbb{Z}$, das die Ausgangskongruenz löst, vermöge $z = 3y$ eine Lösung der simultanen Kongruenz für $z$ ist. Da gilt $\mathrm{ggT}(5, 3) = 1$ (beides Primzahlen) und ferner $2 \cdot 5 + (-3) \cdot 3 = 1$, finden wir, dass $10 = 0 \bmod(5)$ und $10 = 1 \bmod(3)$ sowie $-9 = 1 \bmod(5)$ und $-9 = 0 \bmod(3)$. Damit sind alle $z \in 2 \cdot (-9) + 15\mathbb{Z} = 12 + 15\mathbb{Z}$ Lösungen der simultanen Kongruenz. Umgekehrt liefert der chinesische Restsatz den Ring-Isomorphismus $\Phi : \mathbb{Z}/15\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, (x + 15\mathbb{Z}) \to (x + 5\mathbb{Z}, x + 3\mathbb{Z})$. Dieser Isomorphismus ist insbesondere injektiv, so dass es genau eine $x+15\mathbb{Z}$ gibt sodass $\Phi(x+15\mathbb{Z}) = (2+15\mathbb{Z}, 0+3\mathbb{Z})$. Da wir bereits wissen, dass $12+15\mathbb{Z}$ im Urbild von $(2+15\mathbb{Z}, 0+3\mathbb{Z})$ unter $\Phi$ liegt, folgt, dass wir so tatsächlich alle Lösungen des Kongruenzensystems gefunden haben. Entsprechend finden wir nach den obenstehenden Ausführungen wegen $y = z/3$, dass die Lösungen $y$ gegeben sind durch $y \in 4 + 5\mathbb{Z}$.
(c) Sei $R = \mathbb{Q}[x]$. Gesucht sind alle $f \in \mathbb{Q}[x]$ mit der Eigenschaft, dass $f \equiv 1 \bmod(x^2 + 1)$ und $f \equiv x \bmod(x^2 - 1)$. Wir halten zunächst fest, dass $\mathrm{ggT}(x^2 - 1, x^2 + 1) = 1$ in $\mathbb{Q}[x]$, denn $x^2 + 1$ ist, wie man durch Reduktion modulo 3 sieht, in $\mathbb{Q}[x]$ irreduzibel. Da $\mathbb{Q}[x]$ als Polynomring über dem Körper $\mathbb{Q}$ insbesondere Euklidischer Ring mit der Polynom-Grad-Funktion als Höhenfunktion ist, liefert uns der Euklidische Algorithmus $p, q \in \mathbb{Q}[x]$, so dass $1 = p \cdot (x^2 - 1) + q \cdot (x^2 + 1)$. Im Vorliegenden Fall liefert bereits Inpektion, dass $p = (-1/2)$ und $q = 1/2$ offenbar die gewünschte Eigenschaft haben. Somit finden wir, dass $-1/2 \cdot (x^2 - 1) \equiv 0 \bmod(x^2 - 1)$ und $-1/2 \cdot (x^2 - 1) \equiv 1 \bmod(x^2 + 1)$ erfüllt und ferner $1/2 \cdot (x^2 + 1) \equiv 1 \bmod(x^2 - 1)$ und $1/2 \cdot (x^2 + 1) \equiv 0 \bmod(x^2 + 1)$ gilt. Damit lösen $f \in \mathbb{Q}[x]$ von der Form $f \in -1/2 \cdot (x^2 - 1) \cdot 1 + x \cdot 1/2 \cdot (x^2 + 1) + 1/2 \cdot (-1/2) \cdot (x^2 + 1)(x^2 - 1)\mathbb{Q}[x] = 0.5x^3 - 0.5x^2 + 0.5x + 0.5 + (x^4 - 1)\mathbb{Q}[x]$ die Kongruenz. Bezeichnen wir die Lösungsmenge der simultanen Kongruenz mit $\mathcal{L}$, dann stellen wir fest, dass $0.5x^3 - 0.5x^2 + 0.5x + 0.5 + (x^4 - 1)\mathbb{Q}[x] \subseteq \mathcal{L}$. Für die Umkehrung verwenden wir den chinesischen Restklassensatz. Da $\mathrm{ggT}(x^2 - 1, x^2 + 1) = 0$ gilt $(x^2 - 1) + (x^2 + 1) = (1)$ (denn $1 \in (x^2 - 1) + (x^2 + 1)$ nach der obigen Rechnung), d.h., die beiden Ideale $(x^2 - 1), (x^2 + 1)$ sind relativ prim im $\mathbb{Q}[x]$. Der Chinesische Restsatz liefert nun

einen Isomorphismus

$$\Phi : \mathbb{Q}[x]/(x^4-1) \to \mathbb{Q}[x]/(x^2-1) \times \mathbb{Q}[x]/(x^2+1) \tag{74}$$
$$f + (x^4-1) \mapsto (f + (x^2-1), f + (x^2+1)). \tag{75}$$

Da wir bereits mit $0.5x^3 - 0.5x^2 + 0.5x + 0.5 + (x^4-1)$ ein Urbild von $(x + (x^2 - 1), 1 + (x^2+1))$ unter $\Phi$ gefunden haben, liefert die Injektität des Isomorphismus $\Phi$, dass wir in der Tat so alle Lösungen erhalten haben. Damit gilt also

$$\mathcal{L} = 0.5x^3 - 0.5x^2 + 0.5x + 0.5 + (x^4-1), \tag{76}$$

wie behauptet.
(d) Sei wieder $R = \mathbb{Z}$. Wir untersuchen, ob die Kongruenz $y^2 + 97y \equiv 3 \bmod(101)$ für $y \in \mathbb{Z}$ lösbar ist. Wir sehen, dass $\mathrm{ggT}(97, 101) = 1$, da $97, 101$ beides Primzahlen sind. Angenommen, es ist $y \in \mathbb{Z}$ Lösung der Kongruenz. Dann gilt $y^2 + 97y \equiv 3 \bmod(101)$ also auch $y^2 \equiv 3 \bmod(101 \cdot 97)$. Das bedeutet, dass 3 quadratischer Rest modulo $101 \cdot 97$ ist. Für das Jacobi-Symbol $\left(\frac{3}{97\cdot 101}\right)$ gilt also $\left(\frac{3}{97\cdot 101}\right) = +1$. Andererseits berechnen wir nach den Rechenregeln für das Jacobi-Symbol

$$\left(\frac{3}{97 \cdot 101}\right) = \left(\frac{3}{101}\right) \cdot \left(\frac{3}{97}\right) \tag{77}$$
$$\overset{(*)}{=} \left(\frac{101}{3}\right) \cdot \left(\frac{97}{3}\right) \tag{78}$$
$$\overset{(**)}{=} \left(\frac{2}{3}\right) \cdot \left(\frac{1}{3}\right) \tag{79}$$
$$\overset{(***)}{=} (-1) \cdot 1 \tag{80}$$
$$= -1 \tag{81}$$

wobei in $(*)$ das Quadratische Reziprozitätsgesetz verwendet wurde mit

$$\left(\frac{101}{3}\right)\left(\frac{3}{101}\right) = (-1)^{\frac{101-1}{2}}(-1)^{\frac{3-1}{2}} = -1 \tag{82}$$
$$\left(\frac{97}{3}\right)\left(\frac{97}{3}\right) = (-1)^{\frac{97-1}{2}}(-1)^{\frac{3-1}{2}} = -1, \tag{83}$$

wir in $(**)$ verwendet haben, dass für $(a \equiv b \bmod(n))$ gilt $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$, d.h., $101 = 2 + 99 = 2 + 33 \cdot 3$ und $97 = 32 \cdot 3 + 1$. In $(***)$ haben wir verwendet, dass 1 quadratischer Rest modulo 3 ist, denn es gilt $1^2 \equiv 1 \bmod(3)$. Ferner wurde verwendet, dass $\left(\frac{2}{3}\right) = (-1)^{(3-1)/2} = -1$ nach den Ergänzungssätzen zum Quadratischen Reziprozitätsgesetz. Insgesamt finden wir also, dass die Kongruenz nicht lösbar ist, denn $\left(\frac{3}{97\cdot 101}\right) = -1$ im Widerspruch zur notwendigen Bedingung $\left(\frac{3}{97\cdot 101}\right) = +1$. $\square$

**Aufgabe 52** Wir bestimmen bis auf Reihenfolge als Primfaktoren von $f = x^2 - 1 \in \mathbb{Q}[x]$. Zunächst stellen wir fest, dass für den Polynomring $\mathbb{Q}[x]$ gilt $(\mathbb{Q}[x])^\times = \mathbb{Q}^\times$. Da $\mathbb{Q}[x]$ als Ring über einem Körper Hauptidealring ist, und somit insbesondere auch faktorieller Ring ist ferner jedes irreduzible Element aus $\mathbb{Q}[x]$ Primelement.

Die Umkehrung gilt bereits, da $\mathbb{Q}[x]$ als Hauptidealring auch Integritätsbereich ist. Konkret sind also Polynome vom Grad 1 irreduzibel, d.h., Polynome der Form $\alpha x+\beta$, wobei $\alpha \in \mathbb{Q}^\times$ und $\beta \in \mathbb{Q}$. Da $f(1) = 0 = f(-1)$ ist zunächst $f$ reduzibel und hat die beiden rationalen Nullstellen $+1$ und $-1$. Für die Zerlegung in Primfaktoren machen wir also den Ansatz $p_1 := \alpha_1(x-1)$ und $p_2 = \alpha_2(x+1)$, wobei $\alpha_1, \alpha_2 \in \mathbb{Q}^\times$ Einheiten in $\mathbb{Q}$ und damit in $\mathbb{Q}[x]$ sind. Um zu erreichen, dass $f = p_1p_2$ stellen wir fest, dass diese Gleichung genau dann erfüllt wird, wenn gilt $\alpha_1\alpha_2 = 1 \in \mathbb{Q}^\times$. Wir setzen also $\alpha := \alpha_1$ und notieren $\alpha^{-1} := \alpha_2$ als inverses Element zu $\alpha$ in der Einheitengruppe $\mathbb{Q}^\times$. Da $x-1$ und $x+1$ jeweils die normierten Minimalpolynome von $+1, -1$ in $\mathbb{Q}$ sind, haben wir somit bereits alle Zerlegungen von $x^2-1$ in Primfaktoren in $\mathbb{Q}[x]$ gefunden. Setzen wir $p_\alpha := \alpha(x-1)$ und $q_\alpha := \alpha^{-1}(x+1)$ für $\alpha \in \mathbb{Q}^\times$, so finden wir $f = p_\alpha \cdot q_\alpha$ für beliebiges $\alpha \in \mathbb{Q}^\times$ bis auf Reihenfolge alle möglichen Zerlegungen von $f$ in Primfaktoren. □

**Aufgabe 53** Gesucht sind alle irreduziblen Polynome vom Grad 5 in $\mathbb{F}_2[x]$. Sei $p \in \mathbb{F}_2[x]$ ein beliebiges solches Polynom. Da $p$ irreduzibel und normiert ist, hat $p$ keine Nullstellen in $\mathbb{F}_2$. Sei $L|\mathbb{F}_2$ diejenige Körpererweiterung von $\mathbb{F}_2$, so dass $L$ Zerfällungskörper von $p$ ist. Es gilt insbesondere aufgrund der Irreduzibilität von $p$, dass $[L : \mathbb{F}_2] = \deg p = 5$, so dass $L$ als 5-dimensionaler Vektorraum über $\mathbb{F}_2$ aufgefasst werden kann. Als Vektorraum über einem endlichen Körper hat $L$ genau $2^5 = 32$ Elemente und ist als Körpererweiterung von $\mathbb{F}_2$ selbst ein endlicher Körper getreu dem Hautsatz über endliche Körper. Dieser liefert weiterhin, dass dann bereits gilt $L \simeq \mathbb{F}_{2^5}$ bis auf $\mathbb{F}_2$-Isomorphie. Der Körper $\mathbb{F}_{2^5} = \mathbb{F}_{32}$ seinerseits ist definiert als Zerfällungskörper des Polynoms $(x^{32} - x)$. Wir sehen, dass $x^{32} - x \in \mathbb{F}_2[x]$ und ferner gilt die Teleskopsummen-Identität

$$x^{32} - x = x(x-1)\left(\sum_{k=0}^{30} x^k\right). \tag{84}$$

Angenommen, es gäbe $\zeta \in \mathbb{F}_{32} \setminus \mathbb{F}_2$ sodass $[\mathbb{F}_2(\zeta) : \mathbb{F}_2] \neq 5$. Dann hat $\zeta$ ein Minimalpolynom vom Grad ungleich 5 aber größer als 1, da $\zeta \notin \mathbb{F}_2$. Es gibt einen Zwischenkörper der Erweiterung $\mathbb{F}_{32}|\mathbb{F}_2$,nämlich $\mathbb{F}_2(\zeta)$. Dann gilt laut Gradformel

$$5 = [\mathbb{F}_{32} : \mathbb{F}_2] = [\mathbb{F}_{32} : \mathbb{F}_2(\zeta)] \cdot [\mathbb{F}_2(\zeta) : \mathbb{F}_2]. \tag{85}$$

Das ist aber wegen $[\mathbb{F}_2(\zeta) : \mathbb{F}_2]|5$, 5 Primzahl und den Voraussetzungen an den Grad des Minimalpolynom von $\zeta$ nicht möglich. Also hat $\zeta \in \mathbb{F}_{32} \setminus \mathbb{F}_2$ ein Minimalpolynom vom Grad 5 über $\mathbb{F}_2$. Wir zerlegen nun $\mathbb{F}_{32} \setminus \mathbb{F}_2$ in die 6 Mengen $M_1, ..., M_6$, der Mächtigkeit 5, sodass $M_1, ..., M_6$ jeweils die Nullstellenmenge eines Polynoms $p_1, ..., p_6$ aus $\mathbb{F}_2[x]$ ist. Wir finden somit, dass es genau 6 irreduzible Polynome vom Grad 5 in $\mathbb{F}_2[x]$ gibt, nämlich die Elemente von $\{p \in \mathbb{F}_2[x] | \deg p > 1, p|(x^{32} - x) \text{ in } \mathbb{F}_2[x]\}$. □

**Aufgabe 54 (F16T1A4)** Sei $1 < D \in \mathbb{Z}$ und $R = \mathbb{Z}[\sqrt{-D}]$. Wir zeigen, dass $R^\times = \{\pm 1\}$. Wir stellen zuerst fest, dass $1 \in R^\times$ und wegen $(-1)(-1) = 1$ auch $-1 \in R^\times$. Also gilt $\{\pm 1\} \subseteq R^\times$. Sei nun $a + b\sqrt{-D}$ mit $a, b \in \mathbb{Z}$ in der Einheitengruppe von $R$. Nach Definition einer Einheit gibt es dann $c, d \in \mathbb{Z}$ sodass $c + d\sqrt{-D} \in R^\times$

und $(a+b\sqrt{-D})(c+d\sqrt{-D})=1$. Wegen der Multiplikativität der Normfunktion $N:\mathbb{Z}[\sqrt{-D}]\to\mathbb{Z}_0^+, a+b\sqrt{-D}\mapsto a^2+b^2D$ folgt $N(1)=N((a+b\sqrt{-D})(c+d\sqrt{-D}))=N((a+b\sqrt{-D}))N((c+d\sqrt{-D}))=(a^2+b^2D)(c^2+d^2D)$. Da beide Faktoren auf der rechten Seite Teiler von $+1$ sein müssen in $\mathbb{Z}$ und wegen $1<D\in\mathbb{Z}$ ferner positiv sind, muss gelten $a^2+b^2D=+1=c^2+c^2D$. Da $b\in\mathbb{Z}$ und $D>1$, muss $b=0=d$, da sonst $a^2+b^2D\geq D>1$ und, ebenso, $c^2+d^2D\geq D>1$ im Widerspruch zur Gleichheit zu 1. Also verbleiben nur $a^2=+1=c^2$ mit $a,c\in\mathbb{Z}$ und $a+b\sqrt{-D}\in R^\times$ generisch genügt $b=0$, ist also von der Form $a$ mit ganzzahligem $a$. In $\mathbb{C}$ sind die einzigen beiden Lösungen der Gleichung $a^2=1$ gegeben durch $a=\pm1\in\mathbb{Z}$. Somit finden wir, dass eine Einheit in $R$ die Form $+1$ oder $-1$ hat. Da die Einheit $a+b\sqrt{-D}\in R^\times$ als beliebig vorausgesetzt war, folgt nun auch $R^\times\subseteq\{\pm1\}$. Insgesamt gilt also $R^\times=\{\pm1\}$. Wir setzen nunmehr $D=13$ und betrachten $R=\mathbb{Z}[\sqrt{-D}]$. Wir zeigen als erstes, dass $2\in\mathbb{Z}[\sqrt{-D}]$ irreduzibel ist. Angenommen, 2 wäre reduzibel. Dann gibt es zwei Nicht-Einheiten $a+b\sqrt{-13}, c+d\sqrt{-13}$, sodass $2=(a+b\sqrt{-13})(c+d\sqrt{-13})$. Wir wenden die Normfunktion an,verwenden deren Multiplikativität und bekommen zuerst $N(2)=4=N(a+b\sqrt{-13})N(c+d\sqrt{-13})=(a^2+b^2\cdot13)(c^2+d^2\cdot13)$. Da $a+b\sqrt{-13}, c+d\sqrt{-13}\notin R^\times=\{\pm1\}$, ist $N(a+b\sqrt{-13}), N(c+d\sqrt{-13})>1$. Damit finden wir wegen $a^2+b^2\cdot13|4, c^2+13\cdot d^2|4$, dass nur $a^2+b^2\cdot13=2=c^2+d^2\cdot13$ möglich ist, sonst Widerspruch dazu dass $a+b\sqrt{-13}, c+d\sqrt{-13}$ beide Nicht-Einheiten von $R$ sind. Da $13>2$, kann nur $b=0, d=0$ gelten, d.h., $2=a^2$ und $2=b^2$. Das ist aber nicht möglich, da 2 kein Quadrat in $\mathbb{Z}$ ist. Folglich war die Annahme, 2 sei reduzibel in $R$, falsch und somit ist, da zusätzlich $2\notin R^\times$, 2 irreduzibel. Wir zeigen nun, dass auch $1+\sqrt{-13}$ in $R$ irreduzibel ist. Wir stellen wiederum fest, dass $1+\sqrt{-13}\notin R^\times$. Angenommen, $1+\sqrt{-13}$ wäre nicht irreduzibel. Da es sich bei dem in Rede stehenden Element von $R$ um eine Nicht-Einheit handelt, ist $1+\sqrt{-13}$ dann reduzibel. Es gibt also zwei Nicht-Einheiten $a+b\sqrt{-13}$ und $c+d\sqrt{-13}$ aus $R$, sodass $1+\sqrt{-13}=(a+b\sqrt{-13})(c+d\sqrt{-13})$. Anwendung der Normfunktion wie gehabt liefert uns nun $N(1+\sqrt{-13})=14=N(a+b\sqrt{-13})N(c+d\sqrt{-13})=(a^2+b^2\cdot13)(c^2+d^2\cdot13)$, wobei wir wiederum die Multiplikativität der Normfunktion verwendet haben. Da gilt $14=2\cdot7$ und die Elemente mit Normfunktion 1 gerade nach (a) zu den Einheiten von $R$ korrespondieren, liefert die Forderung $a+b\sqrt{-13}, c+d\sqrt{-13}\notin R^\times$, dass $a^2+b^2\cdot13=2$ und $c^2+d^2\cdot13=7$ bzw. $a^2+b^2\cdot13=7$ und $c^2+b^2\cdot13=2$. Aus Symmetriegründen beschränken wir uns auf den ersten Fall. Da $13>2$, $a,b\in\mathbb{Z}$ ist nur $b=0$ möglich. Da 2 aber kein Quadrat in $\mathbb{Z}$ ist, gibt es kein $a\in\mathbb{Z}$ sodass $a^2=2$. Folglich kann es gewünschte Dekomposition in Nicht-Einheiten nicht geben. Damit war die Annahme, $1+\sqrt{-13}$ wäre reduzibel falsch. Um einzusehen, dass 2 kein Primelement in $R$ ist, nehmen wir an, 2 wäre Primelement in $R$. Dann stellen wir fest, dass einerseits $14=2\cdot7$ andererseits $14=(1+\sqrt{-13})(1-\sqrt{-13})$. Wegen $N(2)=4\not|N(1+\sqrt{-13})=N(1-\sqrt{-13})=14$, ist 2 kein Teiler von $1+\sqrt{-13}$ und auch kein Teiler von $1-\sqrt{-13}$. Wegen $2|14$ haben wir den Widerspruch zur Annahme, 2 wäre Primelement. Also ist 2 kein Primelement. □

**Aufgabe 55 (F14T2A3 ohne c)** Gegeben sei $R=\{a+ib\sqrt{2}|a,b\in\mathbb{Z}\}\subseteq\mathbb{C}$. Wir zeigen zuerst, dass $R$ Teilring von $\mathbb{C}$ ist. Es ist offenbar $1\in R$, denn es gilt $1+i\sqrt{2}\cdot0\in R$. Für $\alpha,\beta\in R$ beliebig ist nun noch zu zeigen $\alpha-\beta\in R$ und

$\alpha \cdot \beta \in R$. Da $\alpha, \beta \in R$ gibt es $a, b, c, d \in \mathbb{Z}$ sodass $\alpha = a + ib\sqrt{2}$ und $\beta = c + id\sqrt{2}$. Nun gilt $\alpha - \beta = (a + ib\sqrt{2}) - (c + i\sqrt{2}d) = (a - c) + (b - d)\sqrt{2}i$. Da $\mathbb{Z}$ Ring ist, gilt $a - c, b - d \in \mathbb{Z}$. Smit ist $\alpha - \beta \in R$. Ferner finden wir $\alpha\beta = (a + ib\sqrt{2})(c + id\sqrt{2}) = (ac - 2bd) + i\sqrt{2}(ad + bc)$. Da mit $a, b, c, d \in \mathbb{Z}$ infolge der Ringeigenschaft von $\mathbb{Z}$, namentlich der Abgeschlossenheit bzgl. Multiplikation und Addition sowie $1 \in \mathbb{Z}$, auch $ab - 2cd \in \mathbb{Z}$ und $ad + bc \in \mathbb{Z}$ ist auch $\alpha\beta \in R$. Wir zeigen nun, dass $R$ zusammen mit $N : R \to \mathbb{N}_0, \alpha \mapsto \alpha\bar{\alpha}$ euklidischer Ring ist. Als Teilring des Körpers $\mathbb{C}$ ist $R$ zumindest Integritätsbereich. Ferner gilt für $\alpha \in R$ der Form $\alpha = a + ib\sqrt{2}$ mit $a, b \in \mathbb{Z}$, dass $N(\alpha) = (a + ib\sqrt{2})(a - ib\sqrt{2}) = a^2 + 2b^2 \in \mathbb{N}_0$ für alle $a, b \in \mathbb{Z}$. Zudem gilt $N(\alpha) = 0$ genau dann wenn $a = 0 = b$, also $\alpha = 0 \in R$. Damit ist $N : R \setminus \{0\} \to \mathbb{N}$. Seien nun $\alpha, \beta \in R$ von der Form $\alpha = a + ib\sqrt{2}$ und $\beta = c + id\sqrt{2}$ mit $a, b, c, d \in \mathbb{Z}$ vorgegeben, wobei $\beta \neq 0$. Zu zeigen ist, dass es $\sigma, \rho \in R$ gibt, sodass gilt $\alpha = \rho\beta + \sigma$ und $N(\sigma) < N(\beta)$. Wir rechnen zunächst in $\mathbb{Q}(i\sqrt{2})$, dass

$$\frac{\alpha}{\beta} = \frac{a + ib\sqrt{2}}{c + id\sqrt{2}} = \frac{(a + ib\sqrt{2})(c - id\sqrt{2})}{c^2 + 2d^2} = \frac{ac + 2db}{c^2 + 2d^2} + \frac{bc - ad}{c^2 + 2d^2} i\sqrt{2} \equiv r + si\sqrt{2}. \tag{86}$$

Nun wählen wir $r_0, s_0 \in \mathbb{Z}$ mit der Eigenschaft, dass $|r - r_0| \leq 0.5$ und $|s - s_0| \leq 0.5$. Definiere nunmehr $\rho := r_0 + is_0\sqrt{2}$. Dann gilt $N(\alpha\beta^{-1} - \rho) = N((r - r_0) + i\sqrt{2}(s - s_0)) = (r - r_0)^2 + 2(s - s_0)^2 \leq (0.5)^2 + 2 \cdot (0.5)^2 = 0.75 < 1$. Multiplikativität der Normfunktion, die als aus der Vorlesung bekannt vorausgesetzt wird, liefert nun mit $d(\beta) \neq 0$ wegen $\beta \neq 0$ nach Voraussetzung $N(\beta) > N(\alpha - \rho\beta)$. Wenn wir nun definieren $\sigma = \alpha - \beta\rho$, dann gilt somit $N(\sigma) = N(\alpha - \beta\rho) < N(\beta)$ und wegen der Teilringeigenschaft natürlich auch $\sigma = \alpha - \beta\rho \in R$. Damit ist der Nachweis der Höhenfunktionseigenschaft von $N$ abgeschlossen und zusammen damit, dass $R$ Integritätsbereich ist, ist der Nachweis, dass $R$ mit $N$ euklidischer Ring ist, abgeschlossen. □

**Aufgabe 56 (H12T3A5)** Gegeben sei das Polynom $f = x^5 - 7x^3 + 503x^2 + 12x - 2012 \in \mathbb{Q}[x]$. Gesucht ist eine Zerlegung in irreduzible Faktoren. Nach dem Satz von Gauss ist jede rationale Nullstelle von $f$ bereits ganzzahlig und Teiler von $-2012 = -4 \cdot 503$, da $f$ normiert ist und ganzzahlige Koeffizienten besitzt. Es gilt $f(1) = 5 - 7 + 503 - 12 - 2012 < 0, f(-1) = -1 + 7 + 503 - 12 - 2012 < 0$. Wir prüfen weiter $f(2) = 32 - 7 \cdot 8 + 503 \cdot 4 + 12 \cdot 2 - 2012 = 56 - 56 + 2012 - 2012 = 0$ und $f(-2) = -32 + 7 \cdot 8 + 503 \cdot 4 - 12 \cdot 2 - 2012 = -56 + 56 + 2012 - 2012 = 0$. Also hat $f$ zumindest die ganzzahligen Nullstellen $2 \,\&\, -2$. Damit $(x^2 - 4)|f$. Wir berechnen:

$$\begin{aligned}
\frac{x^5 - 7x^3 + 503x^2 + 12x - 2012}{x^2 - 4} &= \frac{x^3(x^2 - 4)}{x^2 - 4} + \frac{4x^3 - 7x^3 + 503x^2 + 12x - 2012}{x^2 - 4} \\
&= x^3 + \frac{(-3)x(x^2 - 4)}{x^2 - 4} + \frac{503 \cdot (x^2 - 4)}{x^2 - 4} \\
&= x^3 - 3x + 503
\end{aligned}$$

Damit finden wir $f = (x^2 - 4)(x^3 - 3x + 503)$. Da wir bereits eine Zerlegung von $x^2 - 4 = (x - 2)(x + 2)$ in irreduzible Faktoren gefunden haben, verbleibt es lediglich, eine

Zerlegung von $x^3-3x+503$ in irreduzible Faktoren zu finden. Wiederum stellen wir fest, dass $p = x^3-3x+503 \in \mathbb{Z}[x]$ und daher jede rationale Nullstelle von $p$ nach dem Lemma von Gauss ganzzahlig und Teiler von 503 ist. Da 503 Primzahl ist, kommen nur $\pm 1, \pm 503$ als ganzzahlige Nullstellen in Betracht. Andererseits ist offenbar $p(1) = 501 > 0, p(-1) = 505 > 0$ und $p(-503) = (-503^2+4)\cdot 503 < 0$ und $p(503) = (503^2-2)\cdot 503 > 0$. Damit hat $p$ keine ganzzahligen Nullstellen, also auch keine rationalen Nullstellen wegen Normiertheit und dem Lemma vom Gauss. Als Polynom vom Grad 3 über $\mathbb{Q}$ ist $p$ damit bereits nach einem bekannten Irreduzibilitätskriterium für Polynome niedrigen Grades irreduzibel über $\mathbb{Q}[x]$. Insgesamt haben wir also die folgende Zerlegung von $f$ in irreduzible Faktoren in $\mathbb{Q}[x]$ gefunden,

$$f = (x-2)(x+2)(x^3-3x+503). \tag{87}$$

Ende der Aufgabe. □

**Aufgabe 57 (F18T1A4(a))** Zu zeigen ist hier, dass das Polynom $p = x^5 - 4x + 2 \in \mathbb{Q}[x]$ irreduzibel ist. Wir stellen fest, dass $p$ normiert ist. Da $2|(-4)$ und $2 \not| 1$ sowie $2^2 = 4 \not| 2$, können wir auf $p \in \mathbb{Z}[x]$ das Eisenstein-Kriterium zur Primzahl 2 anwenden. Dieses liefert uns die Irreduzibilität von $p$ über $\mathbb{Z}[x]$. Da $\mathbb{Q}$ der Quotientenkörper des faktoriellen Rings $\mathbb{Z}$ ist, liefert uns ein Resultat von Gauss, dass $p$ bereits über $\mathbb{Q}[x]$ irreduzibel ist. □

**Aufgabe 58 (F12T2A4(a))** Gegeben sei das Polynom $f = x^4 + 4x^2 + 2 \in \mathbb{Q}[x]$. Zu zeigen ist, dass $f$ irreduzibel über $\mathbb{Q}[x]$. Wir stellen zunächst fest, dass $f$ bereits normiert ist und nur ganzzahlige Koeffizienten hat. Es reicht also zu zeigen, dass $f$ in $\mathbb{Z}[x]$ irreduzibel ist. Da $\mathbb{Q}$ der Quotientenkörper des faktoriellen Rings $\mathbb{Z}$ ist, liefert uns das Lemma von Gauss dann, dass $f$ auch über $\mathbb{Q}[x]$ irreduzibel ist. Wir stellen fest, dass $2 \not| 1$, also der Leitkoeffizient von $f$ nicht von der Primzahl 2 restfrei in $\mathbb{Z}$ geteilt wird. Ferner gilt für den einzigen nicht-verschwindenden Koeffizienten von $f$, $2|4$. Für das konstante Glied im Polynom gilt $2^2 \not| 2$, da $4 = 2^2 > 2$. Insofern ist das Eisenstein-Kriterium für die Primzahl 2 auf das Polynom $f \in \mathbb{Z}[x]$ anwendbar. Es liefert die Irreduzibilität von $f$ über $\mathbb{Z}[x]$. Nach der obenstehenden Bemerkung liefert schlussendlich das Lemma von Gauss, dass $f$ auch über $\mathbb{Q}[x]$ irreduzibel ist. □

**Aufgabe 59 (F13T1A2(a))** Sei $f = x^2 - 2 \in \mathbb{Q}[x]$ und $f_n := f(f_{n-1}(x)) \in \mathbb{Q}[x]$ für $n \in \mathbb{N}$ sowie $f_0 = x$. Zu zeigen ist, dass $f_n$ für alle $n \in \mathbb{N}$ irreduzibel ist über $\mathbb{Q}[x]$. Wir bemerken zuerst, dass infolge der Normiertheit von $x^2-2$ auch $f_n$ für alle $n \in \mathbb{N}$ normiert ist. Denn die höchste Potenz von $x$ in $f_n$ ist gerade $x^{2^n}$, was nur zu erreichen ist durch $x^{2^n} = (x^2)^n$. Wir zeigen nun, dass gilt $f_n \equiv x^{2^n} - 2 \bmod(4)$ für alle $n \in \mathbb{N}$. In der Tat finden wir für $n = 1$, dass $x^{2^1} - 2 = f_1 \equiv x^2 - 2 \bmod(4)$. Sei nun für festes aber beliebiges $n$ die Gültigkeit, dass $f_n \equiv x^{2^n} - 2 \bmod(4)$ vorausgesetzt. Wir müssen nun zeigen, dass $f_{n+1} \equiv x^{2^{n+1}} - 2 \bmod(4)$. Es gilt $f_{n+1} = f_n^2 - 2$. Reduktion

mod(4) liefert unter Beachtung der Rechenregeln

$$\begin{aligned} f_{n+1} &\equiv (f_n^2 - 2) \bmod(4) \\ &\equiv (f_n \bmod(4))^2 - 2 \bmod(4) \\ &\equiv [(x^{2^n} - 2)(x^{2^n} - 2) - 2] \bmod(4) \\ &\equiv [x^{2^{n+1}} - 4 \cdot x^{2^n} + 4 - 2] \bmod(4) \\ &\equiv (x^{2^{n+1}} - 2) \bmod(4). \end{aligned}$$

Damit haben wir gezeigt, dass in $\mathbb{Z}[x]$ für jedwedes $n \in \mathbb{N}$ gilt

$$f_n = \sum_{k=0}^{2^n} a_k x^k, \tag{88}$$

wobei $a_{2^n} = 1$, $a_0 \equiv -2 \bmod(4)$ und $a_k \equiv 0 \bmod(4)$ für alle $0 < k < 2^n$. Damit können wir das Eisenstein-Kriterium für die Primzahl 2 anwenden, denn infolge Normiertheit von $f_n$ gilt $2 \not| a_{2^n} = 1$ und $2^2 = 4 \not| a_0$, da sonst $a_0 \equiv 0 \bmod(4)$ im Widerspruch zu $a_0 \equiv -2 \bmod(4) \neq 0 \bmod(4)$. Ferner gilt da $a_k \equiv 0 \bmod(4)$ für alle $1 \leq k \leq 2^n - 1$ auch $2|a_k$, da $2|4$ und $4|a_k$. Das Eisenstein-Kriterium liefert nun die Irreduzibiliät von $f_n$ für beliebiges $n \in \mathbb{N}$. Das Lemma von Gauss liefert nun, dass $f_n$ auch über $\mathbb{Q}[x]$ irreduzibel ist, denn $\mathbb{Q}$ ist zum faktoriellen Ring $\mathbb{Z}$ gehörige Quotientenkörper. □

**Aufgabe 60 (H15T1A4(a) und (b))** Gegeben sei das Polynom $f = x^3 - x + 2 \in \mathbb{Z}[x]$. Wir zeigen zuerst, dass $\bar{f}$, das Bild von $f$ in $\mathbb{F}_3[x]$, irreduzibel ist. Zunächst berechnen wir $\bar{f} = \bar{x}^3 + \bar{2}\bar{x} + \bar{2} \in \mathbb{F}_3[x]$. Es gilt $\bar{f}(\bar{0}) = \bar{2} \neq \bar{0}$, $\bar{f}(\bar{1}) = \bar{1} + \bar{2} + \bar{2} = \bar{2} \neq \bar{0}$ und $\bar{f}(\bar{2}) = \bar{8} + \bar{4} + \bar{2} = \bar{2} \neq \bar{0}$. Also hat $\bar{f}$ keine Nullstelle in $\mathbb{F}_3$. Als Polynom vom Grad 3 ist $\bar{f}$ daher in $\mathbb{F}_3[x]$ irreduzibel. Wir zeigen nun, dass $f$ auch in $\mathbb{Q}[x]$ irreduzibel ist. Da $f$ normiert und ganzzahlig ist, liegt nach dem Lemma von Gauss bereits jede rationale Nullstelle von $f$ in $\mathbb{Z}$. Um nachzuweisen, dass $f$ in $\mathbb{Q}[x]$ irreduzibel ist, reicht es nach dem Lemma von Gauss aus, zu zeigen, dass $\bar{f}$ in $\mathbb{Z}[x]$ irreduzibel ist. Letzteres folgt aber aus dem Reduktionskriterium für die Primzahl 3 zusammen mit der vorher gezeigten Irreduzibiliät von $\bar{f}$ in $\mathbb{F}_3[x]$. Also ist $f$ in $\mathbb{Z}[x]$ und damit bereits in $\mathbb{Q}[x]$ irreduzibel. □

**Aufgabe 61 (F13T3A4)** Sei $\mathbb{F}_3$ der Körper mit 3 Elementen. Gesucht sind zunächst alle irreduziblen Polynome vom Grad $\leq 2$. Wir bestimmen diese durch Fallunterscheidung.

- *Fall 1: Grad* $= 0$. Es ist aus der Vorlesung bekannt, dass die normierten irreduziblen Polynome vom Grad 0 gerade die Einheiten des Körpers $\mathbb{F}_3$ sind. Insofern finden wir $p_1 = \bar{1}$, $p_2 = \bar{2}$, und das konstante Polynom $\bar{0}$ scheidet aus, da es eine Nicht-Einheit ist.

- *Fall 2: Grad* $= 1$. Es ist aus der Vorlesung bekannt, dass ein Polynom vom Grad 1 aus $\mathbb{F}_3[x]$ genau eine Nullstelle in $\mathbb{F}_3$ besitzt und darüber hinaus irreduzibel ist. Da nach Voraussetzung die gesuchten Polynome zusätzlich normiert sind, finden wir die drei Polynome $p_3 = x$, $p_4 = x + \bar{1}$, $p_5 = x + \bar{2} \in \mathbb{F}_3[x]$.

- *Fall 3: Grad = 2.* Es ist aus der Vorlesung bekannt, dass ein normierte Polynom vom Grad 2 irreduzibel ist, wenn es keine Nullstelle in $\mathbb{F}_3$ besitzt. Ein generisches normiertes Polynom aus $\mathbb{F}_3[x]$ ist von der Form $x^2 + ax + b$, wobei $a, b \in \mathbb{F}_3$. Wir können nun ausschließen, dass $b = 0$, denn dann hätte das Polynom bereits $\bar{0}$ als Nullstelle, wäre also nicht irreduzibel. Ferner können wir auch allgemein ausschließen, dass das gesuchte Polynom Produkt von zwei Polynomen vom Grad 1 aus dem vorher betrachteten Fall ist. Wir finden zunächst die folgenden 6 Kandidaten:

  $$q_1 = x^2 + 1,\ q_2 = x^2 + 2,\ q_3 = x^2 + x + 1$$
  $$q_4 = x^2 + 2x + 1,\ q_5 = x^2 + x + 2,\ q_6 = x^2 + 2x + 2.$$

  Durch Einsetzen von $x = 1$ stellen wir fest, dass dies eine Nullstelle von $q_2, q_3$ ist. Diese Polynome fallen also aus. Durch Einsetzen von $x = 2$ stellen wir fest, dass dies eine Nullstelle von $q_4$ ist, Wir haben somit nur noch die folgenden normierten, irreduziblen Polynome:

  $$p_6 = x^2 + 1,\ p_7 = x^2 + x + 2,\ p_8 = x^2 + 2x + 2. \tag{89}$$

Wir haben nun das Polynom $f = x^4 + 9x^2 - 2x + 2$ gegeben. Zu untersuchen ist, ob dieses irreduzibel in $\mathbb{Q}[x]$ ist. Da $\mathbb{Q}$ der Quotientenkörper zum faktoriellen Ring $\mathbb{Z}$ und $f \in \mathbb{Z}[x]$ infolge Ganzzahligkeit der Koeffizienten gilt, liefert das Gauss Lemma zunächst, dass es reicht, zu untersuchen, ob $f$ irreduzibel in $\mathbb{Z}[x]$ ist. Wir bestimmen dazu zunächst das Bild von $f$ unter der Reduktionsabbildung mod(3), d.h., in $\mathbb{F}_3[x]$. Wir finden, dass $\bar{f} = x^4 + x + 2$. Als Polynom vom Grad 4 in $\mathbb{F}_3[x]$ tritt einer der folgenden Fälle ein, in denen $\bar{f}$ nicht irreduzibel, als Nicht-Einheit, somit reduzibel ist. Erstens, $\bar{f}$ kann eine Nullstelle in $\mathbb{F}_3$ haben, und man kann ein irreduzibles normiertes Polynom vom Grad 1 abspalten. Zweitens, $\bar{f}$ lässt sich als Produkt von zwei irreduziblen Polynomen vom Grad 2 schreiben, die wir oben vollständig aufgelistet haben. Wir überprüfen zunächst, ob $\bar{f}$ Nullstellen in $\mathbb{F}_3$ hat. Es gilt $\bar{f}(\bar{0}) = \bar{2} \neq \bar{0}$, $\bar{f}(\bar{1}) = \bar{4} = \bar{1} \neq \bar{0}$ und $\bar{f}(\bar{2}) = \bar{8} = \bar{2} \neq \bar{0}$. Damit kann der erste Falle, man könne einen Linearfaktor aus $\bar{f}$ abspalten, ausgeschlossen werden. Wir stellen nun fest, dass das konstante Glied in $\bar{f}$ gerade $\bar{2}$ ist. Für die Überprüfung von Fall 2 kommt daher nur in Betracht, dass $\bar{f} \stackrel{?}{=} p_6 \cdot p_7$ oder $\bar{f} \stackrel{?}{=} p_6 \cdot p_8$, bis auf Reihenfolge. Der Fall $f$ wäre $p_7 \cdot p_8$ scheidet aus, da das konstante Glied von $p_7 \cdot p_8$ gerade $2 \cdot 2 = 1$ in $\mathbb{F}_3$ ist. Wir berechnen:

$$\begin{aligned} p_6 \cdot p_7 &= (x^2 + 1)(x^2 + x + 2) \\ &= x^4 + x^3 + 2x^2 + x^2 + x + 2 \\ &= x^4 + x^3 + x + 2 \neq \bar{f} \\ p_6 \cdot p_8 &= (x^2 + 1)(x^2 + 2x + 2) \\ &= x^4 + 2x^3 + 2x^2 + x^2 + 2x + 2 \\ &= x^4 + 2x^3 + 2x + 2 \neq \bar{f}. \end{aligned}$$

Damit greift auch Fall 2 nicht und wir stellen fest, dass $\bar{f}$ irreduzibel in $\mathbb{F}_3[x]$ ist. Nach dem Reduktionskriterium folgt also die Irreduzibilität von $f \in \mathbb{Z}[x]$ über dem Polynomring $\mathbb{Z}[x]$. Das Gauss Lemma liefert nun, wie eingangs besprochen, die Irreduzibilität von $f$ über $\mathbb{Q}[x]$. □

**Aufgabe 62** Sei $p$ eine Primzahl. Gesucht ist das $p$-te Kreisteilungspolynom $\Phi_p \in \mathbb{Z}[x]$. Wir verwenden, dass für jede natürliche Zahl, insbesondere also jede Primzahl, gilt

$$x^p - 1 = \prod_{d|p} \Phi_d(x) = \Phi_1(x)\Phi_p(x). \tag{90}$$

Zusammen mit $\Phi_1(x) = x - 1$ kommen wir auf folgende Behauptung, die wir allgemeiner für $n \in \mathbb{N}$ formulieren:

$$\frac{x^n - 1}{x - 1} = \sum_{k=0}^{n-1} x^k. \tag{91}$$

Wir zeigen dies per Induktion über $n$. Für $n = 1$ finden wir auf der linken Seite $(x-1)/(x-1) = 1$. Die Summe rechts läuft von $k = 0$ bis $k = 1-1$, so dass die Summe insgesamt zu 1 evaluiert. Damit haben wir also gezeigt, dass die Aussage für $n = 1$ wahr ist. Wir nehmen nun an, die Aussage $(x^n - 1)/(x - 1) = \sum_{k=0}^{n-1} x^k$ gilt für ein beliebiges aber festes $n$. Zu zeigen ist, dass dann auch $(x^{n+1} - 1)/(x - 1) = \sum_{k=0}^{n} x^k$ gilt. Hierzu schreiben wir

$$\begin{aligned}
\frac{x^{n+1} - 1}{x - 1} &= \frac{(x^{n+1} - x^n) + (x^n - 1)}{x - 1} && (92)\\
&= \frac{x^n(x - 1)}{x - 1} + \frac{x^n - 1}{x - 1} && (93)\\
&= x^n + \sum_{k=0}^{n-1} x^k && (94)\\
&= \sum_{k=0}^{n} x^k. && (95)
\end{aligned}$$

Damit haben wir bewiesen, dass die Aussage auch für die Zahl $n + 1$ gilt. Das Indukionsprinzip liefert nun, dass die oben angegebene Formel für beliebige $n \in \mathbb{N}$ gilt. Insbesondere finden wir für eine beliebige Primzahl $p$, dass

$$\Phi_p(x) = \frac{x^p - 1}{\Phi_1(x)} = \frac{x^p - 1}{x - 1} = \sum_{k=0}^{p-1} x^k. \tag{96}$$

Damit sind die $p$-ten Kreistelungspolynome $\Phi_p$ bekannt. □

**Aufgabe 63** Gesucht ist das Kreisteilungspolynom $\Phi_{15}$. Wir verwenden wiederum die Formel, dass

$$x^{15} - 1 = \prod_{d|15} \Phi_d(x) = \Phi_1(x)\Phi_3(x)\Phi_5(x)\Phi_{15}(x). \tag{97}$$

Aus der vorangegangenen Teilaufgabe ist bekannt, dass $\Phi_3(x) = x^2 + x + 1$ und $\Phi_5(x) = x^4+x^3+x^2+x+1$ sowie $\Phi_1(x) = x-1$. Insbesondere gilt $x^5-1 = \Phi_1(x)\Phi_5(x)$. Es ist leicht einzusehen, dass

$$x^{15} - 1 = (x^5 - 1)(x^{10} + x^5 + 1), \tag{98}$$

indem man bspw. ausmultipliziert. Nun berechnen wir mittels Polynomdivision in $\mathbb{Q}[x]$

$$\frac{x^{10}+x^5+1}{x^2+x+1} = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1. \tag{99}$$

Damit finden wir also

$$\Phi_{15}(x) = \frac{x^{15}-1}{\Phi_1(x)\Phi_3(x)\Phi_5(x)} = \frac{x^{15}-1}{(x^5-1)(x^2+x+1)} = \frac{x^{10}+x^5+1}{x^2+x+1} \tag{100}$$

$$= x^8 - x^7 + x^5 - x^4 + x^3 - x + 1. \tag{101}$$

□

**Aufgabe 64** Gegeben sei eine quadratfreie Zahl $m \in \mathbb{Z} \setminus \{0,1\}$. Gesucht sind diejenigen $n \in \mathbb{N}$, die in $\mathbb{Q}(\sqrt{m})$ liegen. Sei $m$ zunächst beliebig mit den geforderten Eigenschaften. Das Eisenstein-Kriterium für einen Primteiler von $m \neq -1$ zeigt, dass $f_m(x) := x^2 - m$ irreduzibel über $\mathbb{Z}[x]$, und damit nach dem Gauss'schen Lemma auch über $\mathbb{Q}[x]$ ist. Für $m = -1$, verwenden wir, dass $f_{-1} = x^2 + 1$ nach dem Reduktionskriterium für $p = 3$ irreduzibel in $\mathbb{Z}[x]$ und damit, wiederum nach dem Gauss'schen Lemma, in $\mathbb{Q}[x]$ irreduzibel ist. Ferner gilt $f_m(\sqrt{m}) = 0$ für $m \in \mathbb{Z} \setminus \{0,1\}$. Laut Vorlesung ist also $f_m = \mu_{\sqrt{m},\mathbb{Q}}$ das Minimalpolynom von $\sqrt{m}$ über $\mathbb{Q}$. Damit finden wir $[\mathbb{Q}(\sqrt{m}) : \mathbb{Q}] = \deg f_m = 2$. Sei $\alpha \in \mathbb{Q}(\sqrt{m})$ beliebig. Dann gilt $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{m})$, also insbesondere $1 \leq [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq [\mathbb{Q}(\sqrt{m}) : \mathbb{Q}] = 2$. Also ist das Minimalpolynom von $\alpha$ über $\mathbb{Q}$ vom Grad 1 oder 2. Die erste und zweiten Einheitswurzeln sind $+1$ respektive $\pm 1$. Diese sind sogar ganzzahlig und daher in jedem $\mathbb{Q}(\sqrt{m})$ enthalten. Sei nun $n \in \mathbb{N} \setminus \{1,2\}$ beliebig und $\zeta_n$ eine beliebige, primitive $n$-te Einheitswurzel. Dann ist $\zeta_n$ nach Definition des $n$-ten Kreisteilungspolynoms Nullstelle von $\Phi_n(x)$. Aus der Vorlesung ist ferner bekannt, dass $\Phi_n$ für alle $n \in \mathbb{N}$ irreduzibel über $\mathbb{Q}$ ist. Folglich ist $\Phi_n = \mu_{\zeta_n,\mathbb{Q}}$. Wegen $\deg \Phi_n = \Phi(n)$, wobei $\Phi$ die Euler'sche $\phi$-Funktion ist, finden wir also $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \Phi(n)$. Nach Definition ist $\Phi(n) = |\{k \in \mathbb{N} | \mathrm{ggT}(k,n) = 1\}|$. Es gilt $\Phi(n) = 2$ genau dann wenn $n \in \{3,4,6\} =: M$. Es kommen also nur primitive $n$-te Einheitswurzeln in Betracht, für die $n \in M$ gilt. Andernfalls wäre $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \Phi(n) > 2 = [\mathbb{Q}(\sqrt{m}) : \mathbb{Q}]$ im Widerspruch dazu, dass $\zeta_n$ als Element von $\mathbb{Q}(\sqrt{m})$ ein Minimalpolynom vom Grad $\leq 2$ besitzt. Nun gilt $\zeta_3 = \exp(2\pi i/3) = \cos(2\pi/3) + i\sin(2\pi/3) = -0.5 + 0.5\sqrt{3}i$, $\zeta_4 = \exp(2\pi i/4) = \cos(\pi/2) + i\sin(\pi/2) = i$ und $\zeta_6 = \exp(2\pi i/6) = \cos(\pi/3) + i\sin(\pi/3) = 0.5 + 0.5\sqrt{3}i$. Wir sehen nun, dass

$$\{\pm 1\} \subseteq \mathbb{Q}(\sqrt{m})\, \forall m \in \mathbb{Z} \setminus \{0,1,-1,-3\} \tag{102}$$

$$\{\pm 1, \pm i\} \subseteq \mathbb{Q}(\sqrt{-1}) \tag{103}$$

$$\{\pm 1, \pm 0.5 + i0.5\sqrt{3}, \pm 0.5 - i0.5\sqrt{3}\} \subseteq \mathbb{Q}(\sqrt{-3}), \tag{104}$$

jeweils alle Einheitswurzeln angibt, die in den jeweiligen Körpern liegen. □

**Aufgabe 65** Zu zeigen ist $\mathbb{Q}(\zeta_3, \zeta_4) = \mathbb{Q}(\zeta_{12})$, wobei $\zeta_n = \exp(2\pi i/n)$ für alle $n \in \mathbb{N}$. Es reicht die zwei Inklusionen, $\zeta_3, \zeta_4 \in \mathbb{Q}(\zeta_{12})$ und $\zeta_{12} \in \mathbb{Q}(\zeta_3, \zeta_4)$, nachzurechnen.

Wegen

$$\zeta_{12}^4 = \exp\left(\frac{2\pi i}{12}\right)^4 = \exp\left(\frac{2\pi i}{3}\right) = \zeta_3 \tag{105}$$

$$\zeta_{12}^3 = \exp\left(\frac{2\pi i}{12}\right)^3 = \exp\left(\frac{2\pi i}{4}\right) = \zeta_4, \tag{106}$$

folgt aus $\zeta_{12} \in \mathbb{Q}(\zeta_{12})$ auch $\zeta_3 = \zeta_{12}^4 \in \mathbb{Q}(\zeta)$ und $\zeta_4 = \zeta_{12}^3 \in \mathbb{Q}(\zeta_{12})$. Damit ist laut einem Vorlesungsresultat bereits die Inklusion $\mathbb{Q}(\zeta_3, \zeta_4) \subseteq \mathbb{Q}(\zeta_{12})$ nachgewiesen, wobei $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_{12})$ bemerkt wurde. Für den Nachweis der Inklusion $\mathbb{Q}(\zeta_{12}) \subseteq \mathbb{Q}(\zeta_3, \zeta_4)$, beobachten wir, dass gilt $\zeta_3, \zeta_4 \in \mathbb{Q}(\zeta_3, \zeta_4)$, sodass auch $\zeta_3\zeta_4^{-1} \in \mathbb{Q}(\zeta_3, \zeta_4)$, da $\zeta_4 \neq 0$. Hiermit finden wir

$$\zeta_3 \cdot \zeta_4^{-1} = \exp\left(\frac{2\pi i}{3}\right) \cdot \exp\left(\frac{2\pi i}{4}\right)^{-1} \tag{107}$$

$$= \exp\left(\frac{2\pi i \cdot 4}{12} - \frac{2\pi i \cdot 3}{12}\right) \tag{108}$$

$$= \exp\left(\frac{2\pi i}{12}\right) = \zeta_{12}. \tag{109}$$

Da $\mathbb{Q}(\zeta_3, \zeta_3)$ Körper ist, gilt also $\zeta_{12} = \zeta_3 \cdot \zeta_4^{-1} \in \mathbb{Q}(\zeta_3, \zeta_4)$. Da $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_3, \zeta_4)$, folgt insgesamt $\mathbb{Q} \cup \{\zeta_{12}\} \subseteq \mathbb{Q}(\zeta_3, \zeta_4)$, mithin $\mathbb{Q}(\zeta_{12}) \subseteq \mathbb{Q}(\zeta_3, \zeta_4)$. Zusammen mit der bereits beweisenen Inklusion, haben wir also die Gleichheit $\mathbb{Q}(\zeta_3, \zeta_4) = \mathbb{Q}(\zeta_{12})$ etabliert. □

**Aufgabe 66 (H10T2A4)** Sei $m \in \mathbb{N}$ beliebig und sei $f_m \equiv X^{2m} + X^m + 1 \in \mathbb{Z}[X]$. Wir zeigen zuerst, dass jede komplexe Nullstelle von $f_m$ eine Einheitswurzel ist. Hierzu beobachten wir, dass $(X^{2m} + X^m + 1)(X^m - 1) = (X^{3m} + X^{2m} + X^m - X^{2m} - X^m - 1) = X^{3m} - 1$. Insbesondere stellen wir fest, dass eine beliebige Nullstelle von $X^{2m} + X^m + 1$ eine Nullstelle von $X^{3m} - 1$ ist, d.h., eine $3m$-te Einheitswurzel für das vorgegebenene $m$. Wir zeigen nun, dass $f_m$ genau dann irreduzibel über $\mathbb{Q}[x]$ ist, wenn es ein $k \in \mathbb{N}_0$ gibt, sodass $m = 3^k$. Wir zeigen zunächst, dass $m = 3^k$ mit $k \in \mathbb{N}_0$ die Irreduzibilität von $f_m$ impliziert. Dazu bemerken wir, dass laut Teil (a) gilt

$$X^{3^{k+1}} - 1 = (X^{3^k} - 1) f_{3^k}(X). \tag{110}$$

Das Polynom links und der erste Faktor rechts erlauben eine Dekomposition in Kreisteilugspolynome $\Phi_n$ wie folgt,

$$X^{3^{k+1}} - 1 = \prod_{d|3^{k+1}} \Phi_d(X) = \prod_{j=0}^{k+1} \Phi_{3^j}(X) \tag{111}$$

$$X^{3^k} - 1 = \prod_{d|3^k} \Phi_d(X) = \prod_{j=0}^{k} \Phi_{3^j}(X). \tag{112}$$

Indem wir diese Beobachtungen in die vorhergehende Gleichung einsetzen, finden wir nach Division durch die $\Phi_{3^j}$ für $0 \leq j \leq k$ auf beiden Seiten

$$\Phi_{3^{k+1}}(X) = f_{3^k}(X) = X^{2\cdot 3^k} + X^{3^k} + 1. \tag{113}$$

Aus der Vorlesung ist bekannt, dass die Kreisteilungspolynome $\Phi_n$ für alle $n \in \mathbb{N}$ irreduzibel über $\mathbb{Z}[x]$ und nach dem Gauss'schen Lemma also auch irreduzibel über $\mathbb{Q}[x]$ sind, da $\mathbb{Q} = \text{Quot}(\mathbb{Z})$. Sei nun vorausgesetzt, dass $f_m$ irreduzibel in $\mathbb{Q}[X]$ ist. Wir nehmen an, $m \neq 3^k$ für ein $k \in \mathbb{N}_0$. Wiederum erlaubt $X^{3m} - 1$, $X^m - 1$ je eine Darstellung als Produkt der über $\mathbb{Q}[X]$ irreduziblen Kreisteilungspolynome,

$$\prod_{d|3m} \Phi_d(X) = f_m(X) \prod_{d|m} \Phi_d(X). \tag{114}$$

Umformen liefert $f_m(X) = \prod_{d\not|m, d|3m} \Phi_d(X)$. Da $m \neq 3m$, hat $m$ einen Primteiler $p$, der von drei verschieden ist und mit der Potenz $l$ auftaucht, d.h., es gilt $p^l|m$ aber $p^{l+1} \not| m$. Dann gilt $3p^l|3m$. Falls $3|m$ mit maximaler Potenz $L \in \mathbb{N}$, so gilt $\Phi_{p^j 3^L \cdot 3}|f_m$ für alle $0 \leq j \leq k$ aber $3^{L+1} \not| m$. Das liefert uns mindestens zwei irreduziblle Polynome, die $f_m(X)$ teilen. Somit haben wir einen Widerspruch zur Voraussetzung, $f_m$ wäre irreduzibel. Also muss $m = 3^k$ gelten. Insgesamt ist die Äquivalenz damit nachgewiesen.

**Aufgabe 67 (F17T1A5)** Sei $\mathbb{F}_p$ der Körper mit $p$ Elementen und $p$ eine Primzahl. $\bar{\mathbb{F}}_p$ bezeichne den algebraischen Abschluss von $\mathbb{F}_p$ und für ein $r \in \mathbb{N}$ sei $\mathbb{F}_{p^r}$ ein Zwischenkörper der algebraischen Erweiterung $\bar{\mathbb{F}}_p|\mathbb{F}_p$. Sei $n \in \mathbb{N}$ und $A$ eine $n \times n$-Matrix mit der Eigenschaft, dass $\chi_A \in \mathbb{F}_p[x]$ irreduzibel ist. Wir behaupten, dass dann $A$ über $\mathbb{F}_{p^n}$ diagonalisierbar ist. Aus der Vorlesung ist bekannt, dass eine $n \times n$-Matrix über eine Körper $L(|)K$ allgemein diagonalisierbar ist genau dann, wenn für jede Nullstelle aus $L$ des charakteristischen Polynoms $\chi_A = \det(zE_n - A) \in K[x]$, d.h., für jeden Eigenwert, geometrische und algebraische Vielfachheit übereinstimmen $\mu_g(\lambda) = \mu_a(\lambda)$. Für den Fall $K = \mathbb{F}_p$ stellen wir fest, dass $\chi_A \in \mathbb{F}_p[x]$. Ferner ist $\chi_A$ bereits nach Voraussetzung irreduzibel in $\mathbb{F}_p[x]$ und aus der Definition stellen wir fest, dass $\chi_A$ normiert ist. Für eine Nullstelle $\alpha \in \bar{\mathbb{F}}_p$ von $\chi_A$ ist dann $\chi_A$ das Minimalpolynom von $\alpha$ über $\mathbb{F}_p$, $\chi_A = \mu_{\mathbb{F}_p,\alpha}$. Es gilt daher $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = \deg(\chi_A) = n$, sodass $\mathbb{F}_p(\alpha) \simeq \mathbb{F}_p^n$ als $\mathbb{F}_p$-Vektorraum. Nach dem Existenz- und Eindeutigkeitssatz über endliche Körper aus der Vorlesung gilt dann $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^n}$. Da $\alpha \in \bar{F}_p$ eine beliebige Nullstelle von $\chi_A$ ist, folgt daraus, dass bereits alle Nullstellen von $\chi_A$ in $\mathbb{F}_{p^n}$ enthalten sind. Insbesondere ist $\mathbb{F}_{p^n} = \text{Zerf}_{\mathbb{F}_p}(\chi_A)$, d.h., der Zerfällungskörper von $\chi_A$ über $\mathbb{F}_p$. Da $\text{char}(\mathbb{F}_p) = p = \text{char}(\mathbb{F}_{p^n})$ als Ringe, können wir das Vorlesungsresultat verwenden, dass jede endliche Erweiterung von $\mathbb{F}_p$, d.h., insbesondere algebraische, auch eine separable Erweiterung ist. Da $\mathbb{F}_{p^n}|\mathbb{F}_p$ separable Erweiterung ist, gilt $\text{ggT}(\chi_A, \chi_A') = 1$. Laut Vorlesung ist letzteres aber gleichbedeutend damit, dass $\chi_A$ nur einfache Nullstellen in $\mathbb{F}_{p^n}$ hat. Da für jede der $n$ paarweise verschiedenen Nullstellen $\lambda_1, ..., \lambda_n$ von $\chi_A$ jeweils gilt $\mu_a(\lambda_i) = 1$, liefert die bekannte Ungleichung $1 \leq \mu_g(\lambda_i) \leq \mu_a(\lambda_i)$, dass $\mu_g(\lambda_i) = 1 = \mu_a(\lambda_i)$ für alle $1 \leq i \leq n$. Das bedeutet, dass für jeden der $n$ Eigenwerte algebraische und geometrische Vielfachheit übereinstimmen. Das oben zitierte Diagonalisierbarkeitskriterium liefert

nun, dass die Matrix $A$ tatsächlich über $\mathbb{F}_{p^n}$ diagonalisierbar ist. Wir setzen nun $p = 5$ und betrachten die Matrix

$$A = \begin{pmatrix} -1 & 3 & -1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \tag{115}$$

Wir zeigen nun, dass $A$ über $\mathbb{F}_{25=5^2}$ diagonalisierbar ist, nicht aber über $\mathbb{F}_{125=5^3}$. Wir berechnen zuerst das charakteristische Polynom von $A$. Es gilt $\chi_A(z) = \det(zE_3 - A) = (-1)^3 \det(A - zE_3)$ für $\chi_A : \mathbb{F}_5^{\text{alg}} \to \mathbb{F}_5^{\text{alg}}$ und

$$\begin{aligned} \chi_A(z) &= (-1)^3((-z-1)(-z)^2 + 3 - (-1)(-z)) \\ &= (-1)(-z^3 - z^2 - z + 3) \\ &= z^3 + z^2 + z - 3 \\ &= z^3 + z^2 + z + 2 \end{aligned}$$

Wir sehen, dass $\chi_A(1) = 0$, sodass $\chi_A$ nicht irreduzibel ist über $\mathbb{F}_p[z]$. Es gilt aber $\chi_A(z) = (z-1)(z^2 + 2z + 3)$ und $g \equiv z^2 + 2z + 3 \in \mathbb{F}_5[z]$ erfüllt $g(0) = 3 \neq 0$, $g(1) = 1 \neq 0$, $g(2) = 1 \neq 0$, $g(3) = 3 \neq 0$ und $g(4) = 2 \neq 0$. Also hat $g$ keine Nullstelle in $\mathbb{F}_5$ und ist damit irreduzibel über $\mathbb{F}_5[z]$. Da $\mathbb{F}_5^{\text{alg}}$ algebraischer Abschluss von $\mathbb{F}_5$, gibt es ein $\alpha \in \mathbb{F}_5^{\text{alg}}$, sodass $g(\alpha) = 0$. Da $g$ normiert und über $\mathbb{F}_5$ irreduzibel ist, gilt $g = \mu_{\mathbb{F}_5,\alpha}$. Damit ist $[\mathbb{F}_5(\alpha) : \mathbb{F}_5] = \deg g = 2$ und, analog zu oben mit $p = 5$ und $n = 2$, schließen wir, dass $g$ in $\mathbb{F}_{25=5^2}$ zwei einfache Nullstellen hat, die, wegen der Irreduzibilität von $g$ über $\mathbb{F}_5$, sogar in $\mathbb{F}_{25} \setminus \mathbb{F}_5$ liegen. Da $\mathbb{F}_5 \subseteq \mathbb{F}_{25}$ wegen $1|2$, zerfällt also $\chi_A$ über $\mathbb{F}_{25}$ in Linearfaktoren und hat drei verschiedene Nullstellen $\lambda_1 = 1, \lambda_2, \lambda_3$ der Nulstellenordnung 1. Damit finden wir wegen $\mu_a(\lambda_i) = 1$ und $1 \leq \mu_g(\lambda_i) \leq \mu_a(\lambda_i)$ für $1 \leq i \leq 3$, dass geometrische und algebraische Vielfachheit für jeden Eigenwert übereinstimmen. Analog zum ersten Aufgabenteil folgern wir also, dass $A$ über $\mathbb{F}_{25}$ diagonalisierbar ist. Wir zeigen nun noch, dass $A$ nicht über $\mathbb{F}_{125=5^3}$ diagonalisierbar ist. Angenommen, $A$ wäre über $\mathbb{F}_{125}$ diagonalisierbar. Dann würde $\chi_A$ über $\mathbb{F}_{125}$ dergestalt in Linearfaktoren zerfallen, dass für die Nullstellen in $\mathbb{F}_{125}$ geometrische und algebraische Vielfachheit übereinstimmen. Wir haben bereits gesehen, dass $\mathbb{F}_5(\{\lambda_1, \lambda_2, \lambda_3\}) = \mathbb{F}_{25}$ gilt. Da $2 \not| 3$ ist aber der Zerfällungskörper $\mathbb{F}_{25}$ von $\chi_A$ nicht in $\mathbb{F}_{125}$ enthalten. Das ist ein Widerspruch zur Annahme, $A$ ist über $\mathbb{F}_{125}$ diagonalisierbar. Damit ist $A$ nicht über $\mathbb{F}_{125}$ diagonalisierbar und die Behauptung ist bewiesen. □

**Aufgabe 68 (H13T2A1)** Sei $f = x^4 + x + 1 \in \mathbb{F}_2[x]$. Wir zeigen zuerst, dass $f$ über $\mathbb{F}_2$ irreduzibel ist. Offenbar ist $f$ eine Nicht-Einheit, da $f \neq 1$ und $(\mathbb{F}_2[x])^\times = \mathbb{F}_2^\times = \{1\}$. Angenommen, $f$ wäre reduzibel. Dann gibt es eine Zerlegung von $f$ als Produkt nicht konstanter Polynome aus $\mathbb{F}_2[x]$. Sei $G$ der niedrigste Grad in einer solchen Zerlegung. Dann gilt $G \in \{1, 2\}$. Falls $G = 1$, gibt es ein Polynom $g \in \mathbb{F}_2[x]$ vom Grad 1, sodass $g|f$. Insbesondere hat $f$ dann eine Nullstelle in $\mathbb{F}_2$. Allerdings gilt $f(0) = 1 \neq 0$ und $f(1) = 1 \neq 0$, sodass $f$ keine Nullstelle in $\mathbb{F}_2$ besitzt. Also kann $f$ kein Polynom vom Grad 1 als Teiler besitzen. Falls $G = 2$, gibt es ein Polynom $h$ vom Grad 2 in $\mathbb{F}_2[x]$, das irreduzibel ist und $h|f$ erfüllt. Bekannt ist, dass $h = x^2 + x + 1$ das einzige irreduzible Polynom vom Grad 2 in $\mathbb{F}_2[x]$ ist. Aus

Gradgründen bleibt nur noch $f = h^2$ zu testen. Es gilt aber in $\mathbb{F}_2[x]$ aufgrund des "freshman's dream":

$$h^2 = (x^2 + x + 1)^2 = x^2 + x^2 + 1 \neq f. \tag{116}$$

Damit kann $f$ auch keinen irreduziblen Faktor vom Grad 2 haben. Insgesamt haben wir also gesehen, dass $f$ nicht die für reduzible Elemente gewünschte Produktdarstellung erlaubt. Zusammen mit der eingangs bemerkten Eigenschaft, dass $f$ eine Nicht-Einheit ist, folgt die Behauptung, dass $f$ irreduzibel über $\mathbb{F}_2$ ist. Sei nun $\bar{F}_2$ ein algebraischer Abschluss von $\mathbb{F}_2$ und $\alpha \in \bar{\mathbb{F}}_2$ eine Nullstelle vom oben untersuchten $f$. Wir behaupten, dass $\mathbb{F}_2(\alpha) = \mathbb{F}_{16}$. Es ist $f$ normiertes Polynom aus $\mathbb{F}_2[x]$, das irreduzibel über $\mathbb{F}_2$ ist und $\alpha$ als Nullstelle besitzt. Daher ist $f = \mu_{\mathbb{F}_2,\alpha}$, d.h., das Minimalpolynom von $\alpha$ über $\mathbb{F}_2$. Aus der Vorlesung ist bekannt, dass $\mathbb{F}_2(\alpha)$ Erweiterungskörper von $\mathbb{F}_2$ mit Erweiterungsgrad $[\mathbb{F}_2(\alpha) : \mathbb{F}_2] = \deg \mu_{\mathbb{F}_2,\alpha} = 4$ ist. Das bedeutet, $\mathbb{F}_2(\alpha) \simeq \mathbb{F}_2^4$ als $\mathbb{F}_2$-Vektorraum. Da $|\mathbb{F}_2(\alpha)| = 16$ liefert der ebenfalls aus der Vorlesung bekannt Existenz- und Eindeutigkeitssatz für endliche Körper, dass $\mathbb{F}_2(\alpha) = \mathbb{F}_{16}$. Das war zu zeigen. In einem weiteren Schritt behaupten wir, dass $\alpha \in \mathbb{F}_{16}^\times$ ein Erzeuger der Einheitengruppe ist. Da $\alpha \neq 0$, ist $\alpha \in \mathbb{F}_{16}^\times = \mathbb{F}_{16} \setminus \{0\}$ klar. Aus der Vorlesung ist ferner bekannt, dass $\mathbb{F}_{16}^\times$ zyklisch von Ordnung $16 - 1 = 15$ ist. Damit ist nur möglich, dass $\operatorname{ord}(\alpha) \in \{1, 3, 5, 15\}$ ist. Der Fall $\operatorname{ord}(\alpha) = 1$ scheidet wegen $\alpha \notin \mathbb{F}_2$ aus. Der Fall, dass $\operatorname{ord}(\alpha) = 3$ bedeutet, dass $\alpha^3 - 1 = 0$, also, dass $\alpha$ Nulstelle des Polynoms $p = x^3 - 1 \in \mathbb{F}_2[x]$ ist. Wegen $\deg p = 3 < 4 = \deg \mu_{\mathbb{F}_2,\alpha}$ ist dieser Fall ebenfalls unbeachtlich. Falls $\operatorname{ord}(\alpha) = 5$, gilt $\alpha^5 - 1 = 0$. Also ist $\alpha$ Nullstelle des Poloynoms $q = x^5 + 1 \in \mathbb{F}_2[x]$. Da $\deg q = 5 > 4 = \deg \mu_{\mathbb{F}_2,\alpha} = \deg f$, gibt es ein $r \in \mathbb{F}_2[x]$ vom Grad 1, sodass $r \cdot f = q$. Wir sehen, dass $q \in \{x, x + 1\}$ die einzigen Möglichkeiten sind. Es gilt aber $x \cdot (x^4 + x + 1) = x^4 + x^2 + x \neq x^5 + 1 = q$, sodass $r = x + 1$ gelten müsste. Allerdings ist $(x+1)(x^4+x+1) = x^5+x^4+x^2+1 \neq x^4+x+1 = f$. Damit scheiden alle Möglichkeiten, ein Polynom vom Grad 1 aus $\mathbb{F}_2[x]$ zu finden, sodass $q = r \cdot f$ gilt, aus. Da $f$ Minimalpolynom von $\alpha$ über $\mathbb{F}_2$ haben wir einen Widerspruch zur Annahme, dass $\alpha$ Nullstelle von $q$ ist. Insgesamt haben wir somit $\operatorname{ord}(\alpha) \in \{15\}$. Als Element einer zyklischen Gruppe der Ordnung 15, das selbst Ordnung 15 hat, erzeugt $\alpha$ also die zyklische Gruppe $\mathbb{F}_{16}^\times$. □

**Aufgabe 69 (F17T3A5)** Sei $K$ ein Teilkörper von $\mathbb{R}$ und $f \in K[x]$ ein Polynom. Sei $Z$ ein Zerfällungskörper mit $[Z : K] \in 2\mathbb{N} - 1$. Zu zeigen ist, dass $Z$ ebenfalls Teilkörper von $\mathbb{R}$ ist. Sei vorausgesetzt, dass $Z$ kein Teilkörper von $\mathbb{R}$ ist. Da $\mathbb{C}$ der algebraische Abschluss von $\mathbb{R}$ ist, ist $K$ ebenfalls Teilkörper von $\mathbb{C}$. $Z$ ist nun Teilkörper von $\mathbb{C}$ mit $Z \cap \mathbb{R} \setminus \mathbb{R} \neq \emptyset$. Da $K \subseteq \mathbb{R}$, hat $f$ zwei konjugiert komplexe Nullstellen, $\alpha, \bar{\alpha} \in \mathbb{C} \setminus \mathbb{R}$, d.h., insbesondere $\alpha \neq \bar{\alpha}$. Wir definieren $M = K(\alpha, \bar{\alpha})$ und $M_0 = M \cap \mathbb{R}$. Mit $M$ und $\mathbb{R}$ ist auch $M_0$ ein Erweiterungskörper von $K$. Wir behaupten $[M : M_0] = 2$. Betrachte dazu $g = (x - \alpha)(x - \bar{\alpha}) = x^2 + (\alpha + \bar{\alpha})x + \alpha\bar{\alpha}$. Da $\alpha\bar{\alpha}$ reell und in $M$ enthalten, ist $\alpha\bar{\alpha}$ auch in $M_0$ enthalten. Da $\alpha+\bar{\alpha} = 2\Re[\alpha]$ reell und in $M$ enthalten, ist $\alpha + \bar{\alpha}$ auch in $M_0$ enthalten. Damit ist $g \in M_0[x]$ normiert und hat keine Nullstellen in $M_0$. Als Polynom vom Grad 2 ist $g$ also irreduzibel über $M_0$. Damit ist $g$ Minimalpolynom von der Nullstelle $\alpha$ über $M_0$. Laut einem Vorlesungsresultat gilt dann $[M : M_0] = \deg g = 2$. Da $K|M_0|M|Z$ eine Kette von

endlichen Körpererweiterungen definiert, finden wir mittels Gradformel $2|[Z:K]$, d.h., $[Z:K] \in 2\mathbb{N}$. Kontraposition liefert nun die Behauptung. $\square$

**Aufgabe 70** Sei $K|\mathbb{Q}$ galoissch und gelte $[K:\mathbb{Q}] = 8$. Ferner sei $G = \mathrm{Gal}(K|\mathbb{Q})$ abelsch aber nicht zyklisch. Wir zeigen, dass genau eine der folgenden Aussagen gilt. (1) $\mathrm{Gal}(K|\mathbb{Q})$ enthält ein Element der Ordnung 4 oder (2) $K|\mathbb{Q}$ hat genau 7 Zwischenkörper vom Erweiterungsgrad 4. Da $K|\mathbb{Q}$ als Galois-Erweterung vom Erweiterungsgrad 8 insbesondere eine endliche Galois-Erweiterung ist, finden wir für die Ordnung der Galois-Gruppe $G$, dass $|G| = [K:\mathbb{Q}] = 8$. Als endliche und nach Voraussetzung abelsche Gruppe können wir $\mathrm{Gal}(K|\mathbb{Q})$ bis auf Isomorphie über den hauptsatz über endlich erzeugte abelsche Gruppen angeben, da jede endliche abelsche Gruppe insbesondere endlich erezugte abelsche Gruppe ist. Das liefert uns, dass $\mathrm{Gal}(K|\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ oder $\mathrm{Gal}(K|\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Der Fall $\mathrm{Gal}(K|\mathbb{Q}) \simeq \mathbb{Z}/8\mathbb{Z}$ scheidet aus, denn $G$ ist als nicht-zyklisch vorausgesetzt. Die beiden verbleibenden Isomorphietypen sind tatsächlich verschieden, da $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ mit $(0,1)$ ein Element der Ordnung 4 besitzt, es aber in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ nur Elemente maximal der Ordnung 2 gibt. Wir sehen, dass im erstgenannten Fall insbesondere $G$ ein Element der Ordnung 4 enthält. Im zweitgenannten Fall verwenden wir, dass wir schreiben können

$$|G| = \sum_{k=1}^{\infty} |\{g \in G | \mathrm{ord}(g) = k\}|. \tag{117}$$

Wie oben festgestellt, hat $(\mathbb{Z}/2\mathbb{Z})^3$ nur Elemente der Ordnung 1 oder 2. Wegen $|G| = 8$ und der Tatsache, dass das Neutralelement in $G$ das einzige Element aus $G$ mit Ordnung 1 ist, finden wir, dass es 7 verschiedene Elemente der Ordnung 2 in $G$ gibt, $g_1, ..., g_7 \in G$ im Zeichen. Diese erzeugen jeweils eine Untergruppe $U_i = \langle g_i \rangle \leq G$ für alle $1 \leq i \leq 7$. Nach dem Hauptsatz der Galois-Theorie gibt es nun zu jeder dieser (paarweise verschiedenen) Untergruppen genau einen Zwischenkörper $Z_i$ der Erweiterung $K|\mathbb{Q}$, sodass $[Z_i:\mathbb{Q}] = (G:U_i) = 4$ nach dem Satz von Lagrange und für $1 \leq i \leq 7$. Da die im Hauptsatz der Galoistheorie definierte Abbildung zwischen Untergruppen der Galoisgruppe und Zwischenkörpern der galoisschen Erweiterung $K|\mathbb{Q}$ bijektiv ist, folgt aus der paarweisen Verschiedenheit von $U_i$ $(1 \leq i \leq 7)$, dass auch die $Z_i$ paarweise verschieden sind und dass es über diese 7 Zwischenkörper hinaus keine weiteren Zwischenkörper der Erweiterung gibt. Das ist gerade der zweite Fall, dessen Eintreten zu verifizieren war. $\square$

**Aufgabe 71** Wir zeigen, dass $\zeta = \sqrt{2}^{-1} + \sqrt{2}^{-1}i$ eine primitive achte Einheitswurzel ist. Nach der Euler'schen Formel gilt $\exp(2\pi i/8) = \exp(\pi i/4) = \cos(\pi/4) + i\sin(\pi/4) = \sqrt{2}+i\sqrt{2}$. Da $\exp(2\pi i/8)$ Nullstelle von $x^8-1 \in \mathbb{Q}[x]$ ist, ist $\exp(2\pi i/8)$ Einheitswurzel. Da ferner $\exp(2\pi ik/8) \neq 1$ für $1 \leq k \leq 7$ aber $\exp(2\pi i \cdot 8/8) = \exp(2\pi i) = 1$, hat $\exp(2\pi i/8)$ Ordnung 8 in der Gruppe $K_8$ der 8-ten Einheitswurzeln, d.h., der Nullstellen von $x^8 - 1$ in $\mathbb{C}$, und wegen $|K_8| = \mathrm{ord}(\exp(2\pi i/8))$ erzeugt also $\exp(2\pi i/8)$ die Gruppe der 8-ten Einheitswurzeln. Damit ist $\exp(2\pi i/8) = \sqrt{2}^{-1} + i\sqrt{2}^{-1}$ also primitive 8-te Einheitswurzel. Wir müssen nun alle echten Zwischenkörper von $\mathbb{Q}(\zeta)|\mathbb{Q}$ bestimmen. Dazu beachten wir, dass $\mathbb{Q}(\zeta)$ ein 8-ter Kreisteilungskörper ist. Also ist $\mathbb{Q}(\zeta)|\mathbb{Q}$ eine Galois-Erweiterung, und da $1 \leq \deg \mu_{\mathbb{Q},\zeta} \leq$

8, ist es auch eine endliche Galois-Erweiterung. Bekannt ist aus der Vorlesung, dass für die Galois-Gruppe des $n$-ten Kreisteilungskörpers über $\mathbb{Q}$ allgemein gilt $\mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times$, wobei $\zeta_n$ eine primitive $n$-te Einheitswurzel mit $n > 2$ ist. Wir finden für $n = 8$ also $\mathrm{Gal}(\mathbb{Q}(\zeta_8 = \zeta)|\mathbb{Q}) = (\mathbb{Z}/2^3\mathbb{Z})^\times = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{3-2}\mathbb{Z} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, wobei die Klassifikation der Einheitengruppe von Restklassenringen aus der Zahlentheorie-Vorlesung verwendet wurde. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ enthält genau $4 - 1 = 3$ Elemente der Ordnung 2, nämlich alle von $(0, 0)$ verschiedenen Elemente. Diese erzeugen genau 3 verschiedene Untergruppen der Galois-Gruppe, die jeweils Ordnung 2 haben, im Zeichen $U_1, U_2, U_3$. Laut Hauptsatz der Galois-Theorie stehen die Zwischenkörper der Erweiterung $\mathbb{Q}(\zeta) : \mathbb{Q}$ in antitonischer Bijektion zu den Untergruppen der Galois-Gruppe. Die echten Zwischenkörper $\mathbb{Q} \subsetneq Z \subsetneq \mathbb{Q}(\zeta)$ korrespondieren hierbei bijektiv zu den nicht-trivialen Untergruppen der Galois-Gruppe der Erweiterung, d.h., zu denjenigen $U \leq \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$, für die gilt $\{\mathrm{id}_{\mathbb{Q}(\zeta)}\} \subsetneq U \subsetneq \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$. Somit können wir bereits feststellen, dass es genau 3 echte Zwischenkörper $Z_1, Z_2, Z_3$ von $\mathbb{Q}(\zeta)|\mathbb{Q}$ gibt. Für diese gilt laut Gradformel weiterhin, dass $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4 = [\mathbb{Q}(\zeta) : Z_i] \cdot [Z_i : \mathbb{Q}]$ laut Gradformel, wobei $1 \neq [Z_i : \mathbb{Q}], 1 \neq [\mathbb{Q}(\zeta) : Z_i]$ gilt, da es sich um echte Zwischenkörper handelt. Wegen $\zeta\bar{\zeta} = 1$, folgt, dass $\zeta \in \mathbb{Q}(\zeta) = \bar{\zeta} = \zeta^{-1} \in \mathbb{Q}(\zeta)$. Also gilt auch $\zeta + \zeta^{-1} = \sqrt{2} \in \mathbb{Q}(\zeta)$. Ferner gilt damit auch $(\zeta - \sqrt{2}^{-1})\sqrt{2} = i \in \mathbb{Q}(\zeta)$ sowie $i \cdot \sqrt{2} \in \mathbb{Q}(\zeta)$. Nun gilt $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{-1}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{-2}) : \mathbb{Q}] = 2$. Da es sich bei $2, -2$ jeweils um verschiedene quadratfreie Zahlen handelt, gilt $\mathbb{Q}(\sqrt{2}) \neq \mathbb{Q}(\sqrt{-2})$. Da $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$ aber $i \notin \mathbb{R}$, gilt bereits $\mathbb{Q}(i) \neq \mathbb{Q}(\sqrt{2})$. Wäre $\sqrt{-2} \in \mathbb{Q}(i)$, gäbe es $p, q \in \mathbb{Q}$, sodass $\sqrt{-2} = p + qi$. Vergleich von Real- und Imaginärtezil liefert $p = 0$ und $q^2 = 2$ im Widerspruch dazu, dass $\sqrt{2}$ bekanntermaßen irrational ist. Also gilt auch $\mathbb{Q}(\sqrt{-2}) \neq \mathbb{Q}(i)$. Insgesamt haben wir also somit drei, und damit alle, echten Zwischenkörper von $\mathbb{Q}(\zeta)|\mathbb{Q}$ gefunden: $Z_1 = \mathbb{Q}(\sqrt{2}), Z_2 = \mathbb{Q}(i), Z_3 = \mathbb{Q}(\sqrt{-2})$. □

**Aufgabe 72 (H16T2A4)** Sei $p > 2$ eine Primzahl, $K = \mathbb{Q}(\zeta_p, \alpha_p)$ und $\alpha_p = \sqrt[p]{p}$ sowie $\zeta_p = \exp(2\pi i/p)$ eine primitive $p$-te Einheitswurzel. Wir zeigen zunächst, dass $\mathbb{Q}(\zeta_p, \alpha_p)|\mathbb{Q}$ galoissch ist. Als Erweiterung, die durch Adjunktion endlich vieler Elemente an $\mathbb{Q}$ entsteht, ist $K|\mathbb{Q}$ endliche und deswegen auch algebraische Körpererweiterung. Als algebraische Erweiterung über einem Körper der Charakteristik 0 ist laut einem Vorlesungsresultat $K|\mathbb{Q}$ bereits separabel. Um zu sehen, dass $K|\mathbb{Q}$ auch normal ist, betrachten wir das Polynom $f = x^p - p \in \mathbb{Q}[x]$. Dieses ist normiert, und laut dem Eisensteinkriterium zur Primzahl $p$ ist es auch ein irreduzibles Polynom über $\mathbb{Z}$, nach dem Gauss'schen Lemma also auch über $\mathbb{Q}$. Wir sehen ferner, dass $f(\alpha_p) = 0$ und zudem $f(\alpha_p\zeta_p^k) = 0$ für alle $1 \leq k \leq p - 1$, da $\zeta_p$ laut Voraussetzung eine primitive $p$-te Einheitswurzel ist. Die Nullstellenmenge von $f$ ist also $N = \{\alpha_p\zeta_p^k | 0 \leq k \leq p - 1\}$. Wir behaupten, dass $\mathbb{Q}(N) = \mathbb{Q}(\zeta_p, \alpha_p)$. Die Inklusion "$\supseteq$" ist bereits klar nach definition, denn $\alpha_p \in N$ und wegen $\alpha_p \neq 0$ und $\alpha_p, \alpha_p\zeta_p \in \mathbb{Q}(N)$ ist laut Körperaxiomen auch $\zeta_p = \alpha_p\zeta_p/\alpha_p \in \mathbb{Q}(N)$. $\mathbb{Q} \subseteq \mathbb{Q}(N)$ ist offensichtlich. Ebenso ist "$\subseteq$" leicht zu sehen, denn mit $\alpha_p, \zeta_p \in K$ ist auch $\zeta_p^k \in K$ für $1 \leq k \leq p - 1$, somit also auch $\alpha_p\zeta_p^k \in K$ für alle $0 \leq k \leq p - 1$, d.h., $N \subseteq K$. Wiederum ist $\mathbb{Q} \subseteq K$ klar, sodass auch $\mathbb{Q}(N) \subseteq K$ folgt. Insgesamt haben wir also $\mathbb{Q}(N) = K$ etabliert. Damit ist $\mathbb{Q}(\zeta_p, \alpha_p)|\mathbb{Q}$ auch normal, denn $\mathbb{Q}(\zeta_p, \alpha_p) = \mathbb{Q}(N)$ ist gerade der Zerfällungskörper von $f$. Wir müssen nun zeigen,

dass $[K:\mathbb{Q}] = p\cdot(p-1)$. Hierzu beachten wir, dass $\zeta_p$ Nullstelle des $p$-ten Kreisteilungspolynoms $\Phi_p(x) = x^{p-1} + x^{p-2} + ... + 1 \in \mathbb{Q}[x]$ ist. Dieses ist irreduzibel über $\mathbb{Q}$ und wir finden, dass $[\mathbb{Q}(\zeta_p):\mathbb{Q}] = \deg \Phi_p = p-1$. Ferner sehen wir, dass $\alpha_p$ Nullstelle von $f$ ist. Als normiertes und irreduzibles Polynom über $\mathbb{Q}$ gilt also $f = \mu_{\mathbb{Q},\alpha_p}$. Wegen $\deg f = p$ finden wir, dass $[\mathbb{Q}(\alpha_p):\mathbb{Q}] = p$. Wegen $\mathrm{ggT}(p-1,p) = p\cdot(p-1)$ finden wir, dass $p(p-1)|[K:\mathbb{Q}]$ infolge der Zwischenkörpereigenschaft $K|\mathbb{Q}(\zeta_p)|\mathbb{Q}$ und $K|\mathbb{Q}(\alpha_p)|\mathbb{Q}$ und Gradformel. Somit gilt $[K:\mathbb{Q}] \geq p(p-1)$. Gleichheit erreichen wir, indem wir beachten, dass $x^p - p = \mu_{\mathbb{Q},\alpha_p}$ impliziert, dass $\mu_{\mathbb{Q}(\zeta_p),\alpha_p}|\mu_{\mathbb{Q},p}$, also insbesondere $\deg \mu_{\mathbb{Q}(\zeta_p),\alpha_p} \leq \deg \mu_{\mathbb{Q},\alpha_p} = p$. Das liefert uns mit der Gradformel die Abschätzung $[K:\mathbb{Q}] = [\mathbb{Q}(\zeta_p)(\alpha_p):\mathbb{Q}(\zeta_p)]\cdot[\mathbb{Q}(\zeta_p):\mathbb{Q}] \leq p\cdot(p-1)$. Zusammen mit dem vorher bewiesenen, konkludieren wir $[k:\mathbb{Q}] = p(p-1)$, wie behauptet. Wir zeigen nun, dass $\mathbb{Q}(\alpha_p)|\mathbb{Q}$ nicht normal ist. Angenommen, die Körpererweiterung wäre normal, gäbe es ein Polynom $g \in \mathbb{Q}[x]$, dessen Zerfällungskörper $\mathbb{Q}(\alpha_p)$ ist. Andererseits haben wir bereits vorher festgestellt, dass $\mu_{\mathbb{Q},\alpha_p} = x^p - p$ die Nullstelle $\alpha_p\zeta_p \notin \mathbb{R}$ hat, da $\zeta_p \in \mathbb{C}\setminus\mathbb{R}$ für alle Primzahlen $p > 2$. Da für jeden Polynom $g \in \mathbb{Q}[x]$, dass $\alpha_p$ als Nullstelle hat, gilt $\mu_{\mathbb{Q},\alpha_p}|g$, hat $g$ ebenfalls eine echt komplexe Nullstelle $\alpha_p\zeta_p$. Da $\sqrt[p]{p} \in \mathbb{R}$, also $\mathbb{Q}(\alpha_p) \subseteq \mathbb{R}$, finden wir, dass es kein Polynom aus $\mathbb{Q}[x]$ geben kann, dass $\alpha_p$ als Nullstelle hat und bereits über $\mathbb{Q}(\alpha_p)$ zerfällt. Somit ist auch $\mathbb{Q}(\alpha_p)|\mathbb{Q}$ nicht normal. Sei nun $G$ die Galoisgruppe von $K|\mathbb{Q}$. Wegen $[K:\mathbb{Q}] = p(p-1)$ gilt $|G| = p(p-1)$. Angenommen, $G$ wäre abelsch. Laut einem Vorlesungsresultat über abelsche Gruppen gäbe es dann eine Untergruppe $U \leq G$ der Ordnung $p-1$, da $p-q|p(p-1)$. Da $G$ ferner abelsch ist, gilt sogar $U \trianglelefteq G$. Da $\mathrm{Gal}(K|\mathbb{Q}(\alpha_p)) = p-1$ nach den Ergebnissen von vorher und der Gradformel, wäre diese dann Normalteiler von $G$. Das bedeutet aber nach einem Vorlesungsresultat, dass $\mathbb{Q}(\alpha_p)|\mathbb{Q}$ normal ist, im Widerspruch zum bereits Gezeigten. Somit ist $G$ nicht-abelsch. Wir zeigen zum Abschluss, dass $G$ einen Normalteiler der Ordnung $p$ hat. Nach dem dritten Sylow-Satz gilt für die Anzahl $\nu_p$ der $p$-Sylowgruppen von $G$ $\nu_p|(p-1)$ und $\nu_p \equiv 1 \bmod(p)$. Wegen $p-1 < p$, ist nur $\nu_p = 1$ möglich. Laut einer Folgerung aus dem zweiten Sylow'schen Satz bedeutet $\nu_p = 1$ gerade, dass die einzige $p$-Sylowgruppe, $P \leq G$, bereits Normalteiler von $G$ ist. Da $p-1 < p$ und $p$ Primzahl, ist somit die einzige $p$-Sylowgruppe $P$ ein Normalteiler der gesuchten Ordnung von $G$. □

**Aufgabe 73 (F14T3A4)** Sei $L$ der Zerfällungskörper von $x^3 - \pi \in \mathbb{Q}(\pi)[x]$ über $\mathbb{Q}(\pi)$. Wir berechnen zunächst $[L:K]$. In $\mathbb{C}$ hat $x^3 - \pi$ die drei Nullstellen $\sqrt[3]{\pi}\zeta_3^k$, wobei $0 \leq k \leq 2$ und $\zeta_3 = \exp(2\pi i/3)$ eine dritte primitive Einheitswurzel ist. Wir zeigen zuerst, dass $L = \mathbb{Q}(\sqrt[3]{\pi}, \zeta_3)$. Klar ist bereits, dass $\mathbb{Q} \subseteq L, \mathbb{Q}(\sqrt[3]{\pi}, \zeta_3)$. Einerseits gilt wegen $L \equiv \mathbb{Q}(\sqrt[3]{\pi}\zeta_3, \sqrt[3]{\pi}\zeta_3^2, \sqrt[3]{\pi})$, dass $\sqrt[3]{\pi}$ und $\zeta_3 = \sqrt[3]{\pi}\zeta_3/\sqrt[3]{\pi} \in L$. Somit ist "$\supseteq$" nachgewiesen. Für "$\subseteq$" bemerken wir, dass wegen $\sqrt[3]{\pi}, \zeta_3 \in \mathbb{Q}(\zeta_3, \sqrt[3]{\pi})$ auch $\sqrt[3]{\pi}\zeta_3, \sqrt[3]{\pi}\zeta_3^2 \in \mathbb{Q}(\zeta_3, \sqrt[3]{\pi})$. Insgesamt etablieren wir also $L = \mathbb{Q}(\zeta_3, \sqrt[3]{\pi})$. Wir zeigen nun, dass $x^3 - \pi$ irreduzibel über $\mathbb{Q}(\pi)$ ist. Da es sich bei dem Polynom aus Gradgründen bereits um eine Nicht-Einheit handelt, nehmen wir für einen Widerspruchsbeweis an, $x^3 - \pi$ wäre reduzibel. Da $x^3 - \pi$ Polynom vom Grad 3 ist, läge dann bereits eine Nullstelle von $x^3 - \pi$ in $\mathbb{Q}(\pi)$. Das bedeutet, es gäbe Polynome $p, q \in \mathbb{Q}[x]$ mit $q \neq 0$, sodass für eine Nullstelle $x_0$ von $x^3 - \pi$ gilt $x_0 = p(\pi)/q(\pi)$. Da $\pi$ transzendent über $\mathbb{Q}$ laut Tipp ist, langt bereits $q \neq 0$ um einen singulären Nenner zu vermeiden. Dann gilt aber $p(\pi)^3 = \pi q(\pi)^3$. Ist die nied-

rigste Potenz, die in $q$ vorkommt, $k$, d.h., $q = \sum_{l=k}^{\deg q} a_l x^l$, dann ist die niedrigste Potenz in $p > k$ und es gilt $\deg p^3 = 3 \cdot \deg p = 1 + 3 \cdot \deg q$, was den Widerspruch $1 \equiv 0 \bmod(3)$ liefert. Man kann auch das Polynom $h(x) \equiv xp(x)^3 + q(x)^3$ definieren und einen Widerspruch zur Transzendenz von $\pi$ erreichen. In jedem Fall stellen wir fest, dass es keine Nullstelle von $x^3 - \pi$ in $\mathbb{Q}(\pi)$ geben kann, d.h., dass $x^3 - \pi$ irreduzibel über $\mathbb{Q}(\pi)$ ist. Für die primitive dritte Einheitswurzel $\zeta_3$ gilt nun $\zeta_3 \in \mathbb{C} \setminus \mathbb{R}$ und $\zeta_3$ ist Nullstelle des 3-ten Kreisteilungspolynoms $\Phi_3(x) = x^2 + x + 1$. Als Polynom vom Grad 2 mit reellen Koeffizienten hat es zwei konjugiert komplexe Nullstellen, die also insbesondere nicht in $\mathbb{Q}(\pi)$ oder $\mathbb{Q}(\sqrt[3]{\pi})$ liegen können: Die beiden letztgenannten Körper sind nämlich Teilkörper von $\mathbb{R}$. Insbesondere ist $\Phi_3$ irreduzibel über $\mathbb{Q}(\sqrt[3]{\pi})$ und $\Phi_3 = \mu_{\mathbb{Q}(\sqrt[3]{\pi}),\zeta_3}$. Da $x^3 - \pi = \mu_{\mathbb{Q}(\pi),\sqrt[3]{\pi}}$ wegen Normiertheit und Irreduzibilität sowie $\sqrt[3]{\pi}^3 - \pi = 0$, liefert uns die Gradformel $[L : \mathbb{Q}(\pi)] = [\mathbb{Q}(\zeta_3, \sqrt[3]{\pi}) : \mathbb{Q}(\sqrt[3]{\pi})][\mathbb{Q}(\sqrt[3]{\pi}) : \mathbb{Q}(\pi)] = \deg \Phi_p \cdot \deg \mu_{\mathbb{Q}(\pi),\sqrt[3]{\pi}} = 2 \cdot 3 = 6$. Wir bestimmen nun die Zwischenkörper der Erweiterung. Hierzu verwenden wir, dass $\mathrm{Gal}(L|\mathbb{Q}(\pi)) = \mathrm{Aut}_{\mathbb{Q}(\pi)}(L) \simeq U$, wobei $U \leq S_3$ ist, da $L$ der Zerfällungskörper von $x^3 - \pi$ ist. Da $|\mathrm{Gal}(L|\mathbb{Q}(\pi))| = [L : \mathbb{Q}(\pi)] = 6$ folgt, dass $U = S_3$ gelten muss. Somit haben wir $\mathrm{Gal}(L|\mathbb{Q}(\pi)) \simeq S_3$. Laut Hauptsatz der Galoistheorie korrespondieren die Zwischenkörper von $L|\mathbb{Q}(\pi)$ bijektiv mit den Untergruppen von $S_3$. Aus der Vorlesung ist bekannt, dass $S_3$ jeweils genau eine Untergruppe der Ordnung $1, 3, 6$ hat und drei verschiedene Untergruppen der Ordnung 2. Diese korrespondieren laut einem Ergebnis der Galois-Theorie zu genau einem Zwischenkörpern vom Erweiterungsgrad 6, 2 bzw. 1 und zu genau drei verschiedenen Zwischenkörpern vom Erweiterungsgrad 3 über $\mathbb{Q}(\pi)$ (in der durch den Erweiterungsgrad vorgegebenen Reihenfolge). Wir bezeichnen diese mit $M_6, M_2, M_1$ und $M_{31}, M_{32}, M_{33}$, wiederum in derselben Reihenfolge, die durch den Erweiterungsgrad vorgegeben ist. Aus notationsökonomischen Gründen bezeichnen wir die entsprechenden Kandidaten bereits als $M_{\text{indizes}}$ und weisen dann nach, dass diese die gewünschten Eigenschaften haben. Es gilt $M_1 = \mathbb{Q}(\pi), M_6 = \mathbb{Q}(\sqrt[3]{\pi}, \zeta_3)$ und $M_2 = \mathbb{Q}(\pi, \zeta_3)$, da $[\mathbb{Q}(\pi)(\zeta_3) : \mathbb{Q}(\pi)] = \deg \Phi_3 = 2$. Bis auf Umnummerierung setzen wir $M_{3,k+1} = \mathbb{Q}(\pi, \sqrt[3]{\pi}\zeta_3^k)$ und behaupten, dass diese Zwischenkörper paarweise verschieden sind. Es ist klar, dass $M_{31} \neq M_{32}$ und $M_{31} \neq M_{33}$ gilt, denn $M_{31} \subseteq \mathbb{R}$ wohingegen $\zeta_3 \in \mathbb{C} \setminus \mathbb{R}$ und damit auch $\sqrt[3]{\pi}\zeta_3 \in \mathbb{C} \setminus \mathbb{R}$. Angenommen, $M_{32} = M_{33}$. Dann gilt insbesondere $\zeta_3^2 \sqrt[3]{\pi} \in M_{32} = \mathbb{Q}(\pi, \sqrt[3]{\pi}\zeta_3)$. Da $\sqrt[3]{\pi}\zeta_3 \in M_{32}$, finden wir $\zeta_3 = \sqrt[3]{\pi}\zeta_3^3/(\sqrt[3]{\pi}\zeta_3) \in M_{32}$. Damit ist auch $\sqrt[3]{\pi} = \sqrt[3]{\pi}\zeta_3/\zeta_3 \in M_{32}$. Das bedeutet aber $M_{32} \subseteq \mathbb{Q}(\sqrt[3]{\pi}, \zeta_3) = M_6$. Wegen $[M_{32} : \mathbb{Q}(\pi)] = \deg(x^3 - \pi) = 3$ ist das ein Widerspruch zu $[M_6 = L : \mathbb{Q}(\pi)] = 6$. Also ist $M_{32} \neq M_{33}$. Da $\sqrt[3]{\pi}\zeta_3^k$ für jedes $0 \leq k \leq 2$ Minimalpolynom $x^3 - \pi$ über $\mathbb{Q}(\pi)$ besitzt, ergibt sich direkt $[M_{3,k+1} : \mathbb{Q}(\pi)]$ für alle $1 \leq k \leq 2$. Somit haben wir die 6 Zwischenkörper der Galoiserweiterung $L|\mathbb{Q}(\pi)$ bestimmt. Da $\mathrm{Gal}(L|\mathbb{Q}(\pi))$ Ordnung 6 hat, sind die drei Untergruppen der Ordnung 2 gerade die drei 2-Sylowgruppen der Galoisgruppe. Diese können nach der Folgerung aus dem zweiten Sylow'schen Satz keine Normalteiler der Galois-Gruppe sein, denn dies ist äquivalent dazu, dass es nur eine 2-Sylowgruppe der Galoisgruppe gibt. Da die Normalteiler der Galoisgruppe bijektiv zu den über $\mathbb{Q}(\pi)$ normalen Erweiterungen korrespondieren, folgt, dass $M_{31}|\mathbb{Q}(\pi), M_{32}|\mathbb{Q}(\pi), M_{33}|\mathbb{Q}(\pi)$ jeweils nicht-normal sind. Als Erweiterung vom Grad 2 ist $M_2|\mathbb{Q}(\pi)$ laut einem Vorlesungsresultat stets normal und $\mathbb{Q}(\pi)|\mathbb{Q}(\pi)$ ist trivialerweise normal. $L|\mathbb{Q}(\pi)$ ist ebenfalls normal, da $L$

bereits als Zerfällungskörper von $x^3 - \pi$ über $\mathbb{Q}(\pi)$ definiert wurde. $\square$

# 6 Kurs im Sommersemester 19

**Aufgabe 74 (F19T2A1)** Eine Kruppe $K$ ist eine nicht-leere Menge zusammen mit einer Verknüpfung $\cdot : K \times K \to K$, die die folgenden Eigenschaften hat. (i) Es gibt ein $e \in K$, sodass $x \cdot e = x$ für alle $x \in K$. (ii) Die Verknüpfung $\cdot$ ist assoziativ. (iii) Für alle $x \in X$ sind die Abbildungen $K \to K, y \mapsto x \cdot y$ und $K \to K, y \mapsto y \cdot x$ injektiv.
(a) Wir zeigen zunächst, dass $e \cdot x = x$ für alle $x \in K$. Aus dem Axiom (i) folgt für beliebiges $x \in K$, $x \cdot e = x$. Damit schreiben wir $e \cdot x = e \cdot (x \cdot e) = (e \cdot x) \cdot e = x$, wobei wir die Assoziativität der Verknüpfung nach (ii) verwendet haben. Wiederum wegen (i) gilt zudem $x \cdot e = x$. Das Axiom (iii) liefert, dass die Abbildung $K \to K, y \mapsto y \cdot e$ injektiv ist. Damit finden wir wegen $x = x$, dass $e \cdot x = x$ nach Definition einer injektiven Abbildung. Beliebigkeit von $x$ zeigt also, dass neben dem in (i) postulierten rechtsneutralen Element $e$, dieses auch linksneutral ist.
(b) Seien nun $x, y \in K$ mit $y \cdot x = x$. Zu zeigen ist, dass dann $y = e$. Im Falle $y = e$ ist nichts zu zeigen und wir können uns auf die Untersuchung des Falls $y \neq e$ beschränken. Dann wäre allerdings $e \cdot x = x$ und $y \cdot x = x$. Da nach Axiom (iii) die Rechtsmultiplikation injektiv ist, folgt aus $e \cdot x = x = y \cdot x$ bereits $y = e$ im Widerspruch zur Annahme $y \neq e$. Damit war die Annahme falsch und es gilt $y = e$, wie behauptet.
(c) Sei nun vorausgesetzt, dass $K$ eine nicht-leere endliche Menge mit Kruppenstruktur sei. Zu zeigen ist, dass $K$ dann eine Gruppe bzgl. der Kruppenmultiplikation ist. Wir stellen zunächst fest, dass $K \to K, x \mapsto x \cdot y$ und $K \to K, x \mapsto y \cdot x$ als injektive Abbildungen zwischen gleichmächtigen endlichen Mengen jeweils Bijektionen sind. Sei nun $e$ das, nach (a) beidseitige, Neutralelement der Kruppe und $y \in K$ beliebig. Dann gibt es wegen der Bijektivität der o.g. Abbildungen eindeutige $x_1, x_2 \in K$, sodass $x_1 \cdot y = e = y \cdot x_2$. Damit haben wir zu festem $y$ jeweils ein Links- und Rechtsinverses gefunden. Wir müssen noch zeigen $x_1 = x_2$. Hierzu multiplizieren wir $x_1 \cdot y = e$ von rechts mit $x_2$ und nutzen auf der linken Seite die Assoziativität der Verknüpfung und auf der rechten Seite die Neutralität des Elements $e \in K$. Dann finden wir $x_1 = x_1 \cdot e = x_1 \cdot (y \cdot x_2) = x_1 \cdot y \cdot x_2 = (x_1 \cdot y) \cdot x_2 = e \cdot x_2 = x_2$, also $x_1 = x_2$. Damit fallen links- und rechtsinverses Element zu einem vorgegebenen $y \in K$ zusammen. Wir bezeichnen dieses dann mit $y^{-1}$, wie üblich. Da $K$ bereits unter $\cdot$ abgeschlossen ist (als Kruppe), die Verknüpfung $\cdot$ assoziativ ist (Axiom (ii)) und ein eindeutiges neutrales Element (a und b, Axiom (i)) existiert, haben wir mit der eindeutigen Existenz eines inversen Elements zu einem Kruppenelement $y \in K$ bzgl. der Verknüpfung $\cdot$ den Nachweis erbracht, dass im Falle endlicher nicht-leerer Mengen $K$, die Kruppe $K$ auch eine Gruppe ist.
(d) Wir behaupten, dass $(\mathbb{N}_0, +)$ eine Kruppe ist. Hierbei ist klar, dass $\mathbb{N}_0^+$ unter $+ : \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0, (n, m) \mapsto n + m$ abgeschlossen ist. Ferner ist $+$ auch assoziativ, da aus der Vorlesung bekannt ist, dass $(\mathbb{N}_0, +)$ ein Monoid ist mit Neutralelement 0. Da $+$ eine kommutative Verknüpfung ist, beschränken wir uns auf den Nachweis, dass $\mathbb{N}_0 \to \mathbb{N}_0, m \mapsto n + m$ injektiv ist für eine beliebiges aber festes $n \in \mathbb{N}_0$. Seien dazu $m_1, m_2$ mit $m_1 \neq m_2$ aber $n + m_1 = n + m_2$ vorgegeben. Wir können wie in $\mathbb{Z}$ sub-

trahieren, müssen aber gewährleisten, dass wir am Ende nicht-negative Ganzzahlen herausbekommen. Da $n, m_1, m_2 \geq 0$, folgt aus $n + m_1 = n + m_2$ nach "Substraktion" von $n$, $m_1 = m_2$. Das ist aber ein Widerspruch zu $m_1 \neq m_2$ laut Annahme. Also war die Annahme falsch. Damit ist für jedes beliebige $n \in \mathbb{N}_0$ die Abbildung $\mathbb{N}_0 \to \mathbb{N}_0, m \mapsto m+n$ injektiv. Wegen der eingangs gemachten Bemerkung ist damit auch $\mathbb{N}_0 \to \mathbb{N}_0, m \mapsto n + m$ für beliebige $n \in \mathbb{N}_0$ injektiv. Insgesamt haben wir also gezeigt, dass $(\mathbb{N}_0, +)$ eine Kruppe ist. □

**Aufgabe 75 (F19T2A2)** Sei $G \neq \{1_G\}$ eine endliche Gruppe, für welche die Automorphismengruppe $A := \mathrm{Aut}(G)$ transitiv auf $G \setminus \{1_G\}$ operiere.
(a) Zu zeigen ist, dass es eine Primzahl $p$ gibt, sodass $x^p = 1_G$ für alle $x \in G$. Nach Voraussetzung ist $|G| < \infty$. Zu einem beliebigen $X \in G$ ist also $\mathrm{ord}(X)|G$ und wegen $G \neq \{1_G\}$ gibt es mindestens ein $X \in G \setminus \{1_G\}$, sodass $\mathrm{ord}(X) > 1$. Wähle also ein beliebiges $X \in G$ mit $\mathrm{ord}(X) > 1$. Falls $\mathrm{ord}(X)$ eine Primzahl, $p$, ist, gilt $X^p = 1_G$. Für beliebiges $Y \in G \setminus \{1_G\}$ gibt es dann ein $\alpha_Y \in A$ sodass $\alpha_Y(X) = Y$. Nun gilt $Y^p = (\alpha_Y(X))^p = (\alpha_Y(X^p)) = \alpha_Y(1_G) = 1_G$ wegen der Homomorphismuseigenschaften von $\alpha_y \in A$. Da $Y$ beliebig war und stets $1_G^p = 1_G$ gilt, haben wir im Falle, dass $\mathrm{ord}(X) > 1$ eine Primzahl ist, die angegebene Gleichung verifiziert. Falls $\mathrm{ord}(X) > 1$ keine Primzahl ist, ist zumindest $\{1_G\} \subsetneq \langle X \rangle \subseteq G$ eine endliche zyklische Gruppe und damit abelsch. Daher existiert ein $Z \in \langle X \rangle \subset G$ mit $Z \neq 1_G$ und $\mathrm{ord}(Z)|\mathrm{ord}(X)$ als Primteiler. Wir wenden nun Teil (a) auf $Z$ anstelle von $X$ and und finden so eine Primzahl $p_Z$, sodass $X^{p_Z} = 1_G$ für alle $X \in G$. Damit ist gezeigt, dass es unter den Voraussetzungen stets eine Primzahl $p$ gibt, sodass $X^p = 1_G$ für alle $X \in G$.
(b) Zu zeigen ist nun $Z(G) \neq \{1_G\}$. Es ist klar, dass $\{1_G\} \subset Z(G)$, da $1_G$ das Neutralelement von $G$ ist. Zu zeigen ist also, dass es ein $X \in G \setminus \{1_G\}$ gibt, sodass $X \in Z(G)$. Sei $X \in G \setminus \{1_G\}$ beliebig. Nach (a) gilt dann $X^p = 1_G$ für eine geeignete Primzahl $p$. Nun gilt $X \cdot 1_G = X = 1_G \cdot X$. Zu zeigen ist also, dass für beliebiges $Y \in G \setminus \{1_G\}$ gilt $XY = YX$. Wir stellen zunächst fest, dass wegen (a) $\mathrm{ord}(X) \in \{1, p\}$ für alle $X \in G$ ist. Damit ist $G$ eine $p$-Gruppe. Aus der Vorlesung ist bekannt, dass $p$-Gruppen ein nicht-triviales Zentrum haben, d.h., $\{1_G\} \subsetneq Z(G)$, wie behauptet.
(c) Zu zeigen ist nun, dass $G$ abelsch ist. Da $Z(G) \neq \{1_G\}$, gibt es ein $x \in Z(G)$ mit $x \neq 1_G$. Für beliebiges $y \in G$ gilt dann $xy = yx$. Sei nun $g \in G \setminus \{1_G\}$ beliebig und bezeichne $\alpha_G \in A$ den Automorphismus mit $\alpha_g(x) = g$ (Transitivität). Dann gilt $\alpha_g(xy) = \alpha_g(x)\alpha_g(y) = g \cdot h$, wobei $h \in G$ alle Werte annimmt, wenn $y$ ganz $G$ durchläuft. Analog finden wir für die rechte Seite der Gleichung $\alpha_g(yx) = \alpha_g(y)\alpha_g(x) = h \cdot g$. Damit ist gezeigt, dass auch $hg = gh$ für festes $g$ und alle $h \in G$. Wegen $1_G \in Z(G)$ und $Z(G) \leq G$, haben wir insgesamt gezeigt $Z(G) = G$. Das ist laut Vorlesung gleichbedeutend damit, dass $G$ abelsch ist. □

**Aufgabe 76 (F19T3A5)** Zu zeigen ist, dass $S_5$ nicht isomorph zu $A_5 \times \mathbb{Z}_2$ ist. Angenommen, $A_5 \times \mathbb{Z}_2$ wäre isomorph zu $S_5$ vermöge $\psi : A_5 \times \mathbb{Z}_2 \to S_5$. Dann ist $\psi(A_5 \times \{0\}) = A_5$, da $A_5$ der (einzige) Index 2 Normalteiler von $S_5$ ist und $A_5 \times \{0\} \trianglelefteq A_5 \times \mathbb{Z}_2$. Sei nun $(\alpha, \gamma) \in A_5 \times \mathbb{Z}_2$ beliebig. Dann gilt $(\alpha, \gamma) \cdot (0, \beta) = (\alpha, \gamma\beta = \beta\gamma) = (0, \beta) \cdot (\alpha, \gamma)$ für $\beta \in \mathbb{Z}_2$ beliebig. Also ist auch $\{0\} \times \mathbb{Z}_2 \trianglelefteq A_5 \times \mathbb{Z}_2$. Da

Gruppenisomorphismen die Normalteilereigenschaft erhalten, muss auch $\psi(\mathbb{Z}_2) \trianglelefteq S_5$ gelten, wobei das Bild ein Normalteiler der Ordnung 2 ist. Andererseits ist aus der Vorlesung bekannt, dass der einzige (nicht-trivialer) Normalteiler von $S_5$ gerade $A_5$ ist. Damit haben wir einen Widerspruch und $S_5$ ist nicht isomorph zum direkten Produkt von $A_5$ und $\mathbb{Z}_2$. □

**Aufgabe 77 (H15T2A1)** Gesucht sind alle Matrizen $A \in \mathrm{GL}(2, \mathbb{C})$, die mit der Matrix

$$X = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \tag{118}$$

kommutieren. Wir setzen

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2, \mathbb{C}). \tag{119}$$

Dann müssen die Einträge $a, b, c, d \in \mathbb{C}$ erfüllen $ad - bc \neq 0$ und

$$XA = \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix} = \begin{pmatrix} a & a+b \\ c & d \end{pmatrix} = AX. \tag{120}$$

Damit finden wir $c = 0$, $a = d$. Zusammen mit $ad - bc \neq 0$ finden wir also, dass $A \in M$, wobei

$$M = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a \in \mathbb{C} \setminus \{0\},\, b \in \mathbb{C} \right\}. \tag{121}$$

□

**Aufgabe 78 (F19T1A1(c))** Wir sollen drei nicht-isomorphe Gruppen der Ordnung 12 angeben. Wir setzen $G_1 := D_6$, die Symmetriegruppe des regelmäßigen 6-Ecks. Zudem setzen wir $G_2 := \mathbb{Z}_3 \times \mathbb{Z}_4$ und $G_3 := \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Offenbar haben $G_1, G_2, G_3$ jeweils Ordnung 12. Aus der Vorlesung ist bekannt, dass $D_6$ nicht-abelsch ist, wohingegen die als direkte Produkte zyklischer Faktoren definierten Gruppen $G_2, G_3$ abelsch sind. Wir verwenden im Folgenden die Schreibweise für abelsche Gruppe für $G_2, G_3$. Damit kann zumindest $G_1$ nicht isomorph zu $G_2, G_3$ sein. Wir stellen ferner fest, dass $(1,1) \in G_2$ ein Element der Ordnung 12 ist. Denn $12 \cdot (1,1) = (12,12) = (0,0)$ und für die Primteiler $\{2,3\}$ von 12 gilt $12/2 \cdot (1,1) = 6 \cdot (1,1) = (6,6) = (0,2) \neq (0,0)$ sowie $12/3 \cdot (1,1) = 4 \cdot (1,1) = (1,0) \neq (0,0)$. Damit gibt es keine kleinere natürliche Zahl $n$ als 12, die $n \cdot (1,1) = (0,0)$ in $G_2$ erfüllt und wir finden $\mathrm{ord}_{G_2}((1,1)) = 12$. Andererseits gilt für alle $(a,b,c) \in G_3$, dass $\mathrm{ord}((a,b,c)) \leq 6$, denn $6 \cdot (a,b,c) = (2 \cdot (3 \cdot a), 3 \cdot (2 \cdot b), 3 \cdot (2 \cdot c)) = (2 \cdot 0, 3 \cdot 0, 3 \cdot 0) = (0,0,0)$ in $G_3$. Damit gibt es kein Element der Ordnung 12 in $G_3$. Das bedeutet aber bereits, dass $G_2, G_3$ nicht isomorph sein können, denn dann gäbe es einen bijektiven, insbesondere also injektiven Gruppenhomorphismus $\Phi : G_2 \to G_3$. Insbesondere würde $(1,1)$ auf ein Element der Ordnung 6 oder der Ordnung $q$, $q|6$ abgebildet werden. Letzteres widerspricht der Injektivität von $\Phi$. Damit sind auch $G_2$ und $G_3$ nicht isomorph. □

**Aufgabe 79 (H05T3A1(a))** Gesucht sind alle Isomorphietypen von abelschen Gruppen der Ordnung 56. Da abelsche Gruppen endlicher Ordnung notwendigerweise endlich erzeugt sind, können wir den Elementarteilersatz anwenden. Die Elementarteilerketten sind $1|56$, $1|2|28$, $1|2|2|14$. Das liefert uns die Kandidaten $G_1 := \mathbb{Z}_{56}$, $G_2 = \mathbb{Z}_2 \times \mathbb{Z}_2 8$, $G_3 = \mathbb{Z}_2 \times \mathbb{Z}_{14}$. Diese Gruppen sind paarweise nicht isomorph aus Ordnungsgründen: $G_1$ enthält als zyklische Gruppe der Ordnung 56 ein Element der Ordnung 56, $G_2$ enthält Elemente der Ordnung maximal 28 und mit $(0,1) \in G_2$ mindestens ein Element der Ordnung 28. $G_3$ schließlich enthält Elemente maximal der Ordnung 14 und mit $(0,0,1) \in G_3$ mindestens ein Element der Ordnung 14. Annahme der Isomorphie zwischen zwei verschiedenen dieser Gruppentypen führt auf einen Widerspruch zur Injektivitätseigenschaft des Isomorphismus. Da der Elementarteilersatz die endlichen abelschen Gruppen abschließend klassifiziert und wir nachgewiesen haben, dass die resultierenden Isomorphietypen tatsächlich paarweise verschieden sind, ist jede abelsche Gruppe der Ordnung 56 isomorph genau zu einer der Gruppen $G_1, G_2$ bzw. $G_3$. □

**Aufgabe 80 (F06T2A1)** Sei $(G,+)$ eine abelsche Gruppe und $U, V \leq G$ Untergruppen. Zu zeigen ist die Äquivalenz von (i) $G = U \oplus V$ und (ii) für alle $a, b \in G$ haben die Linksnebenklassen $a+U$ und $b+V$ genau ein Element gemeinsam. Für (ii) $\Rightarrow$ (i) müssen wir zeigen, dass (a) $U \cap V = \{0\}$ und (b) $G = U + V$. Wir setzen $a = 0 = b$ in (ii). Dann gilt, dass $0 + V = V$ und $0 + U = U$ genau ein Element gemein haben. Da $0 \in U$ und $u \in V$, wissen wir bereits, dass dies nur das neutrale Element 0 von $G$ sein kann. Mithin gilt Bedingung (a). Für (b) reicht es zu zeigen, dass $G \subseteq U+V$. Wegen $U, V \leq G$ ist $U+V \subseteq G$ bereits klar. Sei also $g \in G$ beliebig. Zu zeigen ist, dass $g \in U + V$. Wir setzen in (ii) $a = g$ und $b = 0$. Dann gibt es ein $v \in V$, sodass mit einem $u \in U$ gilt $g + u = v$, denn $g + U$ und $V$ haben genau ein gemeinsames Element. Durch die Einelementigkeit des Schnitts $(g+U) \cap V$ sind $u, v$ ferner eindeutig festgelegt. Da $U$ Gruppe ist, ist auch $-u \in U$ und wir finden aus $g+u = v$, dass $g = (-u)+v$. Damit ist $g \in U+V$ nachgewiesen und Beliebigkeit von $g \in G$ impliziert die Inklusion $G \subseteq U + V$. Wir müssen noch (i) $\Rightarrow$ (ii) nachweisen. Da $G = U + V$ gilt einerseits $U \cap V = \{0\}$ und andererseits gibt es für jedes $g \in G$ $u \in U$ sowie $v \in V$ mit $g = u + v$. Sei nun ein weiteres Element $g' = u' + v' \in U + V$ gegeben. Zu zeigen ist, dass $g + U$ und $g' + V$ genau ein Element gemein haben. Zunächst gilt $g + u'' = g' + v''$ mit $u'' \in U$ und $v'' \in V$ beliebig für Elemente des Schnitts der beiden Linksnebenklassen. Einsetzen von $g = u + v$ und $g' = u' + v'$ liefert $(u + u'') + v = u' + (v' + v'')$ unter Verwendung der Kommutativität Untergruppen abelscher Gruppen sowie des Assiziativgesetzes. Existenz der eindeutigen Inversen liefert $u + u'' - u' = v' + v'' - v$. Die linke Seite der Gleichung nimmt Werte nur in $U$ an (Abgeschlossenheit von Untergruppen) und analog nimmt die rechte Seite der Gleichung nur Werte in $V$ an. Da laut (i) bereits $U \cap V = \{0\}$, erhalten wir die beiden Gleichungen $u + u'' - u' = 0$ sowie $v' + v'' - v = 0$. Umformung liefert nun $u'' = u' - u$ sowie $v'' = v - v'$. Damit sind $u''$ bzw. $v''$ eindeutig festgelegt und wir haben mit $u' + v \in (g + U) \cap (g' + V)$ das eindeutige Element des Schnitts der beiden Linksnebenklassen gefunden. □

**Aufgabe 81 (F13T2A1)** Wir zeigen zuerst, dass alle Elemente der Faktorgruppe $\mathbb{Q}/\mathbb{Z}$ endliche Ordnung haben. Die Elemente der Faktorgruppe sind Links-Nebenklassen der Form $[q] = \{q' \in \mathbb{Q} | q' - q \in \mathbb{Z}\}$. Wir wählen das Repräsentantensystem durch $R = \{q \in \mathbb{Q} | 0 \leq q < 1\}$. Wir skizzieren den Nachweis der Repräsentantensystemeigenschaft: Durch Schreiben der Elemente einer beliebigen Linksnebensklasse in Dezimalbruchschreibweise, ist klar, dass diese Linksnebenklasse ein Element aus $R$ enthält. Umgekehrt liegt in jeder Linksnebenklasse auch höchstens ein Element aus $R$, denn andernfalls wäre $r_1 - r_2 \in \mathbb{Z}$ für $r_1, r_2 \in R$ mit $r_1 > r_2$, was im Widerspruch zur Bedingung, dass $r \in R \Rightarrow r < 1$, steht. Nach Definition von $\mathbb{Q}$ als Quotientenkörper des faktoriellen Rings $\mathbb{Z}$, können wir jedes Element $[q] \in \mathbb{Q}/\mathbb{Z}$ durch einen Repräsentanten $r \in R$ in der Schreibweise eines vollständig gekürzten Bruchs auffassen:

$$r = \frac{m}{n} \text{ mit } 0 \leq m < n, \text{ ggT}(m, n) = 1. \tag{122}$$

Wir behaupten, dass dann $\text{ord}_{\mathbb{Q}/\mathbb{Z}}([q]) = n$ für alle $[q] \in \mathbb{Q}/\mathbb{Z}$. Denn es gilt für $q \in [q]$, dass $q = k + r$, wo $k \in \mathbb{Z}$ und somit $n \cdot q = nk + nr = nk + m \in \mathbb{Z}$. Damit wissen wir $n \cdot [q] = [0]$, und letzteres ist das Neutralelement von $\mathbb{Q}/\mathbb{Z}$. Die für die Ordnung erforderliche Minimalität des so gefundenen $n$ ist durch die Teilerfremdheit von Zähler und Nenner eines vollständig gekürten Bruchs gewährleistet. Damit ist die Ordnung jedes Elements der Faktorgruppe endlich. Wir zeigen nun, dass die Menge $M$ der Elemente endlicher Ordnung in $\mathbb{R}/\mathbb{Z}$ gerade $M = \mathbb{Q}/\mathbb{Z}$ erfüllt. Wegen des oben bewiesenen, $M \supseteq \mathbb{Q}/\mathbb{Z}$, da $\mathbb{Q} \leq \mathbb{R}$ auch $\mathbb{Q}/\mathbb{Z} \leq \mathbb{R}/\mathbb{Z}$ liefert nach dem Korrespondenzprinzip. Wir zeigen nun $M \subseteq \mathbb{Q}/\mathbb{Z}$. Sei dazu $\alpha \in [0, 1) \subseteq \mathbb{R}$ Repräsentant von $[R] \in \mathbb{R}/\mathbb{Z}$. Dann ist $[R] = \alpha + \mathbb{Z}$. Da $[R] \in M$, gibt es ein $N \in \mathbb{N}$, sodass $N \cdot (\alpha + \mathbb{Z}) = 0 + \mathbb{Z}$, was bedeutet $N \cdot \alpha \in \mathbb{Z}$. Damit gibt es ein $K \in \mathbb{Z}$, sodass $N \cdot \alpha = K$, also $\alpha = K/N \in \mathbb{Q}$ und dieses $K$ kann durch ggf. Umwandlung in Dezimalbrüche als $0 \leq K < N$ mit $\text{ggT}(K, N) = 1$ gewählt werden. Letzteres folgt aus der Faktoriellität von $\mathbb{Z}$ als Ring. Damit ist aber $\alpha + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$. Beliebigkeit von $\alpha + \mathbb{Z} \in M$ liefert nun die Inklusion $M \subseteq \mathbb{Q}/\mathbb{Z}$. Mithin bleibt $\mathbb{Q}/\mathbb{Z} = M$ zusammenfassend zu konstatieren. Zuletzt zeigen wir, dass die Menge $O$ der Elemente endlichen Ordnung in $\mathbb{R}/\mathbb{Q}$ gerade in der Menge $\{0\}$ enthalten sind. Es ist klar, dass $0 + \mathbb{Q}$ als Neutralelement der Faktorgruppe $\mathbb{R}/\mathbb{Q}$ von Ordnung 1 und damit insbesondere von endlicher Ordnung ist. Angenommen, $\alpha + \mathbb{Q}$ mit $\alpha \notin \mathbb{Q}$ wäre ein weiteres Element endlicher Ordnung $\text{ord}_{\mathbb{R}/\mathbb{Q}}(\alpha + \mathbb{Q}) = N' \in \mathbb{N}$. Dann gilt $N'\alpha \in \mathbb{Q}$ und es gibt einen vollständig gekürzten Bruch $q = Z/N \in \mathbb{Q}$, sodass $N'\alpha = Z/N$. Da $N' \neq 0$ liefert die Abgeschlossenheit von $\mathbb{Q}$ unter Multiplikation mit Elementen aus $\mathbb{Q}^\times$, dass $\alpha = Z/(NN') \in \mathbb{Q}$. Dieses Ergebnis widerspricht $\alpha \notin \mathbb{Q}$. Somit war die Annahme, es gäbe ein nicht-rationales $\alpha$ mit $\text{ord}_{\mathbb{R}/\mathbb{Q}}(\alpha + \mathbb{Q}) \in \mathbb{N}$ falsch. Mithin ist $0 + \mathbb{Q}$ tatsächlich das einzige Element endlicher Ordnung in $\mathbb{R}/\mathbb{Q}$. □

**Aufgabe 82 (F13T1A3)** Sei $G := \text{SL}(2, \mathbb{F}_7) = \{A \in \mathbb{GL}(2, \mathbb{F}_7) | \det(A) = 1\}$ und $H = \{E_2 + a \cdot e_{12} | a \in \mathbb{F}_7\}$, wobei $e_{kl}$ die Elementarmatrix bezeichnet, die den Eintrag 1 an der Stelle $(k, l)$ hat und sonst mit 0 befüllt ist. $E_2$ ist die $2 \times 2$ Einheitsmatrx mit Einträgen aus $\mathbb{F}_7$.
(a) Wir zeigen zuerst, dass $H \leq G$ und $|H| = 7$. Zunächst gilt für $A = E_2 + a \cdot e_{12} \in H$ mit $a \in \mathbb{F}_7$ beliebig gewählt, dass $\det(A) = \det(E_2 + a \cdot e_{12}) = 1 \cdot 1 + a \cdot 0 = 1$, sodass

$A \in G$. Beliebigkeit von $a \in \mathbb{F}_7$ impliziert Beliebigkeit von $A \in H$ und liefert $H \subseteq G$. Wir stellen ferner fest, dass $A \in H \Rightarrow A^{-1} \in H$, denn $B := (E_2 - a \cdot e_{12}) \in H$ erfüllt $BA = (E_2 - ae_{12})(E_2 + a \cdot e_{12}) = E_2 + (a - a)e_{12} = E_2$. Eindeutigkeit des inversen liefert, dass $B = A^{-1}$ in $G$ und, wegen $B \in H$, $A^{-1} \in H$. Wir zeigen nun, dass zu $A = E_2 + a \cdot e_{12}, B = E_2 + b\dot{e}_{12} \in H$ für beliebige $a, b \in \mathbb{F}_7$ auch $AB^{-1} \in H$. Es ist $H \ni B^{-1} = E_2 - be_{12}$ und wir finden $AB^{-1} = E_2 + (a - b)e_{12} \in H$, da mit $a, b \in \mathbb{F}_7$ auch $a - b \in \mathbb{F}_7$. Damit ist die Untergruppeneigenschaft $H \leq G$ nachgewiesen. Wir zeigen nun, dass $|H| = 7$ und beachten, dass durch die Zuweisung $\Pi : \mathbb{F}_7 \to H, a \mapsto E_2 + ae_{12}$ ein, wie unmittelbar ersichtlich, Gruppenisomorphismus zwischen $(\mathbb{F}_7, +)$ und $(H, \cdot)$ gegeben ist. Insbesondere ist $\Pi$ bijektiv und die Tatsache, dass $\mathbb{F}_7$ der endliche Körper mit genau 7 Elementen ist, liefert $|H| = |\mathbb{F}_7| = 7$.
(b) Wir zeigen nun, dass $|G| = 336$. Zu diesem Zwecke definieren wir den Gruppenhomomorphismus $\det : \mathrm{GL}(2; \mathbb{F}_7) \to \mathbb{F}_7^\times, A \mapsto \det(A)$ in die Einheitengruppe des Körpers $\mathbb{F}_7$, $\mathbb{F}_7^\times = \mathbb{F}_7 \setminus \{0\}$. Nach Definition von $G$, $\ker \det = G$. Die Homomorphismeneigenschaft der Determinantenabbildung wird hier als bekannt vorausgesetzt. Die Matrix $A = ae_{11} + e_{22} \in \mathrm{GL}(\mathbb{F}_7)$ für $a \in \mathbb{F}_7^\times$ hat $\det A = a$, sodass det Gruppenepimorphismus, also insbesondere surjektiv, ist. Nach dem Homomorphiesatz und dem Satz von Lagrange gilt $|G| = |\ker \det| = |\mathrm{GL}(2, \mathbb{F}_7)|/|\mathbb{F}_7^\times| = |\mathrm{GL}(2; \mathbb{F}_7)|/6$. Wir bestimmen also die Anzahl der Elemente in $\mathrm{GL}(2, \mathbb{F}_7)$. Sei dazu $v_1 \in \mathbb{F}_7^2 \setminus \{(0, 0)\}$ nicht-trivialer (erster) Spaltenvektor einer Matrix $A = (v_1|v_2) \in \mathrm{GL}(2, \mathbb{F}_7)$. Wir haben für $v_1$ genau $7^2 - 7^0 = 7^2 - 1 = 48$ Möglichkeiten. Wegen $A \in \mathrm{GL}_2(\mathbb{F}_7) \Leftrightarrow v_1 \neq (0, 0) \wedge v_2 \notin \mathbb{F}_7 \cdot v_1$, haben wir $7^2 - 7^1 = 42$ Möglichkeiten, $v_2$ zu wählen, um ein $A \in \mathrm{GL}(2, \mathbb{F}_7)$ zu fixieren. Damit folgt $|\mathrm{GL}(2, \mathbb{F}_7)| = 48 \cdot 42$ und, wegen der obigen Überlegungen, $|G| = 42 \cdot 48/6 = 7 \cdot 48 = 336$.
(c) Gesucht ist die Anzahl der Untergruppen der Ordnung 7 von $G$. Aus der letzten Teilaufgabe erhalten wir die Primfaktorzerlegung $|G| = 7 \cdot 2^4 \cdot 3$. Da $7^1$ die höchste $p = 7$-Potenz ist, die $|G|$ teilt, sind die Untergruppen der Ordnung 7 von $G$ genau die 7-Sylowgruppen von $G$. Bezeichne deren Anzahl mit $\nu_7$. Infolge der dritten Sylowschen Satzes gilt $\nu_7 || G|/7^1 = 2^4 \cdot 3$, also $\nu_7 \in \{1, 2, 4, 8, 16, 3, 6, 12, 24, 48\}$. Der dritte Sylow'sche Satz besagt darüber hinaus, $\nu_7 \equiv 1 \bmod(7)$. Damit reduzieren wir die Möglichkeiten, die für $\nu_7$ zur Verfügung stehen, auf $\nu_7 = 1$ oder $\nu_7 = 8$. In Teilaufgabe (a) hatten wir bereits gesehen, dass $H$, definiert wie oben, eine Untergruppe der Ordnung 7 und damit eine 7-Sylow-Gruppe von $G$ ist. Es reicht aus, die Existenz einer weiteren Untergruppe der Ordnung 7 von $G$ nachzuweisen, denn dann ist bereits $\nu_7 \neq 1$, also $\nu_7 = 8$. Wir definieren $H^T \equiv \{E_2 + a \cdot e_{21} | a \in \mathbb{F}_7\}$. Diese Menge enthält gerade die Transponierte aller Element aus $H$. Mittels der rechnerischen Eigenschaften der Matrixtransposition verifiziert man sofort $H^T \leq G$. Da die Transposition auf der Gruppe quadratischen, invertierbaren Matrizen ein Anti-Gruppenisomorphismus ist, folgt $7 = |H| = |H^T|$. Zuletzt stellen wir fest, dass $E_2 + e_{21} \in H^T$ aber $E_2 + e_{21} \notin H$, sodass $H \neq H^T$. Damit haben wir mit $H^T$ eine weitere, von $H$ verschiedene Untergruppe der Ordnung 7 von $G$ gefunden. Infolge des oben Gesagten ist $H^T$ also ebenfalls eine 7-Sylow-Gruppe von $G$, was, wie ebenfalls oben skizziert, $\nu_7 = 1$ ausschließt. Folglich gilt $\nu_7 = 8$. Damit gibt es genau 8 Untergruppen der Ordnung 7 in $G = \mathrm{SL}(2, \mathbb{F}_7)$. □

**Aufgabe 83 (F19T3A2)** Sei $G$ eine Gruppe und für $x, y, g \in G$ sei $(x, y) \bullet g := xgy^{-1}$.
(a) Wir zeigen, dass $\bullet : (G \times G) \times G \to G, ((x, y), g) \mapsto (x, y) \bullet g$ eine transitive Gruppenoperation definiert. Wegen Abgeschlossenheit von $G$ unter Multiplikation und Inversenbildung ist die Wohldefiniertheit der Abbildung klar. Das neutrale Element in $G \times G$ ist $(e, e)$, wobei $e$ das Neutralelement von $G$ ist. Es gilt nun $\bullet((e, e), g) = (e, e) \bullet g = ege^{-1} = ege = eg = g$ für alle $g \in G$. Sei nun $(g_1, h_1)$, $(g_2, h_2) \in G \times G$ beliebig. Dann gilt für jedes $g \in G$, dass $\bullet((g_1, h_1), \bullet((g_2, h_2), g)) = (g_1, h_1) \bullet ((g_2, h_2) \bullet g) = g_1(g_2 g h_2^{-1})h_1^{-1} = (g_1 g_2)g(h_2^{-1}h_1^{-1}) = (g_1 g_2)g(h_1 h_2)^{-1} = \bullet((g_1 g_2, h_1 h_2), g) = \bullet((g_1, h_1) \cdot (g_2, h_2), g)$. Damit ist nachgewiesen, dass es sich bei $\bullet$ um eine Gruppenoperation von $G \times G$ auf $G$ handelt. Wir zeigen nun noch die Transitivität der Operation. Dazu ist zu zeigen, dass $G = (G \times G)(e)$, d.h., dass es lediglich eine, ganz $G$ enthaltende, Bahn gibt. In der Tat, sei $g \in G$ beliebig. Wir zeigen $g \in (G \times G)(e)$ indem wir $(g, e) \in G \times G$ auf $e \in G$ operieren lassen. Dann gilt $(g, e) \bullet e = gee^{-1} = gee = ge = g$, sodass $g \in (G \times G)(e)$, wie behauptet. Beliebigkeit von $g \in G$ impliziert nun $G \subseteq (G \times G)(e)$. Wegen $(G \times G)(e) \subseteq G$ bereits nach Definition einer Bahn, bestätigen wir die Behauptung $(G \times G)(e) = G$ im Ergebnis.
(b) Wir bestimmen zunächst den Kern der Gruppenoperation. Es gilt $\ker \bullet = \{(g, h) \in G | gxh^{-1} = x \, \forall x \in G\}$. Setzen wir $x = e$, so finden wir $gh^{-1} = e$, was wegen der Eindeutigkeit der Inversen $g = h$ liefert. Also gilt $\ker \bullet \subseteq \{(g, g) \in G \times G\}$. Damit formen wir um $(g, g) \in \ker \bullet \Leftrightarrow gxg^{-1} = x \forall x \in G \Leftrightarrow g \in Z(G)$. Damit erhalten wir $\ker \bullet = \{(g, g) | g \in Z(G)\}$. Hiermit finden wir, dass $\ker \bullet = \{(e, e)\}$ genau dann wenn $Z(G) = \{e\}$. □

**Aufgabe 84 (F19T1A2)** Sei $X$ die Menge der diagonalisierbaren $2 \times 2$-Matrizen über $\mathbb{R}$ und $G = \mathrm{GL}(2, \mathbb{R})$. Wir definieren $\odot : G \times X \to X, (B, M) \mapsto BMB^{-1}$.
(a) Zu zeigen ist, dass $\odot$ eine Gruppenoperation ist. Wir zeigen zunächst, dass $\odot$ wohldefiniert ist, in dem Sinne, dass für $M \in X, B \in G$ auch $BMB^{-1} \in X$. Klarerweise gilt $M \in \mathrm{Mat}(2; \mathbb{R})$, sodass auch $BMB^{-1} =: A \in \mathrm{Mat}(2; \mathbb{R})$. Insbesondere sind $A$ und $B$ ähnliche Matrizen. Aus der linearen Algebra ist nun bekannt, dass wenn von zwei zueinander ähnlichen Matrizen eine diagonalisierbar ist, ebenfalls die andere diagonalisierbar ist. Sei nämlich $T \in G$, sodass $T^{-1}MT = D$ in Diagonalgestalt $D$ übergeführt wird. Dann gilt mit $M = B^{-1}AB$, dass $D = T^{-1}B^{-1}ABT = (TB)^{-1}A(TB)$ und, wegen $T, B \in G \Rightarrow TB \in G$ infolge Abgeschlossenheit von $G$, ist auch $A$ diagonalisierbar und hat insbesondere dieselbe Diagonalgestalt $D$ wie $M$. Mithin ist durch $\odot$ tatsächlich eine Abbildung $X \times G \to X$ wohldefiniert erklärt. Wir prüfen nun die Definition einer Gruppenoperation. Das Neutralelement von $G$ ist die $2 \times 2$-Einheitsmatrix. Es gilt für $B = E_2$, die $2 \times 2$-Einheitsmatrix $BMB^{-1} = E_2 M E_2^{-1} = E_2 M E_2 = M$, für alle $M \in X$, sodass $\odot(E_2, M) = M$. Überdies gilt für $B_1, B_2 \in G$ beliebig, dass $\odot(B_1, \odot(B_2, M)) = B_1(B_2 M B_2^{-1})B_1^{-1} = (B_1 B_2)M(B_1 B_2)^{-1} = \odot(B_1 B_2, M)$ für alle $M \in X$. Insgesamt haben wir damit nachgeprüft, dass es sich bei $\odot$ um eine Gruppenoperation handelt.
(b) Die Operation aus (a) ist nicht transitiv. Angenommen, die Operation wäre transitiv, dann gilt $G(E_2) = X$, d.h., es gibt nur eine ganz $X$ enthaltene Bahn der Operation von $G$ auf $X$. Andererseits gilt für beliebiges $B \in G$, dass $BE_2B^{-1} = E_2$, sodass $G(E_2) = \{E_2\}$. Da auch $2E_2 \in X$ diagonalisierbar ist, haben wir den gesuch-

ten Widerspruch, denn $2E_2 \notin G(E_2)$ im Widerspruch zur Annahme, die Operation wäre transitiv.
(c) Gesucht ist nun ein Repräsentantensystem der Bahnen der Operation aus (a). Wir behaupten, dass

$$R \equiv \left\{ \left( \begin{array}{cc} \lambda & 0 \\ 0 & \mu \end{array} \right) \middle| \lambda, \mu \in \mathbb{R}, \lambda \geq \mu \right\}. \tag{123}$$

Um zu zeigen, dass die Menge $R$ ein Repräsentantensystem der Bahnen von der Operation von $G$ auf $X$ ist, müssen wir zeigen, dass jede Bahn ein $A \in R$ enthält und dass jede Bahn höchstens ein $A \in R$ enthält. Sei dazu $M \in X$ vorgegeben. Da $M$ diagonalisierbar ist, gibt es $T \in G$, sodass $TGT^{-1} = D$ in Diagonalgestalt ist. Wir bezeichnen die beiden Diagonaleinträge von $D$ mit $\Lambda_1, \Lambda_2 \in \mathbb{R}$. Indem wir ggf. mit der Matrix $B := (e_{12} + e_{21})(= B^{-1})$ auf $D$ operieren, können wir annehmen, dass $\Lambda_1 \geq \Lambda_2$ ist. Damit sind $\Lambda_1, \Lambda_2 \in \mathbb{R}$ eindeutig festgelegt, und wir finden, dass jede Bahn ein $A \in R$, mit der Ersetzung $\lambda = \Lambda_1$ und $\mu = \Lambda_2$, enthält. Wir nehmen nun an, es lägen $A \neq A'$ in der Bahn zu einem fest vorgegebenem $M$. Dann gäbe es $T \in G$ mit $TAT^{-1} = A'$. Da aber $A, A'$ bereits in Diagonalgestalt sind haben wir einen Widerspruch zu den Aussage, dass zueinander ähnliche diagonalisierbare Matrizen dieselben Eigenwerte haben, $\{\Lambda_1(A), \Lambda_2(A)\} = \{\Lambda_1(A'), \Lambda_2(A')\}$. Der Fall, dass die beiden Diagonalelemente nur in ihrer Reihenfolge vertauscht sind, ist bereits durch Definition von $R$ ausgeschlossen. Mithin haben wir gezeigt, dass jede Bahn der Operation genau ein Element aus $R$ enthält, $R$ also Repräsentantensystem der Bahnen der Operation von $G$ auf $X$ ist. □

**Aufgabe 85 (F18T2A1(d))** Gegeben seine $P_1, ..., P_5 \in \mathbb{R}^2$ mit $P_j = (x_j, y_j)$ für alle $j \in \{1, 2, 3, 4, 5\}$. Zu zeigen ist die Existenz von $(a, b, c, d, e, f) \in \mathbb{R}^6$, sodass $ax_j^2 + bx_jy_j + cy_j^2 + dx_j + ey_j + f = 0$ für alle $1 \leq j \leq 5$. Zu diesem Zwecke betrachten wir das lineare Gleichungssystem $\mathsf{A}\mathbf{X} = \mathbf{0}$, wobei $\mathbf{X} = (X_1, ..., X_6)^T, \mathbf{0} = (0, 0, 0, 0, 0)^T \in \mathbb{R}^5$ und $\mathsf{A} \in \mathcal{M}(5 \times 6, \mathbb{R})$ definiert ist als

$$\mathsf{A} \equiv \left( \begin{array}{cccccc} x_1^2 & x_1y_1 & y_1^2 & x_1 & y_1 & 1 \\ x_2^2 & x_2y_2 & y_2^2 & x_2 & y_2 & 1 \\ x_3^2 & x_3y_3 & y_3^2 & x_3 & y_3 & 1 \\ x_4^2 & x_4y_4 & y_4^2 & x_4 & y_4 & 1 \\ x_5^2 & x_5y_5 & y_5^2 & x_5 & y_5 & 1 \end{array} \right). \tag{124}$$

Offenbar ist $0 \leq \text{rang}(\mathsf{A}) \leq \min\{5, 6\} = 5$. Damit hat das oben angegebenen Gleichungssystem mindestens eine nicht-triviale, d.h., $\neq \mathbf{0}_{\mathbb{R}^6}$, Lösung $\mathbf{X} \in \mathbb{R}^6$. Per Konstruktion des linearen Gleichungssystems sind dessen Lösungen gerade die für die Angabe des Kegelschnitts möglichen Koeffizienten, d.h., $(a, b, c, d, e, f) \in \{\mathbf{X} \in \mathbb{R}^6 | \mathsf{A}\mathbf{X} = \mathbf{0}_{\mathbb{R}^5}\} \supsetneq \{\mathbf{0}_{\mathbb{R}^6}\}$. Damit haben wir nachgewiesen, dass die Punkte $P_1, ..., P_5$ auf einem, möglicherweise entarteten, Kegelschnitt, wie zu Beginn der Aufgabe angegeben, liegen. □

**Aufgabe 86 (F15T1A1)** Gegeben sei der folgenden Endomorphismus von $\mathbb{F}_2$-Vektorräumen: $\Phi : \mathbb{F}_2^3 \to \mathbb{F}_2^3, (x_1, x_2, x_3) \mapsto (x_3, x_2, x_1)$.

(a) Zu bestimmen ist das charakteristische Polynom $\chi_\Phi \in \mathbb{F}_2[X]$ von $\Phi$, die Eigenwerte von $\Phi$ sowie eine $\mathbb{F}_2^3$-Basis von jedem Eigenraum von $\Phi$. Nach Definition ist $\chi_\Phi(X) \equiv \det(X\mathbb{1}_3 - \mathcal{M}_\mathcal{E}^\mathcal{E}(\Phi))$, wobei $\mathcal{M}_\mathcal{E}^\mathcal{E}(\Phi)$ die Darstellungsmatrix von $\Phi$ bezeichnet, wenn $\mathbb{F}_2^3$ auf Bild- und Urbildseite jeweils in der Standardbasis $\mathcal{E} = (\hat{e}_1 = (1,0,0)^T, \hat{e}_2 = (0,1,0)^T, \hat{e}_3 = (0,0,1)^T)$ ausgedrückt wird. Konkret ist

$$\mathcal{M}_\mathcal{E}^\mathcal{E}(\Phi) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}. \tag{125}$$

Damit ergibt sich das charakteristische Polynom durch die Rechnung in $\mathbb{F}_2$

$$\chi_\Phi(X) = \det\left(\begin{pmatrix} X & 0 & 1 \\ 0 & X+1 & 0 \\ 1 & 0 & X \end{pmatrix}\right) = X^2(X+1) + (X+1) = (X^2+1)(X+1) = (X+1)^3, \tag{126}$$

wobei "freshman's dream" im letzten Schritt verwendet wurde. Wir sehen damit, dass es nur den Eigenwert $\lambda = 1$ in $\mathbb{F}_2$ gibt und $\mu_a(\lambda, \Phi) = 3$. Wir bestimmen nun eine Basis des Eigenraums $\mathrm{Eig}(\Phi, \lambda) \subseteq \mathbb{F}_2^3$. Dazu lösen wir das homogene lineare Gleichungssystem $(\mathcal{M}_\mathcal{E}^\mathcal{E}(\Phi) - \lambda\mathbb{1}_3)\mathbf{X} = \mathbf{0}$ nach $\mathbf{X} \in \mathbb{F}_2^3$:

$$\begin{array}{ccc|c} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ \hline 1 & 0 & 1 & 0 \end{array} \tag{127}$$

Somit gilt $\mathbf{X} \in \mathrm{lin}_{\mathbb{F}_2}\{(0,1,0)^T, (1,0,1)^T\}$ ist, d.h., $\mu_g(\lambda, \Phi) = \dim_{\mathbb{F}_2} \mathrm{Eig}(\Phi, \lambda) = 2$. Die gesuchte Basis des Eigenraums ist also bspw. gegeben durch $\{(0,1,0)^T, (1,0,1)^T\}$.
(b) Aus der Vorlesung ist bekannt, dass es genau dann eine Jordan'sche Normalform für eine quadratische Matrix $A$ über einem Körper $K$ gibt, wenn das charakteristische Polynom $\chi_A$ über $K$ in Linearfaktoren zerfällt, mit anderen Worten, $K \supseteq \mathrm{Zerf}(\chi_A)$. Entsprechendes gilt für Endomorphismen $V \to V$, wobei $A$ dann die Darstellungsmatrix des Endomorphismus bzgl. geeigneter Basen des endlichdimensionalen $K$-Vektorraums $V$ auf Bild- und Urbildseite ist. Hier haben wir bereits in Teilaufgabe $A$ gesehen, dass $\chi_A$ über $K$ in Linearfaktoren zerfällt, genauer $\chi_A = (X+1)^3$, sodass $\lambda = 1$ eine dreifache Nullstelle des charakteristischen Polynoms ist. Die oben zitierte Aussage liefert nun, dass eine Basis des $\mathbb{F}_2^3$ dergestalt existiert, dass $\mathcal{M}_\mathcal{E}^\mathcal{E}(\Phi)$ in Jordan-Normalform vorliegt. Diese lässt sich durch Rückgriff auf das Ergebnis $\mu_g(\lambda, \Phi) = 2$ explizit angeben. Es gibt 2 Jordan-Kästchen zum Eigenwert 1, wobei wegen $\dim \mathbb{F}_2^3 = 3$ eines davon die Länge 2 und das andere dann die Länge $3-2 = 1$ hat. Bis auf Reihenfolge bei der Anordnung der Jordan-Kästchen ist die gesuchte Jordan-Normalform, bezeichnet mit $J(\Phi)$, also gegeben durch

$$J(\Phi) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \tag{128}$$

□

**Aufgabe 87 (F13T1A5)** Sei $M = \{A \in \mathrm{Mat}(3\times 3;\mathbb{C}) | \chi_A(z) = (z-1)^3\}$.
(a) Zu zeigen ist, dass $G \equiv \mathrm{GL}(3\times 3;\mathbb{C})$ auf $M$ vermöge $P * M = PMP^{-1}$ operiert. Wir definieren zunächst die Abbildung $\alpha : G\times M \to \mathrm{Mat}(3\times 3;\mathbb{C}), (P,A) \mapsto PAP^{-1}$. Nach Definition gilt für das charakteristische Polynom $\chi_A(z) = \det(A - zE_3)$. Wir finden mit $B \equiv PAP^{-1}$, dass $\chi_B(z) = \det(B - zE_3) = \det(PAP^{-1} - P(zE_3)P^{-1}) = \det(P(AP^{-1} - zE_3P^{-1})) = \det(P(A-zE_3)P^{-1}) = \det(P)\det(A-zE_3)\det(P^{-1}) = \det(PP^{-1})\det(A-zE_3) = \det(A-zE_3) = \chi_A(z)$, d.h., dass das charakteristische Polynom eines Elements aus $M$ unter der Konjugation mit einer Matrix aus $G$ invariant bleibt. Damit ist bereits $\alpha : G\times M \to M, (P,A) \mapsto PAP^{-1}$ wohldefiniert. Wir zeigen nun, dass $\alpha(E_3, A) = A$ für alle $A \in M$ und $\alpha(P, \alpha(Q,A)) = \alpha(PQ, A)$ für alle $P, Q \in G$ und $A \in M$. Es gilt $\alpha(E_3, A) = E_3AE_3^{-1} = E_3(AE_3) = E_3A = A$ für beliebiges $A \in M$. Für beliebige $P, Q \in G$ und $A \in M$ finden wir $\alpha(P, \alpha(Q,P)) = \alpha(P, QAQ^{-1}) = PQAQ^{-1}P^{-1} = (PQ)A(PQ)^{-1} = \alpha(PQ, A)$. Insgesamt haben wir damit gezeigt, dass $\alpha : G\times M \to M, (P,A) \mapsto PAP^{-1}$ eine Gruppenoperation ist, die wir im Folgenden wieder als $\alpha(P,A) = P * A$ für $P \in G$, $A \in M$ abkürzen.
(b) Gesucht ist die Anzahl der Bahnen der Operation. Da $\chi_A(z) = (z-1)^3$ für alle $A \in M$ gilt, wissen wir, dass eine Jordan-Basis zu jedem $A \in M$ existiert. Mit anderen Worten, wir können ein $P \in G$ finden, sodass $P * A = PAP^{-1}$ in Jordan-Normalform vorliegt. Wegen $\deg(\chi_A) = 3$ gibt es genau drei Möglichkeiten, für die Jordan-Normalform (bis auf Reihenfolge der Anordnung der Jordan-Blöcke, was aber durch Konjugation sichergestellt werden kann):

$$J_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \; J_2 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \; J_3 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}. \tag{129}$$

Da die Bahnen der Operation von $G$ auf $M$ letztere disjunkt zerlegen, wissen wir, dass es mindestens 3 Bahnen gibt. Infolge der eingangs gemachten Bemerkung, dass jedes $A \in M$ eine Jordan-Normalform besitzt, also es zu $A \in M$ ein $P = P_A \in G$ gibt, sodass $PAP^{-1} \in \{J_1, J_2, J_3\}$ gibt, finden wir, dass es genau 3 Bahnen der Operation von $G$ auf $M$ gibt. □

**Aufgabe 88 (H10T3A1)** Sei $\cdot G \times M \to M$ die Operation einer Gruppe der Ordnung 91, die auf eine Menge $M$ mit 71 Elementen operiert. Es ist $91 = 7 \cdot 17$. Sei $R$ ein Repräsentantensystem von Bahnen der Länge $> 1$ der Operation von $G$ auf $M$ und sei $F$ die, ggf. leere, Fixpunktmenge der Operation. Dann gilt nach Bahnengleichung

$$71 = |M| = |F| + \sum_{r\in R} |G|/|G_r|, \tag{130}$$

wo $G_r \leq G$ der Stabilisator zu $r \in G$ für die zu untersuchende Operation ist. Für beliebiges aber festes $r \in R$ gibt es drei Möglichkeiten: $|G|/|G_r| \in \{7, 13, 91\}$. Da $|M| = 71 < 91$ scheidet der Fall, dass es ein $r \in R$ gibt mit $|G|/|G_r| = 91$ aus. Wir können die o.g. Summe also umschreiben, indem wir $R = R_7 \uplus R_{13}$ schreiben, wobei $R_7 = \{r \in R | |G|/|G_r| = 7\}$ und $R_{13} = \{r \in R | |G|/|G_r| = 13\}$ definiert wird. Die Disjunktheit der Zerlegung ist dabei direkt klar. Infolgedessen gilt mit $m = |R_7|$

und $n = |R_{13}|$, dass

$$71 = |F| + 7m + 13n. \tag{131}$$

Wegen $F \subseteq M$ ist $0 \leq |F| \leq 71$. Da wir lediglich zeigen wollen, dass die Operation mindestens einen Fixpunkt besitzt, langt es, den Fall $F = \emptyset$, d.h., $|F| = 0$ auszuschließen. Angenommen, $F = \emptyset$. Dann geht die obige Gleichung über in

$$71 = 7m + 13n. \tag{132}$$

Reduktion modulo der teilerfremden Primzahlen 7 bzw. 13 liefert

$$1 \equiv (-1)n \bmod(7)\,,\ 6 = 7m \bmod(13). \tag{133}$$

Da $m, n \geq 0$ sehen wir, dass $n \in (-1) + 7\mathbb{N}$ und $m \in 12 + 13\mathbb{N}_0$. Insbesondere ist also $n \geq 6$, was bereits $0 \leq 7m = 71 - 13 \cdot n = -7$ zur Folge hat, einen offensichtlichen Widerspruch. Damit war die Annahme $F = \emptyset$ falsch und es gilt $\emptyset \neq F \subset M$. Nach Definition von $F$ als Fixpunktmenge der Operation von $G$ auf $M$ hat diese Operation also mindestens einen Fixpunkt. □

**Aufgabe 89 (H10T3A4)** Sei $K|\mathbb{Q}$ mit $K = \mathbb{Q}(\sqrt{2}, \sqrt{11})$ eine Körpererweiterung von $\mathbb{Q}$.
(a) Zu zeigen ist, dass es sich um eine Galois-Erweiterung handelt und die Galois-Gruppe $\mathrm{Gal}(K|\mathbb{Q})$ ist zu finden. $K|\mathbb{Q}$ ist galoissch, wenn $K|\mathbb{Q}$ separabel und normal ist. Die Separabilität ist klar, denn $K|\mathbb{Q}$ ist eine Körpererweiterung über einem Körper der Charakteristik 0. Zudem ist $K|\mathbb{Q}$ endlich, genauer von den Elementen $\{\sqrt{2}, \sqrt{11}\} \subseteq K$ erzeugt. Diese sind beide algebraisch über $\mathbb{Q}$ und haben die Minimalpolynome $\mu_{\mathbb{Q},\sqrt{2}} = x^2 - 2$, $\mu_{\mathbb{Q},\sqrt{11}} = x^2 - 11$. Deren Irreduzibilität und Minimalpolynomeigenschaft sieht man leicht mithilfe des Eisensteinkriteriums für $p = 2$ bzw. $p = 11$. Es verbleibt zu zeigen, dass $K|\mathbb{Q}$ normal ist. Definiere dazu das offenbar nicht-konstante Polynom $f = (x^2 - 2)(x^2 - 11) \in \mathbb{Q}[x]$. Es hat die Nullstellenmenge $N[f] = \{\pm\sqrt{2}, \pm\sqrt{11}\}$. Offenbar ist $N[f] \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{11})$ und $\{\sqrt{2}, \sqrt{11}\} \subsetneq N[f] \subseteq \mathbb{Q}(N[f])$ ist klar. Damit folgt bereits, dass $\mathbb{Q}(N[f]) = K$, sodass $K$ der Zerfällungskörper von $f$ ist. Laut Vorlesung ist damit $K|\mathbb{Q}$ normal. Zusammen mit der Separabilität von oben haben wir den Nachweis, dass $K|\mathbb{Q}$ galoissch ist, erbracht. Zu bestimmen ist nun die Galois-Gruppe von $K|\mathbb{Q}$. Da $11, 2$ quadratfreie und teilerfremde Primzahlen sind, ist bereits $[\mathbb{Q}(\sqrt{11}, \sqrt{2}) : \mathbb{Q}(\sqrt{2})] = [\mathbb{Q}(\sqrt{11}) : \mathbb{Q}]$ nach einem bekannten Vorlesungsresultat. Letzterer Erweiterungsgrad ist wegen $\deg \mu_{\mathbb{Q},\sqrt{11}} = 2$ gleich 2. Zusammen mit der Gradformel finden wir also

$$[\mathbb{Q}(\sqrt{2}, \sqrt{11}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{11}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4. \tag{134}$$

Da laut Vorlesung $|\mathrm{Gal}(K|\mathbb{Q})| = |[\mathbb{Q}(\sqrt{2}, \sqrt{11}) : \mathbb{Q}]| = 4$, wissen wir, dass die Ordnung der Galoisgruppe 4 ist. Da 4 ein Primzahlquadrat ist, ist $\mathrm{Gal}(K|\mathbb{Q})$ zumindest abelsch. Als endliche abelsche Gruppe ist $\mathrm{Gal}(K|\mathbb{Q})$ insbesondere endlich erzeugt, sodass der Hauptsatz über endlich erzeugte abelsche Gruppen liefert, dass

$$\mathrm{Gal}(K|\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \text{ oder } \mathrm{Gal}(K|\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}. \tag{135}$$

Aus Ordnungsgründen sind die beiden Isomorphietypen verschienden, denn im zweiten Fall gibt es ein Element der Ordnung 4, im ersteren Fall nur Elemente der Ordnung $\leq 2$. Wir schließen aus, dass $\mathrm{Gal}(K|\mathbb{Q})$ zyklisch von Ordnung 4 ist. Laut Vorlesung hat eine zyklische Gruppe endlicher Ordnung zu jedem Teiler der Gruppenordnung genau eine Untergruppe (und wegen Zyklizität auch einen Normalteiler), deren Index in der zyklischen Gruppe besagter Teiler ist. Also hat $\mathrm{Gal}(K|\mathbb{Q})$ genau einen Normalteiler der Ordnung 2. Andererseits sehen wir leicht, dass $K_1 = \mathbb{Q}(\sqrt{2})|\mathbb{Q}$ und $K_2 = \mathbb{Q}(\sqrt{11})|\mathbb{Q}$ zwei Körpererweiterungen vom Grad 2 sind, also normal, und als Zwischenkörper der Erweiterung $K|\mathbb{Q}$ auch separabel sind. Insbesondere ist $K_1 \neq K_2$, da $\sqrt{2} \notin K_2$ und $\sqrt{11} \notin K_1$. Laut Hauptsatz der Galoistheorie stehen die Normalteiler der Galoisgruppe in antitonischen Bijektion zu den normalen Zwischenkörpern der Galoiserweiterung $K|\mathbb{Q}$. Dies kann nicht erreicht werden, wenn $\mathrm{Gal}(K|\mathbb{Q})$ lediglich einen Normalteiler vom Index 2 hat, $K|\mathbb{Q}$ aber zwei Zwischenkörper vom Erweiterungsgrad 2. Also bleibt nur die Möglichkeit, dass $\mathrm{Gal}(K|\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ und wir haben die gesuchte Galoisgruppe bis auf Isomorphie spezifiziert.
(b) Gesucht sind nun alle Zwischenkörper von $K|\mathbb{Q}$. Da für einen Zwischenkörper $M$ von $K|\mathbb{Q}$ gilt $[M : \mathbb{Q}]|[K : \mathbb{Q}]$ kann nur $[M : \mathbb{Q}] \in \{1, 2, 4\}$.

- *Fall* $[M : \mathbb{Q}] = 1$. In diesem Fall gibt es nur einen einzigen, trivialen Zwischenkörper, nämlich $M = \mathbb{Q}$.

- *Fall* $[M : \mathbb{Q}] = 4$. In diesem Fall gibt es nur einen einzigen, trivialen Zwischenkörper, nämlich $M = K$.

- *Fall* $[M : \mathbb{Q}] = 2$. In diesem Fall gibt es drei Zwischenkörper, denn diese stehen laut Hauptsatz der Galoistheorie in Bijektion zu den Untergruppen von $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq \mathrm{Gal}(L|K)$. Es ist leicht zu sehen, dass $(1,0), (0,1), (1,1) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ alle von Null verschiedenen Elemente der angegebenen Gruppe sind und jeweils die Ordnung 2 haben. Da diese paarweise verschieden sind, finden wir mit $U_1 = \langle (1,0) \rangle$, $U_2 = \langle (0,1) \rangle$ und $U_3 = \langle (1,1) \rangle$ jeweils drei paarweise verschiedene Untergruppen von $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, die vermöge eines Gruppenisomorphismus zu Untergruppen von Ordnung und Index 2 in $\mathrm{Gal}(K|\mathbb{Q})$ entsprechen. Damit liefert uns der Hauptsatz der Galoistheorie, dass es genau drei Zwischenkörper von $K|\mathbb{Q}$ vom Erweiterungsgrad 2 gibt. Davon haben wir bereits gefunden: $M_1 = \mathbb{Q}(\sqrt{2})$ und $M_2 = \mathbb{Q}(\sqrt{11})$, vgl. Teilaufgabe (a). Wir stellen fest, dass $\sqrt{22} = \sqrt{2} \cdot \sqrt{11} \in K$ aber $\sqrt{22} \notin M_1 \cup M_2$. Andererseits ist $\mu_{\mathbb{Q},\sqrt{22}} = x^2 - 22 \in \mathbb{Q}[x]$ irreduzibel nach Eisenstein zu $p = 2$, normiert und erfüllt $\mu_{\mathbb{Q},\sqrt{22}}$, sodass es sich hierbei tatsächlich um das Minimalpolynom von $\sqrt{22}$ aus $\mathbb{Q}[x]$ handelt. Da dieses Grad 2 hat, folgt $[\mathbb{Q}(\sqrt{22}) : \mathbb{Q}] = 2$, weil der Erweiterungsgrad einer von einem einzelnen, algebraischen Element erzeugten Körpererweiterung laut Vorlesung dem Grad des Minimalpolynoms dieses Elements gleich ist. Damit ist mit $M_3 = \mathbb{Q}(\sqrt{22})$ ein weiterer Zwischenkörper von $K|\mathbb{Q}$ vom Erweiterungsgrad gefunden. Da $M_1, M_2, M_3$ paarweise verschieden sind, haben wir wegen der obigen Ausführungen alle Zwischenkörper von $K|\mathbb{Q}$ vom Erweiterungsgrad 2 gefunden.

Die Zwischenkörper sind also $\mathbb{Q}, \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{11}), \mathbb{Q}(\sqrt{22})$ und $\mathbb{Q}(\sqrt{2}, \sqrt{11})$.
(c) Zu bestimmen ist nun ein primitives Element der Erweiterung, d.h., ein $\alpha \in K$, sodass $K = \mathbb{Q}(\alpha)$. Wir behaupten, dass $\alpha = \sqrt{2} + \sqrt{11}$ ein primitives Element ist. Dazu beachten wir, dass mit $\sqrt{2}, \sqrt{11} \in K$ auch $\alpha \in K$. $\mathbb{Q} \subseteq K$ ist bereits definitionsgemäß klar. Damit ergibt sich $K \supseteq \mathbb{Q}(\alpha)$. Wir müssen noch zeigen, dass $\{\sqrt{2}, \sqrt{11}\} \cup \mathbb{Q} \subseteq \mathbb{Q}(\alpha)$, um $K \subseteq \mathbb{Q}(\alpha)$ zu erhalten. $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$ ist hierbei klar. Wegen $\alpha = \sqrt{2} + \sqrt{11} \in \mathbb{Q}(\alpha)$ ist infolge der Körpereigenschaft von $\mathbb{Q}(\alpha)$ auch $\alpha^{-1} \in \mathbb{Q}(\alpha)$. Es gilt

$$\frac{1}{\sqrt{2} + \sqrt{11}} = \frac{\sqrt{11} - \sqrt{2}}{9}, \tag{136}$$

sodass auch $\sqrt{11} = 0.5(\alpha + 9\alpha^{-1}) \in \mathbb{Q}(\alpha)$ und $\sqrt{2} = 0.5(\alpha - 9\alpha^{-1}) \in \mathbb{Q}(\alpha)$. Damit folgt $\{\sqrt{2}, \sqrt{11}\} \cup \mathbb{Q} \cup \mathbb{Q}(\alpha)$, also auch $K \subseteq \mathbb{Q}(\alpha)$. Insgesamt haben wir also die Gleichheit $K = \mathbb{Q}(\alpha)$ bestätigt. Damit ist der Nachweis, dass $\alpha = \sqrt{2} + \sqrt{11}$ ein primitives Element für $K|\mathbb{Q}$ ist, abgeschlossen. □

**Aufgabe 90 (H09T1A3/F02T3A2)** Gegeben sei eine endliche Gruppe $G$ und eine Untergruppe $U \leq G$, sodass $(G : U) = p$, wobei $p$ der kleinste Primteiler von $|G|$ ist. Zu zeigen ist, dass dann bereits $U \trianglelefteq G$. Hierzu verwenden wir, dass $\cdot : G \times G/U \to G/U$, $(g_1, g_2U) \mapsto (g_1g_2)U$ eine Operation der Gruppe $G$ auf die Menge der Linksnebenklassen $G/U$ darstellt. Diese ist in der Tat wohldefiniert, denn sei $R$ ein Repräsentantensystem der Menge der Linksnebenklassen, so gilt für ein beliebiges $g \in G$ und $r \in R$, $g \cdot_G r = r'u'$, wo $r' \in R$ und $u' \in U$. Diese legt $r'$ eindeutig fest, denn die Menge der Linksnebenklassen $G/U$ bildet eine disjunkte Zerlegung von $G$, wie in der Vorlesung gezeigt wurde. Wählen wir $r$ als Repräsentant einer Linksnebensklasse $hU \in G/U$ finden wir $g \cdot hU = g \cdot rU = (g \cdot_G r)U = r'u'U = r'U \in G/U$, da $u' \in U$. Wir zeigen nun, dass es sich bei der oben definierten Abbildung um eine Gruppenoperation handelt. Seien dazu $g_1, g_2, h \in G$ beliebig und ohne Einschränkung können wir $h$ als Repräsentant der Linksnebenklasse $hU$ wählen. Dann gilt $e_G \cdot hU = (e_G \cdot_G h)U = hU$ und $g_1 \cdot (g_2 \cdot hU) = g_1 \cdot (g_2 \cdot hU) = g_1 \cdot (h'U) = g_1 \cdot_G h'U = (g_1 \cdot_G (g_2 \cdot h))U = (g_1 \cdot_G g_2) \cdot_G hU$, wo $h''$ der Repräsentant der Linksnebenklasse $g_2 \cdot_G hU$ ist, d.h., es gibt eindeutiges $u' \in U$, sodass $g_2 \cdot_G h = h'u'$. Damit ist gezeigt, dass $\cdot$ wie oben definiert tatsächlich eine Gruppenoperation ist. Nun gilt laut Vorlesung, dass die Gruppenoperantion einen (wohldefinierten) Gruppenhomomorphismus $\psi : G \to \mathrm{Per}(G/U), g \mapsto (\psi_g : G/U \to G/U, (g, hU) \mapsto (gh)U)$ definiert, wobei $\mathrm{Per}(G/U)$ die Permutationsgruppe zur Menge $G/U$ ist. Da $|G/U| = p$ wegen $(G : U) = p$, ist $\mathrm{Per}(G/U) \simeq S_p$, wobei $S_p$ die symmetrische Gruppe auf der Menge $\{1, ..., p\}$ bezeichnet. Unter Verwendung dieser Isomorphie erhalten wir aus $\psi$ einen Gruppenhomomorphismus $\Psi : G \to S_p$. Wir zeigen zuerst, dass $\ker \psi \subseteq U$. Sei dazu $g \in \ker \psi$. Dann gilt $\psi(g) = \mathrm{id}_{G/U}$. Sei also $hU$ eine beliebige Linsknebenklasse und $h$ ohne Einschränkung als Repräsentant gewählt. Dann gilt $gh = hu$ mit einem $u \in U$. Dann gilt $h^{-1}gh = u$. Insgesamt schließen wir also $h^{-1} \ker \psi h \subseteq U$. Andererseits wissen wir aus der Vorlesung, dass $\ker \psi \trianglelefteq G$, d.h., insbesondere $h^{-1} \ker \psi h = \ker \psi$. Somit finden wir $\ker \psi \subseteq U$, wie behauptet. Wir wissen nun, dass $\ker \psi \subseteq U$ und $\ker \psi$ eine Gruppe ist. Wir folgern also, dass $\ker \psi \leq U$. Nun ist, da $G$ endlich ist,

nach dem Homomorphiesatz und dem Satz von Lagrange $|G||\ker\psi| = |\mathrm{im}\psi|$. Insbesondere ist $\mathrm{im}\psi \leq S_p$, d.h., $|\mathrm{im}\psi||p! = |S_p|$. Wegen $\ker\psi \leq U \neq G$, ist der Fall, dass $\mathrm{im}\psi = \{e_G\}$ aus Ordnungsgründen ausgeschlossen. Wir können nun verwenden, dass $p$ der kleinste Primteiler von $|G|$ ist. Dann ist nämlich $|\mathrm{im}\psi| = p$. Andernfalls gäbe es, da $p$ der größte und auch ein einfacher Primteiler von $p!$ ist, eine kleiner Primzahl $p'$, sodass $p'||\mathrm{im}\psi|$ und damit dann auch wegen $|\mathrm{im}\psi|||G|$ auch $p'||G|$. Das ist ein Widerspruch zur Minimalitätseigenschaft von $p$. Also gibt es abgesehen von $p$ keinen Primteiler von $|\mathrm{im}\psi|$, und mit dem Fundamentalsatz der Arithmetik folgern wir $|\mathrm{im}\psi| = p$. Damit finden wir aber, dass $|\ker\psi| = n/p$, was nach dem Satz von Lagrange gerade $|U|$ ist. Zusammen mit $G/U \geq \ker\psi$ folgt daraus $\ker\psi = U$. Nach der Normalteilereigenschaft des Kerns eines Gruppenhomomorphismus, hier also $\ker\psi \trianglelefteq G$, haben wir die Normalteilereigenschaft $U \trianglelefteq G$ etabliert. □

**Aufgabe 91 (F98 – G4.24)** Sei $G$ eine Gruppe der Ordnung 750. Zu zeigen ist, dass $G$ einen echten Normalteiler besitzt. Es ist $750 = 5 \cdot 150 = 5^3 \cdot 3 \cdot 2$. Wir bezeichnen für eine Primzahl $p$ die Anzahl der $p$-Sylowgruppen von $G$ mit $\nu_p$. Aus der Primfaktorzerlegung von soeben finden wir, dass es nur 3-, 2- und 5-Sylowgruppen von $G$ gibt. Nach dem dritten Sylow'schen Satz gilt für die Anzahl $\nu_5$ der 5-Sylowgruppen von $G$, $\nu_5 \in \{1, 2, 3, 6\}$, denn $\nu_5|750/125 = 6$. Zudem gilt ebenfalls nach dem dritten Sylow'schen Satz $\nu_5 \equiv 1 \bmod(5)$, was nur für die Möglichkeiten $\nu_5 = 1$ oder $\nu_5 = 6$ erfüllt ist. Falls $\nu_5 = 1$, ist nach einer Ergänzung zum zweiten Sylow'schen Satz die einzige 5-Sylowgruppe ein Normalteiler von $G$. Da diese einzige 5-Sylowgruppe die Ordnung $125 = 5^3$ hat und $1 < 125 < 750$, haben wir in diesem Fall einen nichttrivialen Normalteiler gefunden. Wir zeigen nun, dass der Fall $\nu_5 = 6$ nicht auftreten kann. Dazu beachten wir, dass $G$ auf die Menge $\mathrm{Syl}_5$ der 5-Sylowgruppen durch Konjugation operiert. Aus der Vorlesung ist ferner bekannt, dass dies als Gruppenoperation einen Homomorphismus von Gruppen, $\psi : G \to \mathrm{Per}(\mathrm{Syl}_5)$ definiert. Da $|\mathrm{Syl}_5| = 6$, ist $\mathrm{Per}(\mathrm{Syl}_5) \simeq S_6$, wobei $S_6$ die symmetrische Gruppe für die Menge $\{1, 2, 3, 4, 5, 6\}$ bezeichnet. Sie hat $|S_5| = 6! = 720$ Elemente. Nach dem Homomorphiesatz für Gruppen wissen wir, dass $\psi$ einen Isomorphismus $G/\ker\psi \to \mathrm{im}\psi$ induziert, wobei $\mathrm{im}\psi \leq S_6$ und somit $|\mathrm{im}\psi| \leq 720$ ist. Damit finden wir die Abschätzung $|\ker\psi| \geq 750/720 > 1$, sodass $|\ker\psi| > 1$ und damit $\{e_G\} \subsetneq \ker\psi$. Da $\ker\psi \trianglelefteq G$ als Kern eines Gruppenhomomorphismus können wir bereits ausschließen, dass $\ker\psi$ der triviale Normalteiler $\{e_G\}$ ist. Wir schließen nun noch den Fall aus, dass $\ker\psi = G$. Dann wäre $\psi(g) = \mathrm{id}_{\mathrm{Syl}_5}$ für alle $g \in G$. Mit anderen Worten, es gilt für jede 5-Sylowgruppe $P \in \mathrm{Syl}_5$ $\psi(g)(P) = gPg^{-1} = \mathrm{id}_{\mathrm{Syl}_5}(P) = P$, also $gPg^{-1} = P$ für alle $g \in G$ und alle $P \in \mathrm{Syl}_5$. Das ist aber gleichbedeutend damit, dass jeder der $\nu_5 = 6$ 5-Sylowgruppen ein Normalteiler von $G$ ist. Letzteres ist nach der oben zitierten Ergänzung zum zweiten Sylow'schen Satz nicht möglich, denn dann wäre $\nu_5 = 1$. Also kann der Fall $\ker\psi = G$ nicht auftreten. Da nun $\{e_G\} \subsetneq \ker\psi \trianglelefteq G$ und Kerne von Gruppenhomomorphismen stets Normalteiler sind, haben wir mit $\ker\psi$ einen nichttrivialen, d.h., echten, Normalteiler von $G$ gefunden. □

**Aufgabe 92 (F19T1A1(d))** Zu zeigen ist, dass jede Gruppe der Ordnung 95 zyklisch ist. Sei dazu $G$ eine Gruppe der Ordnung 95. Es gilt nach dem Hauptsatz der Arithmetik, $95 = 5 \cdot 19$. Sowohl 5 als auch 19 sind Primzahlen. Bezeichne für

eine Primzahl $p$ die Anzahl der $p$-Sylowgruppen von $G$ mit $\nu_p$. Nach dem dritten Satz von Sylow gilt dann $\nu_5|19$ und $\nu_p \equiv 1 \bmod(5)$ sowie $\nu_{19}|5$ und $\nu_{19} \equiv 1 \bmod(19)$. Aus der jeweils ersten Bedingung finden wir $\nu_5 \in \{1, 19\}$ und $\nu_{19} \in \{1, 5\}$. Wegen $19 \equiv 4 \bmod(5) \neq 1 \bmod(5)$ bleibt nur $\nu_5 = 1$ übrig. Analog bleibt wegen $5 \equiv 5 \bmod(19) \neq 1 \bmod(19)$ nur $\nu_{19} = 1$ übrig. Somit gibt es also jeweils genau eine 5-Sylowgruppe von $G$ und genau eine 19-Sylowgruppe von $G$. Nach einem Zusatz zum zweiten Satz von Sylow, ist für eine Primzahl $p$ die einzige $p$-Sylowgruppe von $G$ ein Normalteiler von $G$. Bezeichnen wir die gefundenen Sylowgruppen mit $P_5$ und $P_{19}$, sodass $|P_5| = 5$ und $|P_{19}| = 19$, so gilt $P_5 \trianglelefteq G$ und $P_{19} \trianglelefteq G$. Da $P_5$ und $P_{19}$ jeweils von Primzahlordnung sind, sind die isomorph zu zyklischen Gruppen der jeweils selben Ordnung, d.h., $P_5 \simeq \mathbb{Z}/5\mathbb{Z}$ und $\mathbb{Z}/19\mathbb{Z}$. Wir behaupten nun, dass $G$ isomorph zu $P_5 \cdot P_{19}$ ist. Offensichtlich gilt für das Komplexprodukt $P_5 \cdot P_{19} \trianglelefteq G$. Ferner stellen wir fest, dass $P_5 \cap P_{19} = \{e_G\}$, denn es gibt jeweils kein Element der Ordnung 19 in $P_5$ und kein Element der Ordnung 5 in $P_{19}$: In $P_{19}$ gibt es $\Phi(19) = 18$ Elemente der Ordnung 19, wo $\Phi$ die Euler'sche $\Phi$-Funktion ist. Zusätzlich gibt es 1 Element der Ordnung 1, was wegen $P_{19} \leq G$ das Neutralelement $e_G$ ist. Analog schließt man, dass es 4 Elemente der Ordnung 5 in $P_5$ gibt, das verbleibende Element das Neutralelement $e_G$ ist. Dann gilt $|P_5 \cdot P_{19}| = |P_5| \cdot |P_{19}| = 5 \cdot 19 = 95 = |G|$. Wegen $P_5 \cdot P_{19} \leq G$ ist dann bereits $P_5 \cdot P_{19} = G$, d.h., $G$ ist inneres semidirektes Produkt der Sylowgruppen $P_5$, $P_{19}$. Da zusätzlich $P_5, P_{19} \trianglelefteq G$, ist $G$ sogar inneres direktes Produkt von $P_5$ und $P_{19}$. Bekannt ist, dass das innere direkte Produkte zweier Gruppen isomorph zu den äußeren direkten Produkt der beiden Gruppen ist. Wir finden also die Isomorphie $G \simeq P_5 \times P_{19}$. Infolge der oben etablierten Isomorphie zu den zyklischen Gruppen $\mathbb{Z}/5\mathbb{Z}$ und $\mathbb{Z}/19\mathbb{Z}$ gilt sogar $G \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/19\mathbb{Z}$. Wegen $\mathrm{ggT}(5, 19) = 1$ liefert der Chinesische Restsatz in $\mathbb{Z}$ die Isomorphie $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/19\mathbb{Z} \simeq \mathbb{Z}/95\mathbb{Z}$. Damit finden wir $G \simeq \mathbb{Z}/95\mathbb{Z}$. $G$ ist also isomorph zu einer zyklischen Gruppe der Ordnung 95 und damit selbst zyklisch. □

**Aufgabe 93 (H16T2A2)** Seien $A, B$ abelsche Gruppen. Wir definieren das äußere semidirekte Produkt durch $A \rtimes_\phi B := \{(a, b) | a \in A, b \in B\}$ und $(a_1, b_1) \cdot (a_2, b_2) = (a_1\phi(b_1)(a_2), b_1b_2)$, wobei $\phi : B \to \mathrm{Aut}(A)$ ein Gruppenhomomorphismus ist. Als bekannt vorausgesetzt werden darf laut Aufgabenstellung, dass auf diese Weise eine Gruppe definiert wird.

(a) Wir zeigen, dass $A \rtimes_\phi B$ genau dann abelsch ist, wenn $\phi(b) = \mathrm{id}_A$ für alle $b \in B$ ist.
"⇒". Sei $A \rtimes_\phi B$ als abelsch vorausgesetzt. Dann gilt $(a_1, b_1) \cdot (a_2, b_2) = (a_2, b_2) \cdot (a_1, b_1)$ für alle $(a_1, b_1), (a_2, b_2) \in A \rtimes_\phi B$. Ausgeschrieben haben wir $(a_1\phi(b_1)(a_2), b_1b_2) = (a_2\phi(b_2)(a_1), b_2b_1)$. Da $A$ und $B$ jeweils abelsch sind, finden wir für die beiden Komponenten $b_1b_2 = b_2b_1$, was bereits bekannt ist, und $a_1\phi(b_1)(a_2) = a_2\phi(b_2)(a_1)$. Wir setzen nun $b_1 = e_B$. Da $\phi$ nach Voraussetzung Gruppenhomomorphismus ist, gilt $a_1a_2 = a_2\phi(b_2)(a_1)$. Nun setzen wir noch $a_2 = e_A$ und finden $a_1 = \phi(b_2)(a_1)$. Da $a_1 \in A, b_2 \in B$ beliebig sind, finden wir also $\phi(b_2) = \mathrm{id}_A$ für alle $b_2 \in B$.
"⇐". Sei umgekehrt vorausgesetzt, dass $\phi(b) = \mathrm{id}_A$ für alle $b \in B$. Dann gilt für beliebige $(a_1, b_1), (a_2, b_2) \in A \rtimes_\phi B$, dass $(a_1, b_1) \cdot (a_2, b_2) = (a_1\phi(b_1)(a_2), b_1b_2) = (a_1\mathrm{id}_A(a_2), b_1b_2) = (a_1a_2, b_1b_2) = (a_2a_1, b_2b_1) = (a_2\mathrm{id}_A(a_1), b_2b_1) = (a_2\phi(b_2)(a_1), b_2b_1) = (a_2, b_2) \cdot (a_1, b_1)$. Damit ist $A \rtimes_\phi B$ im Falle, dass $\phi$ trivial ist, abelsch.

(b) Wir sollen eine nicht-abelsche Gruppe der Ordnung 2015 konstruieren. Wir stel-

len fest, dass $2015 = 403 \cdot 5 = 13 \cdot 31 \cdot 5$. Das Ergebnis von Teil (a) ist äquivalent dazu, dass das äußere semidirekte Produkt zweier abelscher Gruppen genau dann nicht-abelsch ist, wenn das dazugehörige $\phi : B \to \mathrm{Aut}(A)$ nicht-trivial ist. Da $5, 13, 31$ jeweils Primzahlen sind, konstruieren wir aus den abelschen, sogar zyklischen, Gruppen $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/13\mathbb{Z}$ und $\mathbb{Z}/31\mathbb{Z}$ eine nicht-abelsche Gruppe. Da $|\mathrm{Aut}(\mathbb{Z}/31\mathbb{Z})| = \Phi(31) = 31 - 1 = 30$, wegen $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}) \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ laut Vorlesung für die Automorphismengruppen zyklischer Gruppen von Primzahlordnung, versuchen wir einen nicht-trivialen Homomorphismus $\psi : \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/30\mathbb{Z}$ anzugeben. Dieser lässt sich dann vermöge der vorher etablierten Isomorphie als nicht-trivialer Gruppenhomomorphismus $\phi : \mathbb{Z}/5\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/31\mathbb{Z})$ verstehen. Wir erhalten einen Gruppenhomomorphismus $\psi$ wie beschrieben durch die Wahl $\psi(1) = 6$, denn 6 ist ein Element der Ordnung 5 in $\mathbb{Z}/30\mathbb{Z}$. Mit dem sich daraus ergebenden, nicht-trivialen Gruppenhomomorphismus $\phi$ ist also $\mathbb{Z}/31\mathbb{Z} \rtimes_\phi \mathbb{Z}/5\mathbb{Z}$ nicht-abelsch. Da nun einer der Faktoren im äußeren direkten Produkt $G := \mathbb{Z}/13\mathbb{Z} \times (\mathbb{Z}/31\mathbb{Z} \rtimes_\phi \mathbb{Z}/5\mathbb{Z})$ nicht-abelsch ist, trifft dies auch auf $G$ zu. Per Konstruktion hat $G$ die geforderten 2015 Elemente und ist nicht-abelsch. □

**Aufgabe 94 (F15T1A3)** Sei $G$ eine Gruppe der Ordnung 105. Wir zeigen, dass $G$ einen Normalteiler der Ordnung 5 oder 7 hat. Wegen $105 = 3 \cdot 5 \cdot 7$ ist eine Untergruppe der Ordnung 5 bzw. 7 von $G$ eine 5- bzw. 7-Sylowgruppe von $G$. Sei $\nu_p$ für eine Primzahl $p$ die Anzahl der $p$-Sylowgruppen von $G$. Nach dem dritten Satz von Sylow gilt $\nu_5 | 3 \cdot 7$ und $\nu_5 \equiv 1 \bmod(5)$ sowie $\nu_7 | 3 \cdot 5$ und $\nu_7 \equiv 1 \bmod(7)$. Das liefert $\nu_5 \in \{1, 21\}$ und $\nu_7 \in \{1, 15\}$. Wir nehmen an, dass $G$ keinen Normalteiler der Ordnung 5 oder 7 hat. Nach einer Folgerung zum zweiten Satz von Sylow gilt dann $\nu_5 \neq 1$ und $\nu_7 \neq 1$. Damit finden wir $\nu_5 = 21$ und $\nu_7 = 15$. Da je zwei $p$-Sylowgruppen konjugiert zueinander sind, finden wir, dass $G$ $\Phi(5) \cdot \nu_5 = 84$ Elemente der Ordnung 5 enthält. Da zwei Sylowgruppen zu unterschiedlichen Primzahlen $p, p'$ nur das Neutralement von $G$ gemein haben, enthält $G$ für $\nu_7$ ferner $\Phi(7)\nu_7 = 90$ Elemente der Ordnung 7. Hierbei haben wir wiederum verwendet, dass laut dem zweiten Sylow'schen Satz, je zwei verschiedene (hier: $p = 7$-)Sylowgruppen konugiert zueinander sind, also lediglich das Neutralement von $G$ gemein haben. Die Anzahl der Elemente der Ordnungen 5 bzw. 7 konnten wir, da die relevanten Sylow-Gruppen jeweils von Primzahlordnung, also zyklisch, sind, mit der Euler'schen $\Phi$-Funktion bestimmen. Zusammen stellen wir aufgrund der Eindeutigkeit der Elementordnung von Gruppenelementen fest, dass $G$ mindestens $90 + 84 = 174$ Elemente enthalten muss. Das ist wegen der Voraussetzung $|G| = 105 < 174$ nicht möglich. Damit war die Annahme, $G$ hätte keinen Normalteiler der Ordnung 5 oder 7 falsch, und $G$ hat damit einen Normalteiler der Ordnung 5 oder 7. Wir zeigen nun, dass $G$ auflösbar ist. Wir rekapitulieren die beiden Vorlesungsresultate, dass abelsche Gruppen stets auflösbar sind, und dass $G$ genau dann auflösbar ist, wenn für einen Normalteiler $N$ von $G$ die Faktorgruppe $G/N$ und der Normalteiler $N$ auflösbar sind. Laut dem Vorangegangenen, hat $G$ einen Normalteiler der Ordnung 5 oder der Ordnung 7. Wir bezeichnen den Normalteiler mit $N$ und führen eine Fallunterscheidung nach der Ordnung des Normalteilers durch.

- *Fall 1:* $|N| = 5$. $N$ ist in diesem Fall von Primzahlordnung, damit zyklisch, insbesondere also abelsch und somit auflösbar. Die Faktorgruppe $G/N$ hat

Ordnung 21. Bezeichnen wir die Anzahl der $p$-Sylowgruppen von $G/N$ mit $\mu_p$ für eine Primzahl $p$, so finden wir $\mu_7|3$ und $\mu_7 \equiv 1 \bmod(7)$ infolge des dritten Satzes von Sylow. Damit haben wir $\mu_7 = 1$. Es gibt also genau eine 7-Sylowgruppe von $G/N$. Diese ist nach einer Folgerung zum zweiten Satz von Sylow ein Normalteiler, den wir mit $M_7$ bezeichnen. Da $M_7$ Ordnung 7, insbesondere also Primzahlordnung, hat, ist $M_7$ zyklisch, damit abelsch und somit auflösbar. Die Faktorgruppe $(G/N)/M_7$ hat nach dem Satz von Lagrange also die Ordnung 3, also Primzahlordnung. Analog zu oben ist $(G/N)/M_7$ also zyklisch und somit auflösbar. Mit dem eingangs zitierten Vorlesungsresultat folgt die Auflösbarkeit von $G/N$. Da $G/N$ und $N$ auflösbar sind, liefert dasselbe Resultat also die Auflösbarkeit von $G$.

- *Fall 2:* $|N| = 7$. Auch hier ist $N$ von Primzahlordnung und damit auflösbar. Die Faktorgruppe $G/N$ hat nun die Ordnung 15. Wir bezeichnen die Anzahl der $p$-Sylowgruppen von $G/N$ in diesem Fall für jede Primzahl $p$ mit $\kappa_p$. Wegen des dritten Satzes von Sylow gilt $\kappa_5 \equiv 1 \bmod(5)$ und $\kappa_5|3$. Beide Bedingungen können nur für $\kappa_5 = 1$ erfüllt werden. Damit liefert, wie oben, eine Folgerung aus dem zweiten Satz von Sylow, dass die einzige 5-Sylowgruppe von $G/N$, bezeichnet mit $M_5$, ein Normalteiler von $G/N$ ist. Wir stellen fest, das $(G/N)/M_5$ und $M_5$ jeweils von Primzahlordnung sind, also zyklisch, also abelsch und somit auflösbar. Wie im ersten Fall folgt nun die Aufösbarkeit von $G/N$. Zusammen mit der Auflösbarkeit von $N$, die oben festgestellt wurde, erhalten wir also auch im Fall $|N| = 7$ die Auflösbarkeit von $G$.

In jedem Fall ist $G$ auflösbar. □

**Aufgabe 95 (F14T1A1)** Sei $G$ eine Gruppe der Ordnung 168, die genau 5 Untergruppen der Ordnung 42 hat. Wir sollen zeigen, dass $G$ nicht-einfach ist. Dazu nehmen wir an, dass $G$ einfach ist. Dann hat $G$ außer $\{e_G\}, G \trianglelefteq G$ keine weiteren Normalteiler. Wir bezeichnen die Menge der Untergruppen der Ordnung 42 von $G$ mit $\mathcal{U}$. Laut Vorlesung definiert die Konjugation einer Operation von $G$ auf $\mathcal{U}$, genauer $\cdot : G \times \mathcal{U} \to \mathcal{U}, (g, U) \mapsto gUg^{-1}$. Aus der Vorlesung ist ebenfalls (und allgemeiner) bekannt, dass sich aus der Gruppenoperation ein Gruppenhomormorphismus $\phi : G \to \mathrm{Per}(\mathcal{U}), g \mapsto (U \mapsto gUg^{-1})$ ergibt. Da $|\mathcal{U}| = 5$, ist $\mathrm{Per}(\mathcal{U}) \simeq S_5$ und $|S_5| = 120$. Bekannt ist schließlich, dass Kerne von Gruppenhomomorphismen Normalteiler sind, d.h., $\ker\phi \trianglelefteq G$. Wenn wir also ausschließe können, dass $\ker\phi = \{e_G\}, G$, haben wir einen nicht-trivialen Normalteiler gefunden, somit einen Widerspruch dazu, dass $G$ als einfach angenommen war. Angenommen, $\ker\phi = \{e_G\}$. Dann ist $\phi$ injektiv und es gilt $|G| = |\phi(G)| = 168 \leq |\mathrm{Per}(\mathcal{U})| = 120$. Das geht offenbar nicht, sodass der Fall $\ker\phi = \{e_G\}$ ausscheidet. Falls $\ker\phi = G$, dann gilt für ein beliebiges $U \in \mathcal{U}$ und für alle $g \in G$, dass $gUg^{-1} = U$. Also ist $U$ bereits Normalteiler von $G$. Da $U$ Ordnung 42 hat, ist $\{e_G\} \subsetneq U \subsetneq G$. Somit ist $U$ sogar nicht-trivialer Normalteiler von $G$, im Widerspruch dazu, dass $G$ als einfach angenommen wurde. Mithin war die Annahme, dass $G$ einfach ist, falsch. Damit ist $G$ nicht-einfach. □

**Aufgabe 96 (H14T1A1)** Sei $L|K$ eine endliche Galois-Erweiterung und $p$ eine Primzahl mit der Eigenschaft, dass $p|[L:K]$.
(a) Zu zeigen ist, dass es einen Zwischenkörper $Z$ von $L|K$ gibt, sodass $[L:Z]=p^m$ für ein $m\in\mathbb{N}$, aber $p\not|[Z:K]$. Da $[L:K]<\infty$ nach Voraussetzung, ist die zur Galois-Erweiterung $L|K$ gehörige Galois-Gruppe $G\equiv\mathrm{Gal}(L|K)$ ebenfalls endlich und es gilt $[L:K]=|\mathrm{Gal}(L|K)|$. Laut dem Hauptsatz der Galois-Theorie korrespondieren die Zwischenkörper $Z$ von $L|K$ bijektiv und antitonisch mit den Untergruppen von $\mathrm{Gal}(L|K)$. Insbesondere ist für jede Untergruppe $U\leq G$ der Fixkörper von $L$ unter $U$, $L^U$, der zu $U$ korrespondierende Zwischenkörper der Galois-Erweiterung $L|K$. Zudem gilt $[L^U:K]=(G:U)$ und $[L:L^U]=|U|$. Sei nun $m$ maximal mit der Eigenschaft, dass $p^m|[L:K]=|\mathrm{Gal}(L|K)|$, aber $p^{m+1}\not|[L:K]$. Dann hat $\mathrm{Gal}(L|K)$ mindestens eine $p$-Sylowgruppe, $U$. Setze $Z=L^U$, wobei $L^U$ nach dem Hauptsatz der Galois-Theorie existiert und eindeutig durch das präzise $U$ festgelegt ist. Da $U$ von maximaler $p$-Potenzordnung ist, gilt $p^m||U|=[L:Z]$ und $p\not|(G:U)=[Z:K]$, letzteres da sonst ein Widerspruch zur Maximalität von $m$ resultierte.
(b) Sei nun $K=\mathbb{Q}$ und $L=\mathbb{Q}(\zeta_7)$, wobei $\zeta_7$ eine primitive 7-te Einheitswurzel ist. Wir sollen für die Primzahl $p=3$ einen Zwischenkörper $Z$ mit den in (a) spezifizierten Eigenschaften unter Angabe eines primitiven Elements finden. Laut Vorlesung ist $L|K$ mit $L$ als $P$-ter Kreisteilungskörper zur Primzahl $P=7$ eine Galois-Erweiterung. Die zugehörige Galois-Gruppe $G=\mathrm{Gal}(L|K)$ ist erstens zyklisch und zweitens von der Ordnung $\Phi(P=7)=6$. Da $[L:K]=|\mathrm{Gal}(L|K)|=6=2\cdot 3$, und $G$ zyklisch ist, hat $G$ eine Untergruppe der Ordnung 3. Bezeichnen wir den Erzeuger von $G$ mit $\sigma$, so ist $U=\langle\sigma^2\rangle$. Um den Fixkörper $L^U$ explizit anzugeben, versuchen wir zunächst, ein Element $\alpha\in L^U$ zu finden, d.h., ein $\alpha\in L$ mit $\sigma^2(\alpha)=\alpha$. Wegen $|G|=6$ und Zyklizität ist bspw. durch $\zeta_7\mapsto\zeta_7^a$ mit einer Primitivwurzel modulo 7 $a$. $a=3$ erfüllt wegen $3^2\not\equiv 1\,\mathrm{mod}(7)$ und $3^3\not\equiv 1\,\mathrm{mod}(7)$ diese Eigenschaft. Es ist dann mit der Festlegung des $\sigma\in U$ durch $\sigma(\zeta_7)=\zeta_7^3$, $\sigma^2(\zeta_7)=\zeta_7^{3\cdot 3}=\zeta_7^2$. Damit finden wir, dass $\alpha=\zeta_7+\zeta_7^2+\zeta_7^4$ von $\sigma$ fixiert wird, denn $\sigma(\alpha)=\zeta_7^2+\zeta_7^4+\zeta_7^1=\alpha$. Also ist $\alpha\in L^U$ enthalten. Es gilt $\Phi_7(\zeta_7)=1+\zeta_7+\zeta_7^2+\zeta_7^3+\zeta_7^4+\zeta_7^5+\zeta_7^6=0$. Man sieht, dass $\alpha^2=\zeta_7^2+\zeta_7^4+\zeta_7^8+2\zeta_7^3+2\zeta_7^5+2\zeta_7^6=\zeta_7+\zeta_7^2+2\zeta_7^3+\zeta_7^4+2\zeta_7^5+2\zeta_7^6-2\Phi_7(\zeta_7)=-(\zeta_7+\zeta_7^2+\zeta_7^4)-2=-\alpha-2$. Damit ist $\alpha$ eine Lösung von $\alpha^2+\alpha+2$. Das Polynom $q(x)=x^2+x+2\in\mathbb{Q}[x]$ hat die beiden komplexen Nullstellen $\alpha_\pm=-1/2\pm\sqrt{-7}/2$. Es ist leicht einzusehen, dass $K(\alpha)=K(\sqrt{-7})$. Da $\sqrt{-7}$ Nullstelle des über $\mathbb{Q}$ irreduziblen Polynoms $Q=x^2+7$ ist, finden wir $[K(\sqrt{-7}):K]=2=[L^U:K]$, woraus bereits wegen $L^U\supseteq K(\sqrt{-7})$ Gleichheit folgt. □

**Aufgabe 97 (F11T2A3)** Sei $G\equiv\{v\mapsto Av+b|A\in\mathrm{GL}_2(\mathbb{F}_2),b\in V\}$ für $V=\mathbb{F}_2^2$. Wir beachten zunächst, dass die Menge aller invertierbaren $2\times 2$-Matrizen mit Einträgen aus $\mathbb{F}_2$ als Paar von zwei linear unabhängigen Vektoren aus $\mathbb{F}_2^2\setminus\{0_{\mathbb{F}_2^2}\}$ aufgefasst werden kann. Hierfür haben wir $(2^2-1)\cdot(2^2-2^1)=6$ Möglichkeiten. Also ist $|\mathrm{GL}_2(\mathbb{F}_2)|=6$. Indem wir verwenden, dass $\det(A)=1$ für $A\in\mathrm{GL}_2(\mathbb{F}_2)$, finden wir explizit

$$\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}0&1\\1&0\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix},\begin{pmatrix}1&0\\1&1\end{pmatrix},\begin{pmatrix}1&1\\1&0\end{pmatrix},\begin{pmatrix}0&1\\1&1\end{pmatrix}\right\}=\mathrm{GL}_2(\mathbb{F}_2). \tag{137}$$

Wir zeigen nun, dass $G \simeq S_4$. Wir stellen fest, dass $G \subseteq \mathrm{Per}(\mathbb{F}_2^2)$ gerade nur bijektive Abbildungen von $\mathbb{F}_2^2$ in sich selbst enthält. Denn für beliebiges $v \in \mathbb{F}_2^2$ finden wir mit $A \in \mathrm{GL}_2(\mathbb{F}_2)$, dass $\mathbb{F}_2^2 \ni w = Av+b \Leftrightarrow v = A^{-1}w - A^{-1}b$, sodass zu $g \equiv (v \mapsto Av+b)$ die Umkehrabbildung durch $g^{-1} \equiv (v \mapsto A^{-1}v - A^{-1}b)$ gegeben ist. Wir definieren nun die Abbildung

$$\phi : G \times \mathbb{F}_2^2 \to \mathbb{F}_2^2, (g, v) \mapsto g(v), \tag{138}$$

wobei $g(v) = Av+b$ für $g \in G$ wie oben angegeben. Es ist leicht zu sehen, dass es sich hierbei um eine Gruppenoperation handelt, denn $\phi(e_g, v) = e_g(v) = E_2 v = v$ für alle $v \in \mathbb{F}_2^2$ und $\phi(g \cdot h, v) = (g \cdot h)(v) = (AB)v + Ac + b = A(Bv + c) + b = \phi(g, \phi(h, v))$ für $g = (v \mapsto Av+b), h = (v \mapsto Bv+c) \in G$ und $v \in \mathbb{F}_2^2$. Laut Vorlesung definiert die Gruppenoperation $\phi$ in eindeutigerweise einen Gruppenhomomorphismus $\Phi : G \to \mathrm{Per}(\mathbb{F}_2^2) \simeq S_4$, da $|\mathbb{F}_2^2| = 4$. Zu zeigen ist, dass es sich hierbei um einen Isomorphismus handelt. Indem wir bemerken, dass ein Element $\sigma$ aus $\mathrm{Per}(\mathbb{F}_2^2)$ wegen Bijektivität bereits eindeutig festgelegt ist, wenn wir für $(0,0), (1,0), (0,1) \in \mathbb{F}_2^2$ angeben, auf welche drei verschiedenen Vektoren diese Elemente in $\mathbb{F}_2^2$ abgebildet werden. Wir bezeichnen die Bilder von $(0,0), (1,0), (0,1) \in \mathbb{F}_2^2$ als $v_0, v_1, v_2$ in der angegebenen Reihenfolge. Indem wir $g(v) = Av + v_0$ und $A = (v_1 - v_0, v_2 - v_0)$ setzen, stellen wir fest, dass $\det A \neq 0$, wegen $v_0 \neq v_1 \neq v_2$ jeweils paarweise in $\mathbb{F}_2^2$. Also haben wir mit $g = (v \mapsto (v_2 - v_0, v_1 - v_0)v + v_0)$ ein Element in $G$ gefunden, sodass $\Phi(g) = \chi$. Damit ist $\Phi$ surjektiv. Dieses Element $g$ ist auch eindeutig, $\Phi$ also injektiv: Seien $g_1, g_2$ mit $\Phi(g_1) = \chi = \Phi(g_2)$ $\Phi(g_1 g_2^2) = \mathrm{id}_{\mathbb{F}_2^2}$. Damit ist $(g_1 g_2^{-1})(0,0) = (0,0)$ und $(g_1 g_2^{-1})(1,0) = (1,0)$ sowie $(g_1 g_2^{-1})(0,1) = (0,1)$ und $(g_1 g_2^{-1})(1,1) = (1,1)$ nach Definition von $\Phi$. Das bedeutet aber, dass $g_1 g_2^{-1} = (v \mapsto v)$, also $g_1 = (g_2^{-1})^{-1} = g_2$. Damit ist $\Phi$ ein Isomorphismus, also $G \simeq S_4$. Wir zeigen nun, dass $\mathrm{GL}_2(\mathbb{F}_2) \simeq S_3$. Dazu stellen wir fest, dass die Abbildung $\psi_A : \mathbb{F}_2^2 \to \mathbb{F}_2^2, v \mapsto Av$ linear ist für alle $A \in \mathbb{F}_2^2$, also $0 \mapsto 0$. Wir definieren eine Operation von $\mathrm{GL}_2(\mathbb{F}_2)$ auf $\mathbb{F}_2^2 \setminus \{(0,0)\}$ durch

$$\psi : \mathrm{GL}_2(\mathbb{F}_2) \times \mathbb{F}_2^2 \setminus \{(0,0)\} \to \mathbb{F}_2^2 \setminus \{(0,0)\}, (A, v) \mapsto \psi_A(v). \tag{139}$$

Analog zu oben rechnet man nach, dass es sich hierbei um eine Gruppenoperation handelt, denn $\psi(E_2, v) = \psi_{E_2}(v) = E_2 v = v$ für alle $v \in \mathbb{F}_2^2 \setminus \{(0,0)\}$. Ebenso stellen wir fest, dass $\psi(AB, v) = \psi_{AB}(v) = (AB)v = A(Bv) = A(\psi_B(v)) = \psi_A(\psi_B(v)) = \psi(A, \psi(B, v))$ für alle $A, B \in \mathrm{GL}_2(\mathbb{F}_2)$ und $v \in \mathbb{F}_2^2 \setminus \{(0,0)\}$. Nach einem Vorlesungsresultat erhalten wir aus der Gruppenoperation den Homomorphismus $\Psi : \mathrm{GL}_2(\mathbb{F}_2) \to \mathrm{Per}(\mathbb{F}_2^2 \setminus \{(0,0)\}) \simeq S_3$ wegen $|\mathbb{F}_2^2 \setminus \{(0,0)\}| = 3$, explizit gegeben durch $\Psi(A) = (v \mapsto Av)$. Da eine Matrix $A \in \mathrm{GL}_2(\mathbb{F}_2)$ bereits durch Angabe der (verschiedenen!) Bilder $v_1, v_2 \in \mathbb{F}_2^2 \setminus \{(0,0)\}, v_1 \neq v_2$ von, ohne Einschränkung, $(0,1), (1,0) \in \mathbb{F}_2^2 \setminus \{(0,0)\}$ festgelegt ist, finden wir zu zu $(0,1) \mapsto v_1$, $(1,0) \mapsto v_2$ und, folglich, $(1,1) \mapsto v - 1 + v_2$ die Matrix $A$ zu $A = (v_1 | v_1)$. Man sieht leicht, dass $A \in \mathrm{GL}_2(\mathbb{F}_2)$, denn $v_1, v_2 \in \mathbb{F}_2^2 \setminus \{(0,0)\}$ mit $v_1 \neq v_2$. Ebenso wie oben stellt man fest, dass $A \in \ker \Psi \Leftrightarrow A = E_2$. Damit ist $\Psi$ ein Isomorphismus von Gruppen, und wir haben $\mathrm{GL}_2(\mathbb{F}_2) = S_3$ verifiziert. □

**Aufgabe 98 (F19T2A4)** (a) Zu untersuchen ist, ob $\mathbb{Q}[X]/J$, wo $J = (X^5 - 2, X^6 + X^5 - 2X - 2)$, ein Körper ist. Wir stellen zunächst fest, dass $X^6 + X^5 - 2X - 2$

nicht irreduzibel in $\mathbb{Q}[X]$ ist. Denn es gilt $X^6 + X^5 - 2X - 2 = (X + 1)(X^5 - 2)$. Da $X + 1$, $X^5 - 2 \in \mathbb{Q}[X]$ Nicht-Einheiten sind, ist $X^6 + X^5 - 2X - 2$ also nicht irreduzibel. Insbesondere ist $X^6 + X^5 - 2X - 2 \in (X^5 - 2)$. Wir finden also, dass $J = (X^5 - 2)$. Damit reicht es, zu zeigen, dass $\mathbb{Q}[X]/(X^5 - 2)$ ein Körper ist. Wir stellen zuerst fest, dass $P = X^5 - 2 \in \mathbb{Q}[X]$ nach Eisenstein zur Primzahl $p = 2$ irreduzibel in $\mathbb{Q}[X]$ ist. Da $\mathbb{Q}[X]$ ein faktorieller Ring ist, ist $P$ also ein Primelement in $\mathbb{Q}[X]$, also $J = (P)$ ein Primideal. Da ferner $\mathbb{Q}[X]$ als univariater Polynomring über einem Körper ein Hauptidealring ist, ist $J$ bereits maximal. Die Maximalität des Ideals $J$ bedeutet aber gerade, dass $\mathbb{Q}[X]/J$ ein Körper ist. Weiterführend kann man mithilfe des Einsetzungshomomorphismus unter Verwendung des Homomorphiesatzes für Ringe zeigen, dass $\mathbb{Q}[X]/J \simeq \mathbb{Q}(\sqrt[5]{2})$.
(b) Zu untersuchen ist, ob $\mathbb{Z}[X]/(5, X^3 - 2X^2 + 4)$ ein Körper ist. Als normiertes Polynom vom Grad 3 mit ganzzahligen Koeffizienten, kommen als ganzzahlige Nullstellen von $X^3 - 2X^2 + 4$ nur die Teiler von 4 in Betracht. Wir stellen aber fest, dass keine der Zahlen aus $\{\pm 1, \pm 2, \pm 4\}$ eine Nullstelle von $X^3 - 2X^2 + 5$ ist. Damit ist $X^3 - 2X^2 + 4$ irreduzibel über $\mathbb{Z}[X]$. Wir zeigen nun, dass $\Phi : \mathbb{Z}[X]/(5, X^3 - 2X^2 + 4) \to \mathbb{F}_5[X]/(X^3 - 2X^2 + 4), f + (5, X^3 - 2X^2 + 4) \mapsto \bar{f} + (X^3 - 2X^2 + 4)$ ein Isomorphismus von Ringen ist. $\bar{f}$ bezeichnet dabei die Reduktion des Polynoms $f \in \mathbb{Z}[x]$ modulo 5. Offenbar gilt $\Phi(1 + (5, X^3 - 2X^2 + 4)) = \bar{1} + (X^3 - 2X^2 + 4)$ und, da die Reduktionsabbilung bekanntlich ein Ringhomomomorphismus ist, zusammen mit den Rechenregeln für Faktorringe $\Phi((f + g) + (5, X^3 - 2X^2 + 4)) = \Phi(f + (5, X^3 - 2X^2 + 4)) + \Phi(g + (5, X^3 - 2X^2 + 4))$ sowie $\Phi((f \cdot g) + (5, X^3 - 2X^2 + 4)) = \Phi(f + (5, X^3 - 2X^2 + 4)) \cdot \Phi(5, X^3 - 2X^2 + 4)$ für $f, g \in \mathbb{Z}[X]$. Damit haben wir nachgewiesen, dass es sich um einen Ringhomomorphismus handelt. Für den Nachweis der Surjektivität verwenden wir, dass $f \in \ker \Phi \Leftrightarrow \Phi(f) = 0 + (X^3 - 2X^2 + 4)$ genau dann, wenn jeder der Koeffizienten $a_k$ von $g = \sum_{k=0}^{\deg(f)} a_k X^k$ durch 5 teilbar ist, wobei $g$ derjenige Rest ist, der im euklidischen Ring $\mathbb{Z}[x]$ mit der Gradfunktion als Höhenfunktion bei Division durch $X^3 - 2X^2 + 4$ als Rest verbleibt, also $f = q \cdot X^3 - 2X^2 + 4 + g$. Dann ist aber bereits $f \in (5, X^3 - 2X^2 + 4)$ und es gilt $\ker \Phi \subseteq (5, X^3 - 2X^2 + 4)$. Umgekehrt wird jedes $f \in (5, X^3 - 2X^2 + 4)$ offensichtlich auf $0 \in \mathbb{F}_5[X]/(X^3 - 2X^2 + 4)$ abgebildet vermöge $\Phi$. Es ist nun $X^3 - 2X^2 + 4 \in \mathbb{F}_5[X]$ ebenfalls irreduzibel, denn es hat keine Nullstellen im Körper $\mathbb{F}_5$. Da $\mathbb{F}_5$ ein Körper ist, ist $\mathbb{F}_5[X]$ ein Hauptidealring und insbesondere ein faktorieller Ring. Da $X^3 - 2X^2 + 4$ irreduzibel ist, ist es im faktoriellen Ring $\mathbb{F}_5[X]$ bereits prim, $(X^3 - 2X^2 + 4) \subsetneq \mathbb{F}_5[X]$ also ein Primideal. Mit derselben Begründung ist dann $(X^3 - 2X^2 + 4)$ ein maximales Ideal, also $\mathbb{F}_5[X]/(X^3 - 2X^2 + 4)$ ein Körper. Vermöge Existenz- und Eindeutigkeitssatz für endliche Körper folgert man, dass $\mathbb{F}_5[X]/(X^3 - 2X^2 + 4) \simeq \mathbb{F}_{5^3=125}$. Letzteres ist aber über die Aufgabe hinausgehend. □

**Aufgabe 99 (F19T3A4)** Sei $\mathbb{F}_{11} = \mathbb{Z}/11\mathbb{Z}$ der Körper mit 11 Elementen. Wir zeigen, dass $\mathbb{F}_{11}[X]/(X^2 + 1)$ und $\mathbb{F}_{11}[X]/(X^2 + X + 4)$ jeweils ein Körper mit 121 Elementen sind. Wir stellen zunächst fest, dass $P_1 \equiv X^2 + 1$ und $P_2 \equiv X^2 + X + 4$ jeweils normierte Polynome vom Grad 2 sind, insbesondere also keine Einheiten in $\mathbb{F}_{11}[X]$. Damit $P_1$, $P_2$ jeweils irreduzibel sind, ist zu zeigen, dass sie beide keine Nullstelle in $\mathbb{F}_{11}$ haben. Sonst würden sie jeweils in Linearfaktoren zerfallen,

wären also nicht irreduzibel. Wir sehen aber, dass $X^2 \equiv -1 \bmod(11)$ kein quadratischer Rest ist, denn nach den Ergänzungsätzen zu den Legendre-Symbolen ist $(-1/11) = (-1)^{(p-1)/2} = -1$. Damit gibt es kein $X \in \mathbb{Z}/(11\mathbb{Z}) = \mathbb{F}_{11}$, sodass $X^2 \equiv -1 \bmod(11)$. Also hat $P_1$ keine Nullstelle in $\mathbb{F}_{11}$ und ist damit als Polynom vom Grad 2 bereits irreduzibel über $\mathbb{F}_{11}$. Durch Einsetzen stellen wir zudem fest, dass $P_2(X) \neq 0$ für alle $X \in \mathbb{F}_{11}$. Damit ist auch $P_2$ als Polynom vom Grad 2 irreduzibel über $\mathbb{F}_{11}$. Da $\mathbb{F}_{11}$ ein Körper ist, ist $\mathbb{F}_{11}[X]$ ein Hauptidealring, insbesondere ein faktorieller Ring. Da $P_1, P_2$ in $\mathbb{F}_{11}[X]$ irreduzibel sind, sind sie dort bereits Primelemente. Also ist $(P_1), (P_2) \subsetneq \mathbb{F}_{11}[X]$ jeweils ein Primideal dort. Da $\mathbb{F}_{11}[X]$ faktoriell ist, sind $(P_1), (P_2)$ als Primideale bereits maximale Ideale in $\mathbb{F}_{11}[X]$. Damit ist $\mathbb{F}_{11}[X]/(X^2+1)$ und $\mathbb{F}_{11}[X]/(X^2+X+4)$ jeweils bereits ein Körper. Wir zeigen nun, dass diese Körper jeweils isomorph zu $\mathbb{F}_{11^2=121}$ sind. Dazu beachten wir, dass $P_1, P_2$ im algebraischen Abschluss $\mathbb{F}_{11}^{\text{alg}}$ jeweils eine Nullstelle, $\alpha_1$ bzw. $\alpha_2$ haben. Da $P_1, P_2$ normiert und irreduzibel sind, sind sie die Minimalpolynome von $\alpha_1, \alpha_2$ über $\mathbb{F}_{11}$. Es gibt also Ringhomomomorphismen $\Phi_1 : \mathbb{F}_{11}[X]/(X^2+1) \to \mathbb{F}_{11}(\alpha_1)$ und $\mathbb{F}_{11}[X]/(X^2+X+4) \to \mathbb{F}_{11}(\alpha_2)$, jeweils definiert durch den Einsetzungshomomorphismus – Das ist bekannt aus den Vorlesungen. Da $[\mathbb{F}_{11}(\alpha_1) : \mathbb{F}_{11}] = 2 = [\mathbb{F}_{11}(\alpha_2) : \mathbb{F}_{11}]$, ist wegen des Existenz- und Eindeutigssatzes für endliche Körper $\mathbb{F}_{11}(\alpha_1) \simeq \mathbb{F}_{11^2}$ und $\mathbb{F}_{11}(\alpha_2) \simeq \mathbb{F}_{11^2}$. Durch Komposition der jeweils beiden Bijektionen sehen wir, dass die Körper $\mathbb{F}_{11}[X]/(P_1)$ und $\mathbb{F}_{11}[X]/(P_2)$ jeweils genauso viele Elemente wie $\mathbb{F}_{11^2=121}$ haben, also 121 Elemente, wie behauptet worden ist. Der Isomorphismus $\psi : \mathbb{F}_{11}[X]/(P_1) \to \mathbb{F}_{11}[X]/(P_2)$ für Teil ist gegeben durch Angabe des Bildes von $X$ unter $\psi$. Denn jedes $f \in \mathbb{F}_{11}[X]/(P_1)$ ist von der Form $f = aX + b$ mit $a, b \in \mathbb{F}_{11}$ und die Ringhomomomorphismuseigenschaft von $\psi$ erfordert, dass $\psi(1) = 1$. Damit muss $\psi(X^2 + 1) = 0 + (X^2 + X + 4)$, also $\psi(X)^2 = -1 + (X^2 + X + 4)$. Da $\psi(X)$ maximal ein Polynom vom Grad 1 sein kann, haben wir $(aX+b)^2+1 = 0+(X^2+X+4)$, d.h., $a^2X^2+2abX+b^2+1 = 0+(X^2+X+4)$. Damit finden wir, dass $a^2 \equiv c \bmod(11)$, $2ab \equiv c \bmod(11)$, $b^2 + 1 \equiv 4c \bmod(11)$ für ein $c \in \mathbb{F}_{11}$. Setzen wir $c = 1$, so finden wir, dass $a = 10$ und $b = 5$ erfüllen $(10X+5)^2 = 100X^2+100X+25 = X^2+X+3$, sodass $(10X+5)^2+1 = X^2+X+4$. Damit ist ist $\Phi(X^2 + 1) = 0 + (X^2 + X + 4)$ und wir finden $\Phi(X) = 10X + 5$. □

**Aufgabe 100 (F19T3A1)** Sei $p$ eine Primzahl und sei $\mathbb{Z}_{(p)}$ der Teilring von $\mathbb{Q}$, der definiert ist durch

$$\mathbb{Z}_{(p)} \equiv \left\{ \frac{a}{b} | a \in \mathbb{Z}, b \in \mathbb{N}, p \not| b \right\}. \tag{140}$$

(a) Zu zeigen ist, dass die Abbildung $\phi : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}$ definiert durch $\phi(a + p\mathbb{Z}) = a + p\mathbb{Z}_{(p)}$ ein Isomorphismus von Ringen ist. Wir zeigen zuerst, dass es sich um eine Homomorphismus von Ringen handelt. Dabei können wir laut Aufgabenstellung verwenden, dass $\mathbb{Z}_{(p)}$ ein Teilring von $\mathbb{Q}$ ist. Wir sehen, dass $1 + p\mathbb{Z}$ unter $\phi$ auf das Neutralement $1 + p\mathbb{Z}_{(p)}$ der Multiplikation in $\mathbb{Z}_{(p)}$ abgebildet wird. Seien nun $a, b \in \{0, 1, 2, ..., p-1\}$ Repräsentanten der Restklasse $a + p\mathbb{Z}$ bzw. $b + p\mathbb{Z}$. Dann gilt

$$\begin{aligned} \phi(a + p\mathbb{Z})\phi(b + p\mathbb{Z}) &= (a + p\mathbb{Z}_{(p)})(b + p\mathbb{Z}_{(p)}) = ab + ap\mathbb{Z}_{(p)} + bp\mathbb{Z}_{(p)} = ab + p\mathbb{Z}_{(p)} \\ &= \phi(ab + p\mathbb{Z}). \end{aligned} \tag{141}$$

Ebenso sehen wir

$$\begin{aligned}\phi(a+b+p\mathbb{Z}) &= a+b+p\mathbb{Z}_{(p)} = \big(a+p\mathbb{Z}_{(p)}\big)+\big(b+p\mathbb{Z}_{(p)}\big)\\ &= \phi(a+p\mathbb{Z})+\phi(b+p\mathbb{Z}).\end{aligned} \tag{142}$$

Damit ist die Homomorphismuseigenschaft nachgewiesen. Wir zeigen als nächstes, dass $\phi$ injektiv ist, d.h., $\ker\phi = \{0+p\mathbb{Z}\}$. Zunächst zu "$\supseteq$": Es gilt $\phi(0+p\mathbb{Z}) = 0+p\mathbb{Z}_{(p)}$ und 0 ist das von $\mathbb{Q}$ geerbte Neutralelement bzgl. der Addition in $\mathbb{Z}_{(p)}$. Zu "$\subseteq$": Sei $a+p\mathbb{Z}_p \in \mathbb{Z}/p\mathbb{Z}$ mit $a+p\mathbb{Z} \in \ker\phi$ vorgegeben. Wir wählen $a \in \{0,1,2,...,p-1\}$ als Repräsentant der Restklasse modulo $p$. Es gilt $\phi(a+p\mathbb{Z}_p) = a+p\mathbb{Z}_{(p)} = 0+p\mathbb{Z}_{(p)}$. Das können wir umschreiben zu $a \in p\mathbb{Z}_{(p)}$. Dann gibt es $A \in \mathbb{Z}$ und $B \in \mathbb{N}$, sodass $p \not| B$ und $a = Ap/B$. Da $a$ eine nicht-negative Ganzzahl kleiner $p$ ist, muss $A/B \in \mathbb{N}_0$ sein. Da $a < p$, kann die Gleichheit dann nur für $A/B = 0$ erfüllt sein. Damit finden wir $a = 0$, also $\ker\phi \subseteq \{0+p\mathbb{Z}\}$, wie zu zeigen war. Damit haben wir gezeigt, dass $\phi$ injektiv ist. Zuletzt müssen wir zeigen, dass $\phi$ surjektiv ist. Sei dazu $a+p\mathbb{Z}_{(p)} \in \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}$ vorgegeben. Zu zeigen ist, dass ein $A+p\mathbb{Z} \in \mathbb{Z}/p\mathbb{Z}$ gibt, sodass $\phi(A+p\mathbb{Z}) = a+p\mathbb{Z}_{(p)}$. $a = C/D$ mit $C \in \mathbb{Z}, D \in \mathbb{N}$ und $p \not| D$. Es gilt $\phi(C+p\mathbb{Z}) = C+p\mathbb{Z}_{(p)}$. Wegen $p \not| D$, ist $D \not\equiv 0 \bmod(p)$, also ist $(B+p\mathbb{Z}) \in (\mathbb{Z}/p\mathbb{Z}) = \mathbb{Z}/p\mathbb{Z} \setminus \{0+p\mathbb{Z}\}$, wobei $B \cdot D = 1 \bmod(p)$ eindeutig bestimmt ist. Dann gilt $\phi(C/D+p\mathbb{Z}) = \phi(C+p\mathbb{Z})\phi(D+p\mathbb{Z})^{-1} = C/D+p\mathbb{Z}_{(p)} = a+p\mathbb{Z}_{(p)}$. Damit haben wir auch die Surjektivität nachgewiesen. Insgesamt ist also $\phi$ ein Isomorphismus von Ringen. Alternativ über Homomorphiesatz.
(b) Wir arbeiten hier in $\mathbb{Z}_{(5)}/5\mathbb{Z}_{(5)}$. Gesucht ist das Ergebnis der Addition $2/3 + 1/7 + 5\mathbb{Z}_{(5)}$ dort. Es ist nach Anwendung des Isomorphismus aus Teil (a) $\phi^{-1}(2+5\mathbb{Z}_{(5)})\phi^{-1}(3+5\mathbb{Z}_{(5)})^{-1} + \phi^{-1}(1+5\mathbb{Z}_{(5)})\phi^{-1}(7+5\mathbb{Z}_{(5)})^{-1} = (2+5\mathbb{Z})(2+5\mathbb{Z}) + (1+5\mathbb{Z})(3+5\mathbb{Z}) = 7+5\mathbb{Z} = 2+5\mathbb{Z}$. Also finden wir durch Verkettung der Gleichung mit $\phi$ von außen, dass $2/3+1/7+5\mathbb{Z}_{(5)} = 2+5\mathbb{Z}_{(5)}$. □

**Aufgabe 101 (H06T1A1)** Sei $p = X^3 - X + 2 \in \mathbb{Q}[X]$ und $q = X^2 - 2X + 2 \in \mathbb{Q}[X]$.
(a) Zu zeigen ist, dass $K = \mathbb{Q}[X]/(p)$ ein Körper ist. Wir stellen zuerst fest, dass $\mathbb{Q}[X]$ als univariater Polynomring über dem Körper $\mathbb{Q}$ ein Hauptidealring ist. Das Polynom $p$ hat ganzzahlige Koeffizienten und ist überdies normiert, sodass das Lemma von Gauss liefert, dass jede rationale Nullstelle von $p$ bereits ganzzahlig ist. Überdies müssen diese dann ein Teiler des konstanten Terms, 2, sein. Durch Einsetzen sehen wir, dass $p(0) = 2, p(1) = 2, p(-1) = 2, p(2) = 8, p(-2) = -4$, sodass $p$ nach der vorherigen Argumentation bereits nullstellenfrei in $\mathbb{Q}$ ist. Da $p \notin \mathbb{Q}^\times = (\mathbb{Q}[X])^\times$ als nicht-konstantes Polynom, ist $p$ damit bereits irreduzibel, denn wäre $p$ nicht irreduzibel, wäre es als Nicht-Einheit reduzibel, hätte also als Polynom vom Grad 3 bereits eine Nullstelle in $\mathbb{Q}$. Dem ist aber nicht so. Da $\mathbb{Q}[X]$ faktoriell ist, ist bereits jedes irreduzible Element auch ein Primelement und das Hauptideal $(p)$ ist damit ein Primideal. Aus demselben Grund ist $(p)$ als Primideal im faktoriellen Ring $\mathbb{Q}[X]$ bereits maximales Ideal. Laut elementarer Ringtheorie ist der Quotientenring $\mathbb{Q}[X]/(p)$ infolge der Maximalität von $(p)$ als Ideal dann bereits ein Körper. Damit haben wir die Körpereigenschaft von $\mathbb{Q}[X]/(p)$ nachgewiesen.
(b) Wir sollen nun in $K \equiv \mathbb{Q}[X]/(p)$ ein multiplikatives Inverses zur Restklasse $[q]$ finden. Da $\deg(q) = 2 < \deg(p) = 3$ ist bereits $[q] \neq 0_K$, sodass $[q] \in K^\times$. Damit

ist bereits die Existenz und Eindeutigkeit des Inversen $[q]^{-1} \in K^\times$ gewährleistet. Dieses bestimmen wir mittels Euklidischem Algorithmus. Da $p$ irreduzibel ist, gilt insbesondere $q \not| p$ in $\mathbb{Q}[X]$ und somit $\mathrm{ggT}(p,q) = 1$. Wir wenden den Euklidischen Algorithmus an, um Polynome $x, y \in \mathbb{Q}[X]$ zu finden, sodass $xp + yq = 1$. Das ist möglich, weil $\mathbb{Q}[X]$ mit der Gradfunktion als Höhenfunktion ein euklidischer Ring ist. Polynomdivision liefert:

$$\begin{aligned}(X^3 - X + 2) : (X^2 - 2X - 2) &= X + (X^2 + X + 2) : (X^2 - 2X - 2) \\ &= X + 1 + (3X + 4) : (X^2 - 2X - 2).\end{aligned} \tag{143}$$

Setze $r = 3X + 4$. Dann ist weiter

$$\begin{aligned}(X^2 - 2X - 2) : (3X + 4) &= X/3 + (-10/3X - 2) : (3X + 4) \\ &= X/3 - 10/9 + (22/9) : (3X + 4).\end{aligned} \tag{144}$$

Damit ist $x' = -(X/3 - 10/9)$ und $y' = 1 - (-(X + 1))(X/3 - 10/9)$ mit der Eigenschaft, dass

$$x'p + y'q = 22/9. \tag{145}$$

Multiplikation mit $9/22$ und Reduktion $\mathrm{mod}(p)$ liefert dann $[q]^{-1} = [9/22 + 9/22(X + 1)(X/3 - 10/9)]$. □

**Aufgabe 102 (H00T2A2)** Wir suchen die Anzahl der Elemente in $\mathbb{Z}/15015\mathbb{Z} =: R$ mit der Eigenschaft, dass $x^2 = x$ für das $x \in R$. Zunächst stellen wir fest, dass $15015 = 1001 \cdot 15$. Ferner gilt $1001 = 13 \cdot 11 \cdot 7$ und $15 = 5 \cdot 3$. Damit hat 15015 jeweils nur einfache Primfaktoren und es gilt $15015 = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$. Da $p, q \in \{3, 5, 7, 11, 13\}$ teilerfremd genau dann sind, wenn $p \neq q$, sind $(p)$ und $(q)$ für alle voneinander verschiedenen Primzahlen jeweils ko-prim, $(p) + (q) = R$. Nach chinesischem Restklassensatz erhalten wir also einen Isomorphismus von Ringen

$$\Phi : \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z} \to \mathbb{Z}/15015\mathbb{Z}, \tag{146}$$

wobei $([a]_3, [a]_5, [a_7], [a]_{11}, [a]_{13}) \mapsto [a]_{15015}$ für $a \in \mathbb{Z}$ und $[a]_k = a \,\mathrm{mod}(k)$ indiziert. Die Multiplikation ist dabei komponentenweise definiert. Da jeweils modulo einer Primzahl reduziert wird, ist jeder der Faktoren des Rings auf der Urbild-Seite des Isomorphismus aus dem Chinesischen Restsatz sogar ein Körper. Wir suchen nun zuerst in den einzelnen Faktoren Elemente $y \in \mathbb{Z}/p\mathbb{Z}$, die $y^2 = y$ erfüllen. Durch Umschreiben der Gleichung sehen wir, dass $y$ dann Nullstelle des Polynoms $P(y) = y^2 - y$ ist. Dieses hat als Polynom zweiten Grades keine oder zwei Nullstellen, hier also jeweils $y \in \{0, 1\}$ für jeden der Primfaktoren $p \in \{3, 5, 7, 11, 13\}$ von 15015. Wir haben also für jeden der 5 Faktoren genau 2 Möglichkeiten, die korrespondierende Komponente zu erfüllen, sodass die Gleichung $x^2 = x$, $x \in \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}$ gewährleistet wird. Damit finden wir, dass es genau $|\{0, 1\}|^{|\{3,5,7,11,13\}|} = 2^5 = 32$ Elemente mit der gewünschten Eigenschaft gibt. Hierbei befinden wir uns weiterhin auf der Seite des Produktrings. Da $\Phi$ ein Isomorphismus von Ringen ist, insbesondere also bijektiv und mit den Multiplikationsverknüpfungen der beiden Ringen kompatibel ist, ist die Anzahl der Elemente für $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times$

$\mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}$ und $\mathbb{Z}/15015\mathbb{Z}$ mit $y^2 = y$ gleich, d.h., auch in $\mathbb{Z}/15015\mathbb{Z}$ gibt es $2^5 = 32$ Elemente mit der geforderten Eigenschaft. Explizit finden wir bspw. die Elemente $\Phi(1,0,0,0,0), \Phi(0,1,0,0,0), \Phi(0,0,1,0,0), \Phi(0,0,0,1,0), \Phi(0,0,0,0,1) \in \mathbb{Z}/15015\mathbb{Z}$, die den Anforderungen im zweiten Teil der Aufgabenstellung genügen. Das sind dann ganz konkret (in dieser Reihenfolge) die Elemente $[5005]_{15015}, [3003]_{15015}$, $[2145]_{15015}, [1365]_{15015}, [1155]_{15015} \in \mathbb{Z}/15015\mathbb{Z}$, wie man leicht durch Einsetzen in die Abbildungsvorschrift aus dem Chinesischen Restsatz bestätigt. □

**Aufgabe 103 (F19T2A3(a))** Sei $m \geq 1$ eine ungerade ganze Zahl. Zu zeigen ist, dass

$$\sum_{k=1}^{m-1} k^m \equiv 0 \,\mathrm{mod}(m). \tag{147}$$

Sei also $m$ eine beliebige ungerade Ganzzahl mit $m \geq 1$. Offenbar hat die obenstehende Summe $m-1$ Summanden, d.h., eine gerade Anzahl an Summanden. Da die Summe nach Voraussetzung an $m$ endlich ist, können wir sie umordnen,

$$X \equiv \sum_{k=1}^{m-1} k^m = \sum_{k=1}^{(m-1)/2} \left(k^m + (m-k)^m\right). \tag{148}$$

Auf die rechte Seite können wir für jeden einzelnen Summanden in Klammern den binomischen Lehrsatz anwenden. Das liefert uns unter Beachtung, dass für $m$ als ungerade Zahl gilt $(-1)^m = -1$, die gewünschte Aussage

$$\begin{aligned} X &= \sum_{k=0}^{(m-1)/2} \left( k^m + \sum_{l=0}^{m} \binom{m}{k} m^l (-k)^{m-l} \right) \\ &= \sum_{k=0}^{(m-1)/2} \sum_{l=1}^{m} \binom{m}{k} m^l (-k)^{m-l} \\ &= m \sum_{k=0}^{(m-1)/2} \sum_{l=1}^{m} \binom{m}{k} m^{l-1} (-k)^{m-l} \\ &\equiv 0 \,\mathrm{mod}(m). \end{aligned} \tag{149}$$

Sei nun $m \in \mathbb{N}$ beliebig und $x_1, ..., x_m$ ganze Zahlen. Zu zeigen ist, dass eine nichtleere Teilmenge $I \subseteq \{1, 2, 3, ..., m\}$ existiert, sodass

$$\sum_{i \in I} x_i \equiv 0 \,\mathrm{mod}(m). \tag{150}$$

Wir betrachten für alle $j \in \{1, ..., m\}$ die Terme

$$T_j = \left( \sum_{k=1}^{j} x_k \right) \mathrm{mod}(m). \tag{151}$$

Falls bereits ein Index $J$, $1 \leq J \leq m$ existiert, sodass $T_J \equiv 0 \,\mathrm{mod}(m)$, dann erfüllt die Menge $I = \{1, ..., J\}$ die gewünschten Eigenschaften. Falls hingegen kein

$J$, $1 \leq J \leq m$ mit der oben genannten Eigenschaft existiert, dann gibt es zwei verschiedene Indizes $J_1, J_2 \in \{1, 2, ..., m\}$, sodass $T_{J_1} = T_{J_2} \bmod(m)$, denn es stehen nur $m-1$ verschiedene Werte zur Verfügung, die die Terme $T_j$ jeweils annehmen können, und wir betrachten $m$ dieser Terme. Ohne Einschränkung ist $J_1 < J_2$. Durch Substraktion finden wir, dass $I = \{J_1 + 1, ..., J_2\}$ nun die Menge mit den gewünschten Eigenschaften ist. □

**Aufgabe 104 (F19T1A3)** Wir betrachten den Ring $R = \mathbb{Z}[\sqrt{-3}]$ und die multiplikative Funktion $N(a + b\sqrt{-3}) = a^2 + 3b^2$. Zunächst bestimmen wir die Einheitengruppe von $R$. Bekannt ist, dass $1 = 1 + 0 \cdot \sqrt{-3}$ das Neutralelement bzgl. der Multiplikation in $R$ ist. Es gilt $N(1) = 1$. Für eine beliebige Einheit $a \in R^\times$ gilt nun $N(a)N(b) = N(1) = 1$, nach Definition einer Einheit und der als gegeben vorausetzbaren Multiplikativität von $N$. Nach Definition von $N$ gilt ferner, dass $N(a) \geq 1$ für alle $a \in R$. Somit muss für eine Einheit gelten, dass $N(a) = 1$. Die einzigen Elemente aus $R$, die diesen Bedingung erfüllen sind 1 und $-1$. Wir sehen, dass 1 als Neutralelement $1 \cdot 1 = 1$ erfüllt und $(-1) \cdot (-1) = 1$ gilt. Beide Elemente sind also Einheiten, und, wegen der Notwendigkeit der hergeleiteten Bedingung an eine Einheit, auch die einzigen beiden Einheiten von $R$ sind. Somit ist $R^\times = \{1, -1\}$. Wir zeigen nun, dass jedes Element $x = a + b\sqrt{-3} \in R$ mit $N(x) = 4$ irreduzibel ist. Hierzu schreiben wir aus $a^2 + 3b^2 = 4$. Angenommen, ein derartiges Element wäre nicht irreduzibel. Wegen $N(x) = 4 > 1$ ist $x$ damit eine Nicht-Einheit, also reduzibel. Insofern gibt es zwei Nicht-Einheiten $y, z \in R$, sodass $x = yz$. Aus der Multiplikativität der Normfunktion finden wir $4 = N(x) = N(yz) = N(y)N(z)$, sodass $N(y), N(z)|4$ und $N(y) \neq 1 \neq N(z)$, da die einzigen beiden Elemente in $R$, die diese Bedingung erfüllen bereits Einheiten sind. Also gilt $N(y) = 2 = N(z)$. Da $3 > 0$, ist die einzige Möglichkeit, dass $y = a_y + 0 \cdot \sqrt{-3}$ und $z = a_z + 0 \cdot \sqrt{-3}$. Dann gilt $a_y^2 = 2 = a_z^2$. Da 2 aber kein Quadrat in $\mathbb{Z}$ ist, können wir diese Bedingungen nicht erfüllen. Folglich gibt es keine Nicht-Einheiten $y, z \in R$, sodass $x = yz$. Also ist $x$ nicht reduzibel, als Nicht-Einheit mithin irreduzibel. Wir behaupten zuletzt, dass $R$ nicht faktoriell ist. Hierzu betrachten wir das Element $4 \in R$. Es gilt $4 = (1+\sqrt{-3})(1-\sqrt{-3})$ und $4 = 2 \cdot 2$. Da $4 = N(1+\sqrt{-3}) = N(1-\sqrt{-3}) = N(2)$, sind $2, 1+\sqrt{-3}, 1-\sqrt{-3}$ irreduzibel in $\mathbb{Z}[\sqrt{-3}]$. Wäre $R$ faktoriell, so besäße 4 eine bis auf Reihenfolge und Einheiten eindeutige Faktorisierung in irreduzible Elemente. Dies ist aber nicht der Fall, wie wir durch die Angabe der beiden Faktorisierungen von 4 gesehen haben. Folglich ist $\mathbb{Z}[\sqrt{-3}]$ nicht faktoriell. □

**Aufgabe 105 (F13T3A4)** (a) Wir bestimmen zunächst alle normierten, irreduziblen Polynome in $\mathbb{F}_3[x]$, die den Grad $\leq 2$ haben. Da $(\mathbb{F}_3[x])^\times = \mathbb{F}_3$ kommt für ein irreduzibles Polynom lediglich ein $f \in \mathbb{F}_3[x]$ mit $\deg(f) \in \{1, 2\}$ in Betracht. Bekanntlich sind die Polynome vom Grad 1 in einem Polynomring über einem Körper irreduzibel. Damit finden wir $x+1, x+2, x$ als irreduzible, normierte Polynome vom Grad 1 in $\mathbb{F}_3[x]$. Für die normierten irreduziblen Polynome vom Grad 2 kommen nur die Polynome der Form $x^2 + ax + b$ mit $a \in \mathbb{F}_3$ und $b \in \{1, 2\}$ in Betracht. Wäre $b = 0$, so könnten wir den irreduziblen Faktor $x$ abspalten, was der Irreduzibilität des betrachteten Polynoms vom Grad 2 zuwiderliefe. Außer acht bleiben ferner die drei Polynome $(x+1)^2 = x^2+2x+1$, $(x+2)^2 = x^2+x+1$ und $(x+2)(x+1) = x^2+2$, denn

auch in diesem Fällen könnten wir einen Linearfaktor abspalten. Somit sind lediglich $x^2+2x+2, x^2+1, x^2+x+2$ Kandidaten für die gesuchten irreduziblen Polynome vom Grad 2, die normiert sind. Per Konstruktion haben diese keine Nullstellen in $\mathbb{F}_3$ und sind daher als Polynome vom Grad 2 bereits irreduzibel. Zusammenfassend ist die Menge der normierten, irreduziblen Polynome vom Grad $\leq 2$ in $\mathbb{F}_3[x]$ also gegeben durch

$$I = \left\{x, x+1, x+2, x^2+2x+2, x^2+x+2, x^2+1\right\}. \tag{152}$$

(b) Gegeben sei das Polynom $p = x^4+9x^2-2x+2 \in \mathbb{Q}[x]$. Offenbar ist $p$ normiert und hat ganzzahlige Koeffizienten. Wir schließen zunächst aus, dass $p$ eine, nach dem Lemma von Gauss, ganzzahlige Nullstelle hat. Dann lässt sich zumindest kein Linearfaktor von $p$ abspalten, d.h., $p$ kann höchstens in zwei Polynome vom Grad 2 faktorisieren, die, ebenfalls nach dem Lemma von Gauss, aus $\mathbb{Z}[x]$ stammen. Eine ganzzahlige Nullstelle von $p$ müsste das konstante Glied 2 restfrei teilen, also $x_0 \in \{1, 2, -1, -2\}$. Wir sehen aber, dass $p(1) = 10$, $p(-1) = 14$, $p(2) = 54$, $p(-2) = 62$. Die Unmöglichkeit, Linearfaktoren abzuspalten transferiert sich wegen der Morphismuseigenschaft der Reduktionsabbildung auch auf $p \bmod(3) \in \mathbb{F}_3[x]$. Damit kann $p$ höchstens in zwei Polynome vom Grad 2 faktorisieren. Dies prüfen wir in $\mathbb{F}_3[x]$ vermöge des Reduktionskriteriums, denn $3 \nmid 1$. Es gilt $p \equiv x^4+x+2 \bmod(3)$. Zudem sind $(x^2+1)(x^2+x+2) = x^4+x^3+x+2$ und $(x^2+1)(x^2+2x+2) = x^4+2x^3+2x+2$ die einzigen Möglichkeiten aus irreduziblen Polynomen vom Grad 2 Polynome vom Grad 4 zu erzeugen, deren konstantes Glied 2 ist. Beide stimmen nicht mit dem modulo 3 reduzierten $p$ überein. Da $\mathbb{F}_3[x]$ als Polynomring über einem Körper ein Hauptideal- und damit faktorieller Ring ist, folgt mit der Unmöglichkeit, einen Linearfaktor von $p \bmod(3)$ abzuspalten (s.o.), dass $p \bmod(3)$ in $\mathbb{F}_3[x]$ irreduzibel ist. Das Reduktionskriterium liefert nun die Irreduzibilität von $p$ in $\mathbb{Z}[x]$. Laut dem Lemma von Gauss impliziert das die Irreduzibilität von $p$, aufgefasst als Element von $\mathbb{Q}[x]$. □

**Aufgabe 106 (F14T3A2)** (a) Sei $c \in R$, wobei $R$ ein kommutativer Ring mit 1 ist. Für $a, b \in R$ definieren wir $a \equiv b \bmod(c)$ genau dann wenn ein $d \in R$ existiert, sodass $a - b = c \cdot d$. Wir zeigen, dass es sich hierbei um eine Äquivalenzrelation handelt. Offenbar liegt bereits eine Relation auf $R$ vor. Wir zeigen, dass diese Relation reflexiv, symmetrisch und transitiv ist. Für beliebiges $a \in R$ gilt offenbar $a - a = 0 = c \cdot 0$, sodass $a \equiv a \bmod(c)$. Seien nun $a, b \in R$ mit der Eigenschaft, dass $a \equiv b \bmod(c)$. Dann gilt $a-b = c \cdot d \Leftrightarrow b-a = -(a-b) = -(c \cdot d) = c \cdot (-d)$. Da auch $-d \in R$ für $d \in R$ folgt $b \equiv a \bmod(a)$. Mithin ist die vorliegende Relation symmetrisch. Seien nun $a_1, a_2, a_3 \in R$, sodass gilt $a_1 \equiv a_2 \bmod(c)$ und $a_2 \equiv a_3 \bmod(c)$. Dann gibt es $d_{12}, d_{23} \in R$, sodass $a_1 - a_2 = cd_{12}$ und $a_2 - a_3 = cd_{23}$. Addition der beiden Gleichungen und Anwendung des Distributivgesetzes liefert $a_1 - a_3 = c(d_{12} + d_{23})$. Wegen $d_{12} + d_{23} \in R$, wenn $d_{12}, d_{23} \in R$, gilt $a_1 \equiv a_3 \bmod(c)$. Damit ist die Transitivität der Relation nachgewiesen. Insgesamt ist die angegebene Relation eine Äquivalenzrelation.
(b) Sei nun $R = \mathbb{Z}$. Zu bestimmen sind alle Lösungen der Kongruenz $51y \equiv 34 \bmod(85)$. Da $17 \cdot 5 = 85$, $2 \cdot 17 = 34$ und $3 \cdot 17 = 51$ liefert uns die Kürzungsregel für lineare Kongruenzen, dass die angegebene Gleichung zu $3y \equiv 2 \bmod(5)$ äquivalent

ist. Da 5 eine Primzahl ist, gilt $3 \in (\mathbb{Z}/5\mathbb{Z})^\times$ und genauer $3^{-1} = 2$. Damit finden wir $y \equiv 4 \bmod(5)$. In $\mathbb{Z}$ kommen also $y \in \{4+5k | k \in \mathbb{Z}\}$ als Lösungen der Kongruenz in Frage. Tatsächlich ist für beliebiges $k \in \mathbb{Z}$ $51 \cdot (4+5k) \equiv 17 \cdot 3 \cdot 4 \equiv 17 \cdot 2 \equiv 34 \bmod(85)$.
(c) Sei nun $R = \mathbb{Q}[x]$ und $f \in R$ erfülle $f \equiv 1 \bmod(x^2+1)$ und $f \equiv x \bmod(x^2+1)$. Da $0.5(x^2+1) - 0.5(x^2-1) = 1$ gilt $\mathrm{ggT}(x^2+1, x^2-1) = 1$, d.h., $x^2-1$ und $x^2+1$ sind in $R$ relativ prim. Wir schreiben also

$$f(x) = 1 + p(x)(x^2+1) = x + q(x)(x^2-1) \tag{153}$$

Umformen liefert $x - 1 = p(x)(x^2+1) - q(x)(x^2-1)$. Da $1 = 0.5(x^2+1) - 0.5(x^2-1)$, finden wir, dass $q(x) = 0.5(x-1) = p(x)$. Wegen $f(x) = x + q(x)(x^2-1) = 0.5x^3 - 0.5x^2 + 0.5x + 0.5$. Die Gesamtheit aller in Frage stehenden $f \in \mathbb{Q}[x]$ ist also gegeben durch $f \in 0.5x^3 - 0.5x^2 + 0.5x + 0.5 + (\mathrm{kgV}(x^2-1)(x^2+1)))$. Daraus folgt $f(x) = 0.5x^3 - 0.5x^2 + 0.5x + 0.5 + g(x) \cdot (x^4 - 1)$, wo $g(x) \in \mathbb{Q}[x]$.
(d) Sei nun $R = \mathbb{Z}$. Wir suchen alles Lösungen der Kongruenz $y^2 + 97y \equiv 3 \, 101$. Durch das Sieb des Erathostenes stellen wir fest, dass 101 eine Primzahl ist. In $\mathbb{Z}/101\mathbb{Z} = \mathbb{F}_{101}$ gilt $y^2 + 97y = 3 \Leftrightarrow y^2 - 4y - 3 = 0 \Leftrightarrow (y-2)^2 - 7 = 0 \Leftrightarrow (y-2)^2 \equiv 7 \bmod(101)$, wobei wir die Gleichung im letzten Schritt wieder in $\mathbb{Z}$ aufgefasst haben. Wir sehen also, dass die Gleichung genau dann Lösungen hat, wenn 7 ein Quadrat in $\mathbb{Z}/101\mathbb{Z}$ ist. Hierzu verwenden wir das Legendre-Symbol

$$\left(\frac{7}{101}\right) = -\left(\frac{101}{7}\right) = -\left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1. \tag{154}$$

Also ist 7 kein quadratischer Rest modulo 101, somit hat die Gleichung $(y-2)^2 \equiv 7 \bmod(101)$ keine Lösungen in $\mathbb{Z}$, also auch nicht die dazu äquivalente Ausgangsgleichung $y^2 + 97y \equiv 3 \bmod(101)$. □

**Aufgabe 107 (F19T1A4)** Sei $\alpha = \sqrt[3]{2+\sqrt{2}} \in \mathbb{R}$ und sei $\zeta = \exp(2\pi i/3)$ die primitive dritte Einheitswurzel.
(a) Zu finden ist das Minimalpolynom von $\alpha$ über $\mathbb{Q}$. Es gilt

$$\begin{aligned} \alpha &= \sqrt[3]{2+\sqrt{2}} \\ \Rightarrow \alpha^3 &= 2 + \sqrt{2} \\ \Rightarrow (\alpha^3 - 2) &= \sqrt{2} \\ \Rightarrow (\alpha^3 - 2)^2 &= 2 \\ \Rightarrow \alpha^6 - 4\alpha^3 + 2 &= 0. \end{aligned} \tag{155}$$

Definiere nun das Polynom $p(x) \equiv x^6 - 4x^3 + 2 \in \mathbb{Q}[x]$. Offenbar ist $p$ ein Polynom mit ganzzahligen Koeffizienten, dessen Leitkoeffizient 1 ist. Also gilt $p \in \mathbb{Z}[x]$ und $p$ ist normiert. Dann ist $p$ nach dem Eisenstein-Kriterium zur Primzahl 2 irreduzibel über $\mathbb{Z}$, nach dem Lemma von Gauss also ebenfalls irreduzibel über dem Quotientenkörper $\mathbb{Q} = \mathrm{Quot}(\mathbb{Z})$. Schließlich ist per Konstruktion $p(\alpha) = 0$. Als normiertes, irreduzibles Polynom in $\mathbb{Q}[x]$, das $\alpha$ als Nullstelle besitzt, gilt also $p = \mu_{\mathbb{Q},\alpha}$, d.h., $p$ ist das Minimalpolynom von $\alpha$ über $\mathbb{Q}$.

(b) Wir bestimmen nun die Nullstellen von $p$ in $\mathbb{Q}^{\text{alg}} \subseteq \mathbb{C}$, dem algebraischen Abschluss von $\mathbb{Q}$ in $\mathbb{C}$. Da $\deg(p) = 6$, erwarten wir sechs Nullstellen (mit Vielfachheiten gezählt). Es gilt in der Tat,

$$\begin{aligned} 0 &= x^6 - 4x^3 + 2 \\ \Rightarrow 2 &= (x^3 - 2)^2 \\ \Rightarrow \pm\sqrt{2} &= x^3 - 2 \\ \Rightarrow 2 \pm \sqrt{2} &= x^3 \\ \Rightarrow \sqrt[3]{2 \pm \sqrt{2}}\zeta^k &= x = x_{\pm,k}, \end{aligned} \tag{156}$$

wobei $\zeta = \exp(2\pi i/3)$ die oben angegebene primitive dritte Einheitswurzel ist und $k \in \{0, 1, 2\}$. Insgesamt gibt es also sechs verschiedene Nullstellen von $p$ in $\mathbb{Q}^{\text{alg}}$. Wir bezeichnen die entsprechende Nullstellenmenge von $p$ mit $N$. Zu zeigen ist nun noch $\mathbb{Q}(N) = \mathbb{Q}(\alpha, \beta, \zeta)$, wobei $\beta = \sqrt[3]{2 + \sqrt{2}}$. Hierzu beachten wir, dass $0 \neq \alpha = x_{+,0} \in N$ und $\beta = x_{-,0} \in N$ sowie $\zeta = x_{+,1}/x_{+,0} \in \mathbb{Q}(N)$. Wegen $\mathbb{Q} \subseteq \mathbb{Q}(N)$ gilt zusammen mit $\{\alpha, \beta, \zeta\} \subseteq \mathbb{Q}(N)$ auch automatisch $Q(\alpha, \beta, \zeta) \subseteq \mathbb{Q}(N)$. Umgekehrt lässt sich jedes Element aus $N$ schreiben als entweder $\zeta^k \cdot \alpha$ oder $\zeta^k \cdot \beta$, je nachdem ob eine Summe oder eine Differenz im äußeren Radikanden zu finden ist. Hierbei gilt $k \in \{0, 1, 2\}$, denn $\zeta^3 = 1$ für $\zeta$ als dritte Einheitswurzel. Insgesamt gilt also $\mathbb{Q} \subseteq \mathbb{Q}(\alpha, \beta, \zeta)$ und nach den vorangegangenen Überlegungen $N \subseteq \mathbb{Q}(\alpha, \beta, \gamma)$. Damit ist $\mathbb{Q}(\alpha, \beta, \zeta) \supseteq \mathbb{Q}(N)$. Insgesamt haben wir also die Gleichheit $\mathbb{Q}(N) = \mathbb{Q}(\alpha, \beta, \zeta)$ etabliert. Da $\mathbb{Q}(N) = \text{Zerf}(p, \mathbb{Q})$ bereits nach Definition, haben wir bewiesen, dass $\mathbb{Q}(\alpha, \beta, \zeta)$ der Zerfällungskörper von $p = \mu_{\mathbb{Q},\alpha}$ über $\mathbb{Q}$ ist. Wir bezeichnen $L = \mathbb{Q}(\alpha, \beta, \zeta)$ im Folgenden.
(c) Wir zeigen nun, dass $\text{Gal}(L|\mathbb{Q}) =: G$ einen Normalteiler $N$ vom Index 6 besitzt. Laut dem Hauptsatz der Galoistheorie stehen die Normalteiler der Galoisgruppe $G$ vermöge einer antitonischen Bijektion in Korrespondenz zu den normalen Zwischenkörpern der Galoiserweiterung $L|\mathbb{Q}$. In der Tat handelt es sich bei $L|\mathbb{Q}$, denn $\mathbb{Q}$ ist als von endlich vielen über $\mathbb{Q}$ algebraischen Elementen eine endliche und damit endlich-algebraische Erweiterung von $\mathbb{Q}$. Da $\mathbb{Q}$, aufgefasst als Ring, Charakteristik 0 hat, ist $L|\mathbb{Q}$ separabel. Nach Teil (b) ist $L$ ferner der Zerfällungskörper von $\mu_{\mathbb{Q},\alpha} \in \mathbb{Q}[x]$. Laut Vorlesung ist demnach $L|\mathbb{Q}$ normal. Definitionsgemäß ist $L|\mathbb{Q}$ als normale und separable Körpererweiterung eine Galois-Erweiterung. Damit haben wir sicher gestellt, dass das Problem korrekt gestellt ist. Wir zeigen in einem ersten Schritt, dass $\sqrt[3]{2} \in L$. Hierzu beachten wir, dass

$$\alpha \cdot \beta = \sqrt[3]{2 + \sqrt{2}} \cdot \sqrt[3]{2 - \sqrt{2}} = \sqrt[3]{\left(2 + \sqrt{2}\right)\left(2 - \sqrt{2}\right)} = \sqrt[3]{4 - 2} = \sqrt[3]{2}. \tag{157}$$

Wegen $\alpha, \beta \in L$ folgt wegen der Abgeschlossenheit des Körpers $L$ unter der Multiplikation $\alpha \cdot \beta = \sqrt[3]{2} \in L$. Wir versuchen nun einen echten Zwischenkörper $M$ zu konstruieren, sodass $\mathbb{Q} \subsetneq M \subsetneq L$. Dies erreichen wir, wenn wir $q(x) = x^3 - 2 \in \mathbb{Q}[x]$ betrachten. Nach Eisenstein zur Primzahl 2 ist das Polynom $q$, mit ganzzahligen Koeffizienten, in $\mathbb{Z}[x]$ irreduzibel, und somit nach dem Lemma von Gauss auch im Polynomring $\mathbb{Q}[x]$ über $\mathbb{Q} = \text{Quot}(\mathbb{Z})$. Da $q$ normiert ist und $q(\sqrt[3]{2}) = 0$ ist $q$ offenbar das Minimalpolynom von $\sqrt[3]{2}$ über $\mathbb{Q}$. Damit ist $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = \deg(q) = 3$.

Die Nullstellen von $q$ sind $\sqrt[3]{2}\zeta^k$ mit $k \in \{0,1,2\}$. Offenbar ist $M \equiv \mathrm{Zerf}(q|\mathbb{Q}) \equiv \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\zeta, \sqrt[3]{2}\zeta^2) = \mathbb{Q}(\zeta, \sqrt[3]{2})$. Nun gilt $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg(x^2 + x + 1) = 2$ und $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, also $2|[M : \mathbb{Q}]$, $3|[M : \mathbb{Q}]$. Nach der Gradformel gilt $[M : \mathbb{Q}] \leq [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] \cdot [\mathbb{Q}(\zeta) : \mathbb{Q}] = 6$. Da 2 und 3 relativ prim sind, folgt $[M : \mathbb{Q}] = 6$. Definiere nun $U = \mathrm{Gal}(L|M)$. Dann gilt $(G : U) = [M : \mathbb{Q}] = 6$ nach der Ergänzung zum Hauptsatz der Galoistheorie aus der Vorlesung und ferner $U \trianglelefteq G$, weil $M$ als Zerfällungskörper von $q \in \mathbb{Q}[x]$ eine normale Körpererweiterung über $\mathbb{Q}$ ist. $\square$

**Aufgabe 108 (F19T1A5)** Sei $f \in \mathbb{C}[z]$. $f'$ bezeichne die Ableitung von $f$ und $\deg(f)$ den Grad von $f$. Ferner sei $n_0(f) \in \mathbb{N}_0$ die Anzahl der Nullstellen von $f$, gezählt *ohne* Vielfachheiten. Zu zeigen ist, dass für $f \neq 0$ gilt

$$\deg(f) = \deg(\mathrm{ggT}(f, f')) + n_0(f). \tag{158}$$

Falls $\deg(f) = 0$, dann ist $f$ konstant und es gilt $f' = 0$. Da dann $\mathrm{ggT}(f, f') = 0$ und $n_0(f) = 0$ wegen $f \neq 0$ konstant, haben wir die angegebene Gleichung im Falle $\deg(f) = 0$ für nicht-verschwindendes $f$ bestätigt. Sei also $f \in \mathbb{C}[z]$ vom Grad $N \geq 1$. Dann ist

$$f(z) = \sum_{k=0}^{N} a_k z^k, \tag{159}$$

wobei wir ohne Einschränkung $a_N = 1$ annehmen können. Laut dem Fundamentalsatz der Algebra und der algebraischen Abgeschlossenheit von $\mathbb{C}$ erlaubt $f$ eine Darstellung der Form

$$f(z) = \prod_{k=1}^{|Z|=n_0(f)} (z - z_k)^{n(z_k)}, \tag{160}$$

wobei $Z$ die Nullstellenmenge von $f$ in $\mathbb{C}$ ist und $n(z_k) \in \mathbb{N}$ die Vielfachheit der einzelnen Nullstellen $z_k \in Z$ zählt, sodass $n(z_1) + ... + n(z_{|Z|}) = N = \deg(f)$. Sukzessives Anwenden der Leibniz-Eigenschaft der Ableitung liefert

$$f'(z) = \sum_{k=1}^{n_0(f)} n(z_k)(z - z_k)^{n(z_k)-1} \prod_{l=1,\, k\neq l}^{n_0(f)} (z - z_l)^{n(z_l)}. \tag{161}$$

Da gerade die Polynome vom Grad 1 die irreduziblen Elemente aus $\mathbb{C}[z]$ sind und $\mathbb{C}[z]$ als univariater Polynomring über dem Körper $\mathbb{C}$ faktoriell ist, sehen wir, dass

$$\mathrm{ggT}(f, f')(z) = \prod_{k=1}^{n_0(f)} (z - z_k)^{n(z_k)-1}. \tag{162}$$

Nun gilt offensichtlich

$$\deg(\mathrm{ggT}(f, f')) = \sum_{k=1}^{n_0(f)} (n(z_k) - 1) = \sum_{k=1}^{n_0(f)} n(z_k) - n_0(f) = N - n_0(f). \tag{163}$$

Wegen $N = \deg(f)$ können wir die letzte Gleichung so umformen, dass die Behauptung

$$\deg(f) = \deg(\mathrm{ggT}(f, f')) + n_0(f) \tag{164}$$

reproduziert wird. □

**Aufgabe 109 (F09T2A4)** Gegeben sei $K = \mathbb{Q}(\sqrt[5]{3}, \sqrt{7})$.
(a) Zu zeigen ist, dass $K = \mathbb{Q}(\alpha)$, wobei $\alpha = \sqrt[5]{3} \cdot \sqrt{7}$. Um die Gleichheit zu zeigen, überprüfen wir zunächst $\mathbb{Q} \cup \{\sqrt[5]{3}, \sqrt{7}\} \subseteq \mathbb{Q}(\sqrt[5]{3}\sqrt{7})$. Es gilt $\sqrt[5]{3} = (7^3 \cdot 3)^{-1} \cdot (\sqrt[5]{3}\sqrt{7})^6 \in K$ und $\sqrt{7} = (49 \cdot 3)^{-1} \cdot (\sqrt[5]{3}\sqrt{7})^5$. Somit gilt $\{\sqrt[5]{3}, \sqrt{7}\} \subseteq \mathbb{Q}(\alpha)$. Hierbei ist klar, dass $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$. Umgekehrt zeigen wir, dass $\mathbb{Q} \cup \{\sqrt[5]{3}\sqrt{7}\} \subseteq K$. Wiederum ist $\mathbb{Q} \subseteq K$ klar. Wegen $\sqrt[5]{3}, \sqrt{7} \in K$ ist auch $\sqrt[5]{3}\sqrt{7} = \alpha \in K$. Damit ist $\mathbb{Q} \cup \{\sqrt[5]{3}\sqrt{7}\} \subseteq K$. Laut Vorlesung ist mit dem Nachweis der beiden Inklusionen bereits $K = \mathbb{Q}(\alpha)$ gezeigt.
(b) Wir bestimmen nun den Grad der Körpererweiterung $K|\mathbb{Q}$. Zunächst stellen wir fest, dass $\mathbb{Q}(\sqrt[5]{3})$ und $\mathbb{Q}(\sqrt{7})$ Zwischenkörper der Erweiterung sind. Da $p = x^5 - 3 \in \mathbb{Q}[x]$ normiert, nach Eisenstein zur Primzahl $p = 3$ irreduzibel ist und $p(\sqrt[5]{3}) = 0$ gilt, ist $p$ das Minimalpolynom von $\sqrt[5]{3}$ über $\mathbb{Q}$ ist. Analog ist $q = x^2 - 7 \in \mathbb{Q}[x]$ normiert, nach Eisenstein zu $p = 7$ irreduzibel und es gilt $q(\sqrt{7}) = 0$, sodass $q$ das Minimalpolynom von $\sqrt{7}$ über $\mathbb{Q}$ ist. Laut Vorlesung ist der Grad des Minimalpolynoms $p$ bzw. $q$ dann gleich dem Grad der Körpererweiterung, d.h., $[\mathbb{Q}(\sqrt[5]{3}) : \mathbb{Q}] = 5$ und $[\mathbb{Q}(\sqrt{7}) : \mathbb{Q}] = 2$. Offenbar sind 2 und 5 relativ prim zueinander, und es gilt $\mathrm{ggT}(5, 2) = 10 | [K : \mathbb{Q}]$. Wegen $[\mathbb{Q}(\sqrt[3]{5}, \sqrt{7}) : \mathbb{Q}(\sqrt{7})] \leq [\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = 5$, folgt $[K : \mathbb{Q}] = 10$.
(c) Wir bestimmen nun das Minimalpolynom von $\alpha$ über $\mathbb{Q}$. Wir bezeichnen dieses mit $\mu$. Aus Teil (b) ist bekannt, dass $K|\mathbb{Q}$ eine Körpererweiterung vom Grad 10 ist, somit endlich.Für $\alpha \in K$ existiert somit ein (eindeutiges) Minimalpolynom $\mu \in \mathbb{Q}[x]$, das darüber hinaus normiert ist und Grad 10 hat. Dieses bestimmen wir also zu $\mu = x^{10} - 7^5 \cdot 3^2$. Denn erstens hat $\mu$ bereits den Grad des Minimalpolynoms, ist in diesem Sinne also minimal, zweitens gilt $\mu(\alpha) = 0$ und drittens ist $\mu$ normiert. Zusammen mit einem Vorlesungsresultat folgt daraus bereits, dass $\mu$ tatsächlich das Minimalpolynom ist, denn andernfalls gäbe es ein Polynom von echt kleinerem Grad als 10 das Minimalpolynom von $\alpha$ über $\mathbb{Q}$ ist. Letzteres widerspräche allerdings der Tatsache, dass $\deg(\mu_{\mathbb{Q},\alpha}) = [K : \mathbb{Q}] = 10$. □

**Aufgabe 110 (F17T2A4)** Sei $f = x^3 + 2x + 2 \in \mathbb{Q}[x]$ und $\alpha$ eine Nullstelle von $f$.
(a) Zu zeigen ist zunächst, dass $\{1, \alpha, \alpha^2\}$ eine Basis von $\mathbb{Q}(\alpha)$ ist. Zunächst ist $f$ als Polynom mit integralen Koeffizienten nach dem Eisensteinkriterium zu $p = 2$ irreduzibel über $\mathbb{Z}$, nach dem Lemma von Gauß also auch über $\mathbb{Q}$. Damit hat $f$ keine rationalen Nullstellen und es gilt $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Als normiertes, irreduzibles Polynom, welches $\alpha$ als Nullstelle besitzt, ist $f$ das Minimalpolynom von $f$ über $\alpha$. Damit hat $\mathbb{Q}(\alpha)$ als $\mathbb{Q}$-Vektorraum die Dimension 3, somit und wegen linearer Unabhängigkeit von $\{1, \alpha, \alpha^2\}$ über $\mathbb{Q}$ die Basis $\{1, \alpha, \alpha^2\}$.
(b) Wir sollen $(1 + \alpha)^{-1}$ in der Basis $\{1, \alpha, \alpha^2\}$ schreiben. Hierzu verwenden wir, dass $1 + \alpha \in (\mathbb{Q}(\alpha))^\times$, denn $\mathbb{Q} \not\ni \alpha \neq -1 \in \mathbb{Q}$. Somit ist $1 = (1 + \alpha)(1 + \alpha)^{-1}$ und

die Expansion $(1+\alpha)^{-1} = a + b\alpha + c\alpha^2$ liefert $1 = a + (a+b)\alpha + (b+c)\alpha^2 + c\alpha^3 = a - 2c + (a+b-2c)\alpha + (b+c)\alpha^2$. Koeffizientenvergleich unter Ausnutzung der linearen Unabhängigkeit der Menge $\{1, \alpha, \alpha^2\}$ über $\mathbb{Q}$ liefert das $3 \times 3$-Gleichungssystem $1 = a - 2c$, $0 = a - 2c + b$, $0 = b + c$, aus dem wir $b = -1$, $c = 1$, $a = 3$ folgern. Somit gilt

$$(1+\alpha)^{-1} = 3 - \alpha + \alpha^2. \tag{165}$$

Damit ist gesuchte Zerlegung gefunden. □

**Aufgabe 111 (H17T2A3)** Gegeben seien die Polynome $f = x^7 - x - 1 \in \mathbb{Q}[x]$ und $p = x^7 + x + 1 \in \mathbb{F}_2[x]$.
(a) Wir zeigen, dass $p$ keine Nullstellen in $\mathbb{F}_2$, in $\mathbb{F}_4$ und in $\mathbb{F}_8$ hat. Zunächst sehen wir durch Einsetzen, dass $p(0) = 1$ und $p(1) = 1$ in $\mathbb{F}_2$ gilt. Also hat $p$ keine Nullstellen in $\mathbb{F}_2$. Da $f(0) = 1$ auch in $\mathbb{F}_4$ gilt, müsste eine Nullstelle von $f$ in $\mathbb{F}_4$ in der multiplikativen Gruppe $(\mathbb{F}_4)^\times$ liegen. Aus der Vorlesung ist bekannt, dass $\mathbb{F}_4^\times \simeq \mathbb{Z}/3\mathbb{Z}$, sodass jedes $\chi \in \mathbb{F}_4^\times$ die Ordnung 3 hat. Damit ist $\chi^7 = \chi$ und somit müsste $0 = p(\chi) = 2\chi + 1 = 1 \neq 0$, da $\mathrm{char}(\mathbb{F}_4) = 2$. Somit hat $p$ auch in $\mathbb{F}_4$ keine Nullstellen. Zuletzt behandeln wir den Fall, ob $p$ in $\mathbb{F}_8$ eine Nullstelle hat. Analog zu oben, muss $\chi \in \mathbb{F}_8^\times \simeq \mathbb{Z}/7\mathbb{Z}$ für eine potentielle Nullstelle $\chi$ von $p$ gelten, wobei die Isomorphie wiederum aus der Vorlesung bekannt ist. Da $\chi$ Ordnung 7 in $\mathbb{F}_8^\times$ hat, folgt $\chi^7 = 1$ und somit $p(\chi) = \chi^7 + \chi + 1 = 2 + \chi = \chi = 0$, denn $\mathrm{char}(\mathbb{F}_8) = 2$ und $\chi$ ist Nullstelle nach Annahme. Letzteres ist aber ein Widerspruch zu $\mathbb{F}_8^\times \ni \chi \neq 0$. Somit haben wir gezeigt, dass $p$ keine Nullstellen in aller drei genannten Körpern hat.
(b) Wir zeigen als nächstes, dass $p$ in $\mathbb{F}_2[x]$ irreduzibel ist. Offenbar ist $p$ eine Nicht-Einheit. Angenommen, $p$ wäre reduzibel. Da $p$ keine Nullstellen in $\mathbb{F}_2$ hat und $\mathbb{F}_2[x]$ als univariater Polynomring über dem Körper $\mathbb{F}_2$ ein Hauptidealring und somit ein faktorieller Ring ist, erlaubt $p$ einer Faktorisierung der Form $p = p_1 \cdot \cdots \cdot p_r$, wo $r \geq 2$, bestehend aus irreduziblen Polynomen. Da $p$ keine Nullstelle in $\mathbb{F}_2$ hat gilt für jeden der Faktoren $\deg(p_i) \geq 2$. Einer der Faktoren hat ferner sogar $\deg(p_i) \in \{3, 5\}$. Insbesondere gibt es also einen irreduziblen Faktor $q$ vom Grad 2. Sei nun $\mathbb{F}_2^{\mathrm{alg}}$ der algebraische Abschluss von $\mathbb{F}_2$. Dann zerfällt $p$ über $\mathbb{F}_2^{\mathrm{alg}}$ in Linearfaktoren. Insbesondere erzeugen die Nullstellen des Faktors $q$ über $\mathbb{F}_2$ einen Vektorraum der Dimension 2, $\mathbb{F}_2^2 \simeq \mathbb{F}_4$, wobei die Isomorphie aufgrund des Existenz- und Eindeutigkeitssatzes für endliche Körper gilt. Damit hätte aber $f$ bereits in $\mathbb{F}_4$ mindestens eine Nullstelle, im Widerspruch zu dem Ergebnis von Teil (a), demzufolge $f$ keine Nullstelle in $\mathbb{F}_4$ hat. Somit war die Annahme, $p$ wäre reduzibel, falsch. Als Nicht-Einheit in $\mathbb{F}_2[x]$ ist $p$ daher irreduzibel.
(c) Wir zeigen nun, dass $f$ in $\mathbb{Q}[x]$ irreduzibel ist. Als normiertes Polynom mit ganzzahligen Koeffizienten ist $f$ offenbar primitiv. Zudem ist $p$ unter der Reduktionsabbildung $\mod(2) : \mathbb{Z}[x] \to \mathbb{F}_2[x]$ das Bild von $f$. Da $p$ nach Teil (b) irreduzibel in $\mathbb{F}_2[x]$ ist, liefert das Reduktionskriterium die Irreduzibilität von $f$ über $\mathbb{Z}$. Nach dem Lemma von Gauss ist also $f$ irreduzibel über $\mathbb{Q}$, was zu zeigen war. □

**Aufgabe 112 (H00T1A3)** Sei $K = \mathbb{F}_{2^{2000}}$.
(a) Zu bestimmen ist die Anzahl der Teilkörper von $K$. Es gilt $2000 = 20 \cdot 100 = 2^4 \cdot 5^3$.

Aus der Vorlesung ist bekannt, dass ein endlicher Körper $\mathbb{F}_{p^k}$ mit einer Primzahl $p$ und einer natürlichen Zahl $k$ genau die Teilkörper der Form $\mathbb{F}_{p^l}$ hat, wo $l|k$. Die Teiler von 2000 sind nun gerade die Zahlen in$\{1, 2, 2^2, 2^3, 2^4, 5, 2 \cdot 5, 2^2 \cdot 5, 2^3 \cdot 5, 2^4 \cdot 5, 5^2, 5^2 \cdot 2, 5^2 \cdot 2^2, 5^2 \cdot 2^3, 5^2 \cdot 2^4, 5^3, 5^3 \cdot 2, 5^3 \cdot 2^2, 5^3 \cdot 2^3, 5^3 \cdot 2^4\}$. Insgesamt gibt es also 20 verschiedene Teiler von 2000 und somit, aufgrund der Existenz und Eindeutigkeit der endlichen Körper, 20 verschiedene Teilkörper von $\mathbb{F}_{2^{2000}}$.
(b) Wir bestimmen nun die Anzahl der erzeugenden Elemente der Erweiterung $K|\mathbb{F}_2$. Damit $\alpha \in K$ ein erzeugendes Element von $K$ ist, also $K = \mathbb{F}_2(\alpha)$ ist es erforderlich, dass $\deg \mu_{\mathbb{F}_2,\alpha} = [K : \mathbb{F}_2] = 2000$. Mit anderen Worten ist ein Element $\alpha \in K$ gesucht, das in keinem der Zwischenkörper $M$ von $K|\mathbb{F}_2$ liegt, die $M \neq K$ erfüllen. Somit kommen

$$N = \left|\mathbb{F}_{2^{2000}} \setminus \left(\mathbb{F}_{2^{2^4 \cdot 5^2}} \cup \mathbb{F}_{2^{2^3 \cdot 5^3}}\right)\right| \tag{166}$$

Elemente in Betracht. Hierbei haben wir wegen $\mathbb{F}_{2^k} \subseteq \mathbb{F}_{2^l}$ lediglich die größten zueinander teilerfremden Teiler von 2000 betrachten müssen, denn im Sinne der Mächtigkeit als Menge sind die Zwischenkörper von $K$ in $\mathbb{F}_{2^{2^4 \cdot 5^2}}$ oder $\mathbb{F}_{2^{2^3 \cdot 5^3}}$ enthalten. Bekannt ist für zwei endliche Mengen $A, B$, dass $|A \cup B| = |A| + |B| - |A \cap B|$. Umformung dieser Gleichung liefert

$$\begin{aligned} N &= |\mathbb{F}_{2^{2000}}| - |\mathbb{F}_{2^{2^4 \cdot 5^2}} \cup \mathbb{F}_{2^{2^3 \cdot 5^3}}| \\ &= |\mathbb{F}_{2^{2000}}| - |\mathbb{F}_{2^{2^4 \cdot 5^2}}| - |\mathbb{F}_{2^{2^3 \cdot 5^3}}| + |\mathbb{F}_{2^{2^4 \cdot 5^2}} \cap \mathbb{F}_{2^{2^3 \cdot 5^3}}| \\ &= 2^{2000} - 2^{400} - 2^{1000} + 2^{200}, \end{aligned} \tag{167}$$

denn $\mathbb{F}_{2^{2^4 \cdot 5^2}} \cap \mathbb{F}_{2^{2^3 \cdot 5^3}} \simeq \mathbb{F}_{2^{2^3 \cdot 5^2}} = \mathbb{F}_{2^{200}}$. □

**Aufgabe 113 (F17T3A5)** Sei $K$ ein endlicher Körper mit $q$ Elementen und sei $f = x^2 + x + 1 \in K[x]$. Wir zeigen, dass $f$ genau dann irreduzibel ist, wenn $q \equiv -1 \bmod(3)$. Den Beweis führen wir durch Kontraposition. Angenommen, $q \not\equiv -1 \bmod(3)$. Dann ist $q \equiv 0 \bmod(3)$ oder $q \equiv 1 \bmod(3)$. Im ersten Fall ist $K$ ein endlicher Körper der Charakteristik 3. Dann gilt $f(1) = 1 + 1 + 1 = 3 = 0$ und $f$ hat eine Nullstelle in $K$, denn $1 \in K$. Damit ist $f$ in diesem Fall bereits reduzibel. Falls $q \equiv 1 \bmod(3)$, dann gilt $q = 3 \cdot l + 1$ und $|K^\times| = 3l$ wobei $l \in \mathbb{N}$. Da $K^\times$ als Einheitengruppe eines endlichen Körpers eine zyklische Gruppe ist, gibt es ein Element $\alpha \in K^\times$, das die Ordnung 3 hat. Es gilt dann $0 = \alpha^3 - 1 = (\alpha - 1)(\alpha^2 + \alpha + 1)$. Zudem ist $\alpha = 1$ nicht möglich, denn dann hätte $\alpha$ die Ordnung $1 < 3$ im Widerspruch zur Minimalität der Ordnung 3 von $\alpha$. Somit gilt $\alpha^2 + \alpha + 1 = 0$ und $f$ hat mit $\alpha$ bereits eine Nullstelle in $K^\times \subseteq K$, ist also als Polynom vom Grad 2 reduzibel. Sei umgekehrt vorausgesetzt, dass $f$ nicht irreduzibel ist. Als Polynom vom Grad 2 ist $f$ eine Nicht-Einheit, somit also reduzibel. Folglich gibt es ein $\alpha \in K$, sodass $f(\alpha) = 0$. Da $f(0) = 1 \neq 0$ gilt sogar $\alpha \in K^\times$. Wegen $(\alpha + 1)f(\alpha) = 0$, d.h., $\alpha^3 = 1$ ist $\alpha$, das höchstens die Ordnung 3 hat. Falls $\alpha = 1$ kann $f(\alpha = 1) = 0$ nur gelten, wenn $3 \equiv 0$, d.h., $\mathrm{char}(K) = 3$ und somit $q \equiv 0 \bmod(3)$. Falls andererseits $\alpha \neq 1$, so ist $\alpha$ ein Element der Ordnung 3 in der Einheitengruppe $K^\times$. Diese hat Ordnung $|K^\times| = q - 1$ und ist die Forderung, dass $K^\times$ ein Element der Ordnung 3 enthält, bedeutet $3|q - 1$ und, mit anderen Worten, $q \equiv 1 \bmod(3)$. Damit sind beide Richtungen nachgewiesen. □

**Aufgabe 114 (H05T1A4)** Sei $L \subseteq \mathbb{C}$ der Zerfällungskörper von $f = X^7+1-i \in \mathbb{Q}(i)[X]$. Ferner sei für eine natürliche Zahl $n$ $\zeta_n = \exp(2\pi i/n)$.
(a) Wir zeigen zunächst, dass $\mathbb{Q}(\zeta_7, i) = \mathbb{Q}(\zeta_{28})$. Hierzu reicht es Vorlesung aus, zu zeigen, dass $\zeta_7, i \in \mathbb{Q}(\zeta_{28})$ und $\zeta_{28} \in \mathbb{Q}(\zeta_7, i)$. Zunächst gilt $i = \exp(2\pi i/4)$, $\zeta_7 = \exp(2\pi i/7)$ und $\zeta_{28} = \exp(2\pi i/(28))$. Somit $i = \exp(2\pi i/4) = \exp(2\pi i/28)^7$ und $\exp(2\pi i/7) = \exp(2\pi i/28)^4$. Somit ist $i, \zeta_7 \in \mathbb{Q}(\zeta_{28})$. Umgekehrt gilt $i^3 \cdot \zeta_7^{-5} = \exp(2\pi i \cdot 21/28)\exp(-2\pi i 20/28) = \exp(2\pi i/28) = \zeta_{28}$, sodass auch $\zeta_{28} \in \mathbb{Q}(i, \zeta_7)$. Damit ist die Gleichheit $\mathbb{Q}(i, \zeta_7) = \mathbb{Q}(\zeta_{28})$ nachgewiesen. Nun zeigen wir noch, dass $[\mathbb{Q}(\zeta_7, i) : \mathbb{Q}(i)] = 6$. Hierzu stellen wir zunächst fest, dass nach dem soeben Bewiesenen $[\mathbb{Q}(\zeta_{28}) : \mathbb{Q}(i)] = [\mathbb{Q}(\zeta_7, i) : \mathbb{Q}(i)]$. Bekanntermaßen ist $\zeta_{28}$ eine Nullstelle des 28-Kreisteilungspolynoms $\Phi_{28} \in \mathbb{Q}[x]$, wobei $\Phi_{28}$ sogar das Minimalpolynom von $\zeta_{28}$ über $\mathbb{Q}$ ist. Laut Vorlesung ist $\deg(\Phi_{28}) = \Phi(4 \cdot 7) = 2 \cdot 6 = 12$, wobei wir die wohlbekannten Eigenschaften der Euler'schen $\Phi$-Funktion verwendet haben. Zudem gilt $[\mathbb{Q}(i) : \mathbb{Q}] = \deg(\mu_{\mathbb{Q},i}) = \deg(x^2 + 1) = 2$, wobei $x^2 + 1$ in $\mathbb{Q}$ nach dem Lemma von Gauss und dem Reduktionskriterium zu $p = 3$ irreduzibel ist und als normiertes Polynom $i$ als Nullstelle hat, also dessen Minimalpolynom ist. Da ferner $\mathbb{Q}(i)$ ein Zwischenkörper von $\mathbb{Q}(\zeta_{28})|\mathbb{Q}$ ist, liefert die Gradformel für die involvierten endlichen Körpererweiterungen $[\mathbb{Q}(\zeta_{28}) : \mathbb{Q}(i)] = [\mathbb{Q}(\zeta_{28}) : \mathbb{Q}]/[\mathbb{Q}(i) : \mathbb{Q}] = 12/2 = 6$.
(b) Nun zeigen wir $[L : \mathbb{Q}(i)] = 42$. Wir stellen zunächst fest, dass $-\sqrt[7]{1+i} = -\sqrt[7]{2}\exp(2\pi i/28) \in L$. Nun ist $-\sqrt[7]{2}$ eine reelle, irrationale Zahl, die das Minimalpolynom $x^7 + 2$ über $\mathbb{Q}$ hat. Denn das angegebene Polynom hat offenbar $-\sqrt[7]{2}$ als Nullstelle, ist nach Eisenstein zu $p = 2$ irreduzibel und normiert. Wir stellen zudem fest, dass $L = \mathbb{Q}(\zeta_{28}, \sqrt[7]{2})$, denn die Nullstellen von $f$ sind gerade $-\sqrt[7]{1+i}\zeta_7^k$, wo $0 \leq k \leq 6$. Damit sehen wir, direkt aus der weiter oben angegebene Darstellung einer der Nullstellen von $f$, dass $L \subseteq \mathbb{Q}(\zeta_{28}, \sqrt[7]{2})$. Andererseits ist auch $\zeta_7 = -\sqrt[7]{1+i}\zeta_7/(-\sqrt[7]{1+i}) \in L$. Zudem ist $L \ni -2/(-\sqrt[7]{2}\exp(2\pi i/28))^7 = \exp(2\pi i/4) = i \in L$. Damit ist auch $\zeta_{28} = i^3\zeta_7^{-5} \in L$. Somit ist $-(-\sqrt[7]{1+i})/\zeta_{28} = \sqrt[7]{2} \in L$, also $\mathbb{Q}(\zeta_{28}, \sqrt[7]{2}) = L$, wie behauptet. Da zudem auch $\zeta_{28} \in L$ nicht-reell ist, gilt $[\mathbb{Q}(\zeta_{28}, \sqrt[7]{2}) : \mathbb{Q}(\sqrt[7]{2})] = [\mathbb{Q}(\zeta_{28}) : \mathbb{Q}] = 12$. Damit liefert die Gradformel zunächst $[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt[7]{2})][\mathbb{Q}(\sqrt[7]{2}) : \mathbb{Q}] = 12 \cdot 7$. Da $\mathbb{Q}(i)$ ein Zwischenkörper der endlichen Körpererweiterung $L|\mathbb{Q}$ ist, folgt $[L : \mathbb{Q}(i)] = [L : \mathbb{Q}]/[\mathbb{Q}(i) : \mathbb{Q}] = 12 \cdot 7/2 = 6 \cdot 7 = 42$. Damit haben wir bewiesen, dass $[L : \mathbb{Q}(i)] = 42$.
(c) Wir zeigen nun, dass $L$ unter der komplexen Konjugation abgeschlossen ist. Aus Teil (b) wissen wir bereits, dass $L = \mathbb{Q}(\sqrt[7]{2}, \zeta_{28})$. Da $\zeta_{28} = \exp(2\pi i/28)$ ist $\bar{\zeta}_{28} = \zeta_{28}^{-1} = \zeta_{28}^{27} \in L$. Da ferner $\sqrt[7]{2}$ reell und $\mathbb{Q} \subseteq \mathbb{R}$ sind, ist $\mathbb{Q}(\zeta_{28}, \sqrt[7]{2})$ bereits unter der komplexen Konjugation abgeschlossen.
(d) Wir zeigen nun, dass $L|\mathbb{Q}$ galoissch ist. Dazu stellen wir fest, dass $\mathbb{Q}$ ein Körper der Charakteristik 0 ist. Als endliche Erweiterung von $\mathbb{Q}$, ist $L|\mathbb{Q}$ algebraisch und aus Gründen der Charakteristik bereits separabel. Wir zeigen noch, dass $L$ separabel ist. Dazu stellen wir fest, dass wegen Teil (b) $L = \mathbb{Q}(\sqrt[7]{2}, \zeta_{28})$ der Körper $L$ bereits der Zerfällungskörper des Polynoms $P = (X^7 - 2)\Phi_{28}(X) \in \mathbb{Q}[X]$ ist. Laut Vorlesung ist $L|\mathbb{Q}$ damit bereits normal. Als normale und separable Körpererweiterung ist $L|\mathbb{Q}$ definitionsgemäß galoissch. □

**Aufgabe 115 (F19T2A5)** Sei $L|\mathbb{Q}$ eine endliche Galois-Erweiterung mit Galois-Gruppe $G \simeq S_3 \times H$, wobei $|H| = 88$.

(a) Zu zeigen ist, dass $\mathbb{Q}(\sqrt[5]{5}) \cap L = \mathbb{Q}$. Wir sehen, dass $P = x^5 - 5 \in \mathbb{Q}[x]$ ganzzahlig und normiert ist. Nach Eisenstein zur Primzahl $p = 5$, ist $P$ irreduzibel in $\mathbb{Z}[x]$, nach dem Lemma von Gauss also auch in $\mathbb{Q}[x]$. Zudem ist $P(\sqrt[5]{5}) = 0$. Damit ist $P$ das Minimalpolynom von $\sqrt[5]{5}$ über $\mathbb{Q}$. Da $\deg P = 5$ folgt $[\mathbb{Q}(\sqrt[5]{5}) : \mathbb{Q}] = 5$. Da $|G| = |S_3||H| = 6{\cdot}88$ haben wir $[L : \mathbb{Q}] = |G| = 6{\cdot}88$ nach einem Zusatz zum Hauptsatz der Galoistheorie. Klar ist, dass $\mathbb{Q} \subseteq L \cap \mathbb{Q}(\sqrt[5]{5})$ nach der Erweiterungskörpereigenschaft von $L$. Um auch die umgekehrte Inklusion zu sehen, nehmen wir an, es gäbe einen echten Zwischenkörper $M$ von erstens $L|\mathbb{Q}$ und $\mathbb{Q}(\sqrt[5]{5})|\mathbb{Q}$. Nach der Gradformel gilt für den Erweiterungsgrad der Zwischenerweiterung $M|\mathbb{Q}$, dass $[M : \mathbb{Q}]|[L : \mathbb{Q}] = 6 \cdot 88$ und $[M : \mathbb{Q}]|[\mathbb{Q}(\sqrt[5]{5}) : \mathbb{Q}] = 5$. Damit ist $1 < [M : \mathbb{Q}] \leq \mathrm{ggT}(6 \cdot 88, 5) = 1$. Das ist ein offenkundiger Widerspruch, sodass die Annahme, es existierte ein echter Zwischenkörper $M$ für beide Erweiterungen von $\mathbb{Q}$, falsch war. Da der Schnitt $\mathbb{Q}(\sqrt[5]{5}) \cap L$ selbst ein Körper ist, folgt $\mathbb{Q}(\sqrt[5]{5}) \cap L = \mathbb{Q}$, wie behauptet. □ (b) Wir zeigen nun, dass es einen Zwischenkörper $M$ von $L|\mathbb{Q}$ gibt, sodass $[M : \mathbb{Q}] = 8$ und $M$ der Zerfällungskörper eines Polynoms vom Grad 8 in $\mathbb{Q}[x]$ ist. Zunächst besagt der Hauptsatz der Galoistheorie, dass die Zwischenkörper von $L|\mathbb{Q}$ in antitonischer Bijektion zu den Untergruppen der Galoisgruppe $G$ stehen. Für dieser Aufgabe konkret bedeutet das, dass zu einer Untergruppe $U \leq G$ durch den Fixkörper $L^U$ ein Zwischenkörper von $L|\mathbb{Q}$ gegeben ist. $L^U|\mathbb{Q}$ ist ferner normal genau dann wenn $U \trianglelefteq G$ ist. Ein Zusatz zum Hauptsatz der Galoistheorie besagt schlussendlich, dass $[L^U : \mathbb{Q}] = (G : U)$. Wir stellen fest, dass $S_3 \times Q \trianglelefteq G$ genau dann wenn $Q \trianglelefteq H$. Wir suchen nun einen Normalteiler $Q$ von $H$, der die Ordnung 11 hat. Sei $\nu_{11}$ die Anzahl der 11-Sylowgruppen von $H$. Es gilt nach dem dritten Satz von Sylow $\nu_{11}|8$ und $\nu_{11} \equiv 1 \bmod(11)$. Die erste Bedingung liefert zunächst $\nu_{11} \in \{1, 2, 4, 8\}$ und die zweite Bedingung fixiert zu guter Letzt $\nu_{11} = 1$. Nach einer Folgerung aus dem zweiten Satz von Sylow ist aber $\nu_{11} = 1$ gleichbedeutend damit, dass die einzige 11-Sylowgruppe von $H$, bezeichnet mit $Q$, ein Normalteiler von $H$ ist. Unter Beachtung der eingangs vorgestellten Äquivalenz, haben wir somit einen Normalteiler, nämlich $U = S_3 \times Q$, von $S_3 \times H = G$ gefunden. Dieser erfüllt $|S_3 \times Q| = 11 \cdot 6$. Der Satz von Lagrange liefert $(G : U) = 88 \cdot 6/(11 \cdot 6) = 8 = [L^U : \mathbb{Q}]$. Somit ist der gesuchte Zwischenkörper durch $L^U =: M$ gegeben. Da $L^U|\mathbb{Q}$ den Erweiterungsgrad 8 hat, gibt es nach dem Satz vom primitiven Element ein $\alpha \in L^U$, sodass $L^U = \mathbb{Q}(\alpha)$. Da $L^U|\mathbb{Q}$ laut dem oben Bewiesenen normal ist, zerfällt das Minimalpolynom von $\alpha$, $\mu_{\mathbb{Q},\alpha} \in \mathbb{Q}[x]$ in $L^U$. Damit ist $\mathbb{Q}(\mu^{-1}_{\mathbb{Q},\alpha}(\{0\})) \subseteq \mathbb{Q}(\alpha) = L^U$ und die Inklusion ist wegen $\mu_{\mathbb{Q},\alpha}(\alpha) = 0$ klar. Somit haben wir gezeigt, dass $M = L^U$ der Zerfällungskörper eines Polynoms $f = \mu_{\mathbb{Q},\alpha} \in \mathbb{Q}[x]$ ist, das den Grad 8 hat. □

# 7 Kurs im Wintersemester 2019/2020

**Aufgabe 116 (F15T3A1)** Sei $G$ eine Gruppe und seien $U_1, U_2, V \leq G$ Untergruppen, mit der Eigenschaft, dass $V \subseteq U_1 \cup U_2$. Wir zeigen, dass $V \subseteq U_1$ oder $V \subseteq U_2$ gilt. Angenommen, es ist $V \not\subseteq U_1$ und $V \not\subseteq U_2$. Dann gibt es ein $u_1 \in V$, sodass $u_1 \notin U_1$ und ein $u_2 \in V$, sodass $u_2 \notin U_2$. Da $V$ eine Gruppe ist, ist auch $u_1 u_2^{-1} \in V \subseteq U_1 \cup U_2$. Letzteres bedeutete, dass $u_1 u_2^{-1} \in U_1$ oder $u_1 u_2^{-1} \in U_2$. Im ersten Fall, dass $u_1 u_2^{-1}$ erhalten wir zusammen mit $u_2 \in V \setminus U_2 \subseteq (U_1 \cup U_2) \subseteq U_2 \subseteq U_1$, dass wegen der Verknüpfungseigenschaft $u_1 u_2^{-1} u_2 = u_1 \in U_1$. Das widerspricht der

vorhergehenden Feststellung, dass $u_1 \notin U_1$. Also kann dieser Fall nicht auftreten. Analog finden wir im Fall, dass $u_1 u_2^{-1} \in U_2$, dass $u_2 u_1^{-1} = (u_1 u_2^{-1})^{-1} \in U_2$, wiederum infolge der Gruppeneigenschaft von $U_2$. Da $u_1 \in V \setminus U_1 \subseteq (U_1 \cup U_2) \setminus U_1 \subseteq U_2$, ist auch $u_2 = (u_2 u_1^{-1}) u_1 \in U_2$, im Widerspruch zum oben festgestellten, $u_2 \in V \setminus U_2$, also insbesondere $u_2 \notin U_2$. □

**Aufgabe 117 (F17T2A2)** (a) Sei $G$ eine multipülikativ geschriebene Gruppe der Ordnung $n$ und $g \in G$. Ferner gelte für jeden Primteiler $p$ von $n$, dass $g^{n/p} \neq e_G$. Zu zeigen ist, dass $g$ dann bereits ganz $G$ erzeugt. Da $g \in G$ gilt $\langle g \rangle \leq G$, sodass $\mathrm{ord}(g) = |\langle g \rangle| \leq |G| = n$. Zudem gilt nach Lagrange $\mathrm{ord}(g) | n$. Angenommen, $\mathrm{ord}(g) < n$, dann gibt es ein $m \in \mathbb{N} \setminus \{1\}$, sodass $\mathrm{ord}(g) \cdot m = n$, d.h., $\mathrm{ord}(g) = n/m$. Sei nun $p$ ein beliebiger Primteiler von $m$ (damit auch von $n$). Dann ist $g^{\mathrm{ord}(g) \cdot (m/p)} = e_G$ nach Definition der Ordnung von $g$ einerseits, andererseits $g^{\mathrm{ord}(g) \cdot m/p} = g^{n/m \cdot m/p} = g^{n/p} \neq e_G$ nach Voraussetzung. Wir erhalten somit einen Widerspruch, sodass die Annahme, $\mathrm{ord}(g) < n$ falsch war. Es bleibt nur die Möglichkeit, dass $\mathrm{ord}(g) = n$. $g$ erzeugt also eine Untergruppe der Ordnung $n$ von $G$, das selbst Ordnung $n$ hat, d.h., $\langle g \rangle = G$.
(b) Wir zeigen $4^{3^m} \equiv 1 + 3^{m+1} \bmod(3^{m+2})$ für alle $m \geq 0$. Wir beweisen diese Aussage per Indktion über $m$. Für $m = 0$ gilt $4^{3^0} = 4^1 = 4$ und $4 = 1 + 3^{0+1}$, also insbesondere $4 \equiv 1 + 3^{0+1} \bmod(3^{0+2})$, denn $3^{0+2} = 9 > 4$. Wir setzen nun voraus, dass $4^{3^m} \equiv 1 + 3^{m+1} \bmod(3^{m+2})$ für beliebiges aber fest gewähltes $m \geq 0$ gilt und zeigen, dass dann auch $4^{3^{m+1}} \equiv 1 + 3^{m+2} \bmod(3^{m+3})$. Aus der Voraussetzung erhalten wir zunächst ein $k \in \mathbb{N}_0$, sodass

$$
\begin{aligned}
4^{3^{m+1}} &= \left(4^{3^m}\right)^3 \\
&\overset{\text{Ind.-V.}}{=} \left(k \cdot 3^{m+2} + \cdot \left(1 + 3^{m+1}\right)\right)^3 \\
&= \left(k \cdot 3^{m+2} + \cdot \left(1 + 3^{m+1}\right)\right)^3 \\
&= 3^{3 \cdot (m+2)} k^3 + 3 \cdot 3^{2 \cdot (m+2)} \cdot k^2 \cdot (1 + 3^{m+2}) + 3 \cdot k 3^{m+2} \cdot (1 + 3^{m+1})^2 + (1 + 3^{m+1})^3 \\
&\equiv 0 + 0 + 0 + \left(1 + 3^{m+1}\right)^3 \bmod(3^{m+3}) \\
&\equiv \left(1 + 3 \cdot 1^2 \cdot 3^{m+1} + 3 \cdot 3^{2 \cdot (m+1)} \cdot 1 + 3^{3 \cdot (m+1)}\right) \bmod(3^{m+3}) \\
&\equiv \left(1 + 3^{m+2} + 0 + 0\right) \bmod(3^{m+3}) \\
&\equiv \left(1 + 3^{m+2}\right) \bmod(3^{m+3}).
\end{aligned}
$$

Hierbei haben wir verwendet, dass $3m + 3 \geq m + 3$ und $2m + 3 \geq m + 3$ für alle $m \geq 0$.
(c) Wir sollen zeigen, dass die Restklasse von 2 in $\mathbb{Z}/3^e\mathbb{Z}$ die Einheitengruppe $(\mathbb{Z}/3^e\mathbb{Z})^\times$ erzeugt. Aus der Vorlesunge ist bekannt, dass $(\mathbb{Z}/3^e\mathbb{Z})^\times$ eine Gruppe der Ordnung $\Phi(3^e) = (3-1) \cdot 3^{e-1} = 2 \cdot 3^{e-1}$ ist. Falls $e = 0$ ist die Gruppe einelementig es gilt $\bar{2} = \bar{1}$. Falls $e = 1$, dann ist $|(\mathbb{Z}/3\mathbb{Z})^\times| = 2$ und $\bar{2} \neq \bar{1}$ impliziert, dass $\bar{2}$, das Bild von 2 in $\mathbb{Z}/3^e\mathbb{Z}$, die in Rede stehende Einheitengruppe erzeugt. Sei also $e \geq 2$ beliebig aber fest. Dann ist $|(\mathbb{Z}/3^e\mathbb{Z})^\times| = 2 \cdot 3^{e-1} = n$ eine Zahl, die nur die beiden Primteiler 2 und 3 hat, und ferner $\bar{2} \in (\mathbb{Z}/3^e\mathbb{Z})^\times$. Wir stellen fest, dass das Neutralelement des Restklassenrings $\mathbb{Z}/3^e\mathbb{Z}$ und dessen Einheitengruppe $(\mathbb{Z}/3^e\mathbb{Z})^\times$ übereinstimmt. Laut Aufgabenteil (a) gilt dann $\langle \bar{2} \rangle = (\mathbb{Z}/3^e\mathbb{Z})^\times$, wenn $\bar{2}^{2 \cdot 3^{e-1}/3} \not\equiv \bar{1}$

und $\bar{2}^{2\cdot 3^{e-1}/2} \not\equiv \bar{1}$. Bedingung zwei in der Konjunktion ist wegen $e \geq 2$ erfüllt, denn angenommen $\bar{2}^{3^{e-1}} \equiv \bar{1}$ in $(\mathbb{Z}/3^e\mathbb{Z})^\times$, dann ist auch in $\mathbb{Z}/3^e\mathbb{Z}$ $\bar{2}^{3^{e-1}} \equiv \bar{1} \bmod(3^e)$, also erst recht $\bar{2}^{3^{e-1}} \equiv 1 \bmod(3)$. Da $\bar{2}^3 \cdot \bar{2}^{3^{e-2}} \equiv 2^{\bar{3}^0} \cdot 2^{\bar{e-2}} \bmod(3)$ für alle $e \geq 2$, erhalten wir $\bar{2}^{3^{e-1}} \equiv \bar{2} \bmod(3)$ im Widerspruch zur Annahme. Somit gilt im Ergebnis $\bar{2}^{3^{e-1}} \not\equiv \bar{1}$ in $(\mathbb{Z}/3^e\mathbb{Z})^\times$. Um zu zeigen, dass auch Bedingung eins zutrifft, nehmen wir an, dass $\bar{2}^{2\cdot 3^{e-2}} \equiv \bar{1}$. Dann gilt $(\bar{2}^2)^{3^{e-2}} \equiv \bar{4}^{3^{e-2}} \equiv \bar{1} + \bar{3}^{e-1} \bmod(3^e) \not\equiv \bar{1} \bmod(3^e)$ wegen $3^{e-1} < 3^e$ für alle $e \geq 2$. Nach dem oben zitierten und in Teil (a) bewiesenen Resultat folgt dann, dass $\bar{2}$ tatsächlich die Einheitengruppe $(\mathbb{Z}/3^e\mathbb{Z})^\times$ erzeugt. □

**Aufgabe 118** Wir sollen alle abelschen Gruppen der Ordnung 2020 bis auf Isomorphie klassifizieren. Zunächst sei $G$ eine abelsche Gruppe der Ordnung $n = |G| = 2020 = 20 \cdot 101 = 2^2 \cdot 5 \cdot 101$. Die Zahlen 2, 5 und 101 sind Primzahlen, sodass wir die bis auf Reihenfolge eindeutige Zerlegung der Gruppenordnung in Primzahlen gefunden haben. Da $G$ insbesondere endlich ist, ist $G$ auch endlich erzeugt. Nach dem Hauptsatz über endlich erzeugte abelsche Gruppen ist $G$ daher isomorph zu einem äußeren direkten Produkt von zyklischen Faktoren der Form $G \simeq \mathbb{Z}/d_1 \times \cdots \mathbb{Z}/d_s\mathbb{Z}$, wobei $s \geq 1$, $d_i \in \mathbb{N}$ für $1 \leq i \leq s$ und $d_i | d_{i+1}$ für alle $1 \leq i < s$ und $d_1 > 1$. Für diese sogenannten Elementarteilerketten finden wir die Möglichkeiten

$$2|1010 \quad , \quad 2020.$$

Damit haben wir die zwei Kandidaten $G_1' := \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/1010\mathbb{Z}$ und $G_2' := \mathbb{Z}/2020\mathbb{Z}$ für die gesuchte Klassifikation. Indem wir den Chinesischen Restsatz auf den zweiten Faktor in $G_1$ und auf $G_2$ anwenden, können wir Faktoren von 2-Potenzordnung "herausziehen": Damit finden wir

$$G_1' \simeq G_1'' := \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/505\mathbb{Z}, \tag{168}$$
$$G_2' \simeq G_2'' := \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/505\mathbb{Z}. \tag{169}$$

Anwendung des Chinesischen Restsatzes auf den jeweils letzten zyklischen Faktor von $G_1''$ bzw. $G_2''$ liefert uns nun zusammen mit der Transitivität der Isomorphie-Relation

$$G_1' \simeq G_1 := \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/101\mathbb{Z}, \tag{170}$$
$$G_2' \simeq G_2 := \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/101\mathbb{Z}. \tag{171}$$

Damit ist also $G \simeq G_1$ oder $G \simeq G_2$. Wir zeigen nun noch, dass $G_1 \not\simeq G_2$. Angenommen, $G_1 \simeq G_2$. Dann beachten wir, dass $g = (1, 0, 0) \in G_2$ ein Element der Ordnung 4 in $G_2$ ist. Andererseits hat $G_1$ kein Element der Ordnung 4, denn angenommen $(a, b, c, d) \in G_1$ wäre ein Element der Ordnung 4 in $G_2$, dann wäre $4a = 4b = 0$ in $\mathbb{Z}/2\mathbb{Z}$ aber gleichzeitig $2a \neq 0 \neq 2b$ in $\mathbb{Z}/2\mathbb{Z}$. Da aber $a, b \in \mathbb{Z}/2\mathbb{Z}$ Ordnung 2 haben, kann die zweite Forderung nicht erfüllt werden. Damit haben wir einen Widerspruch zur Annahme, es gäbe in $G_1$ ein Element der Ordnung 4. Da unter Isomorphie von Gruppen insbesondere die Elementordnung erhalten bleibt, haben wir insgesamt ein Widerspruch zur Annahme, dass $G_1 \simeq G_2$. Somit sind $G_1$ und $G_2$ in der Tat verschiedene Isomorphietypen und die Gruppe $G$ ist von genau einem der beiden (verschiedenen) Typen. □

**Aufgabe 119 (H17T1A3)** Wir sollen zeigen, dass keine der Gruppe $G_1 = (\mathbb{Z}/13\mathbb{Z})^\times$, $G_2 = (\mathbb{Z}/28\mathbb{Z})^\times$, $G_3 = A_4$ und $G_4 = D_6$ jeweils zu einer anderen Gruppe aus der Liste isomorph ist. Zunächst stellen wir fest, dass $G_1$ und $G_2$ als Einheitengruppen von Restklassenringen abelsch sind. Insbesondere gilt mit dem Chinesischen Restsatz der Ringtheorie $G_2 \simeq (\mathbb{Z}/2^2\mathbb{Z})^\times \times (\mathbb{Z}/7\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Zudem ist $G_1 \simeq \mathbb{Z}/\Phi(13)\mathbb{Z} = \mathbb{Z}/12\mathbb{Z}$. Ferner ist $A_4$ eine nicht-abelsche Gruppe, denn es gilt in Zykel-Notation $A_4 \ni (123)$, $A_4 \ni (12)(34)$ und $(123) \odot (12)(34) = (413) \neq (432) = (12)(34) \odot (123)$, da bereits der Träger der jeweiligen Produkte verschieden ist. Die Gruppe $D_6$ wird von einem Element $\tau \in S_6$ der Ordnung 2 und einem Element $\sigma \in S_6$ der Ordnung 6 erzeugt, sodass $\tau\sigma\tau = \sigma^{-1}$. Aus der letzteren Relation erhalten wir unter Beachtung, dass $\tau^{-1} = \tau$ $\tau\sigma = \sigma^{-1}\tau$. Da aber $\sigma^{-1} = \sigma$, wenn man Kommutativität von $D_6$ Annähme, zu $\sigma^2 = 1$, also einem Widerspruch zu $\mathrm{ord}(\sigma) = 6 > 2$ führte, ist auch $D_6$ nicht-abelsch. Somit gilt zumindest, dass $G \not\simeq H$, wobei $G \in \{G_1, G_2\}$ eine der abelschen Gruppen und $H \in \{G_3, G_4\}$ einer der nicht-abelschen Gruppen ist. Es bleibt also zu zeigen, dass (i) $G_1 \not\simeq G_2$ und (ii) $G_3 \not\simeq G_4$.

- *Zu (i).* Wir stellen fest, dass $\bar{1} \in G_1$ ein Element der Ordnung 12 ist. Andererseits hat $G_2$ kein Element der Ordnung 12, denn für alle $(a, b) \in G_2$ gilt bereits $6(a, b) = (6a, 6b) = (\bar{0}, \bar{0})$, sodass $\mathrm{ord}((a, b)) \leq 6 < 12$ gilt. Da unter einem Isomorphismus $G_1 \to G_2$ insbesondere die Ordnung von $\bar{1} \in G_1$ erhalten bliebe, kann ein Isomorphismus $G_1 \to G_2$ nicht existieren.

- *Zu (ii).* Es ist $A_4 \leq S_4$, und ein beliebiges Element aus $A_4$ lässt sich entweder als Identität, Doppeltransposition oder 3-Zykel in disjunkter Zykel-Schreibweise ausdrücken. In jedem Fall gilt für beliebiges $\sigma' \in A_4$, dass $\mathrm{ord}(\sigma') \leq 3$. Andererseits gibt es nach Definition von $D_6$ ein Element $\sigma \in D_6$, das die Ordnung 6 hat. Analog zu (i) von gerade eben schließt man also, dass $D_6$ und $A_4$ nicht isomorph sind.

Damit haben wir gezeigt, dass $G_1$, $G_2$, $G_3$, $G_4$ paarweise nicht-isomorph sind. □

**Aufgabe 120 (F19T1A1(d))** Sei $G$ eine Gruppe der Ordnung 95. Wir zeigen, dass $G$ zyklisch ist. Es ist $95 = 5 \cdot 19$. Bezeichne $\nu_p$ für eine Primzahl $p$ die Anzahl der $p$-Sylowgruppen von $G$. Dann ist nach dem dritten Sylowschen Satz $\nu_{19}|5$, also $\nu_{19} \in \{1, 5\}$ und erfüllt zudem $\nu_{19} \equiv 1 \bmod(5)$. Damit ist nur $\nu_{19} = 1$ möglich. Analog gilt $\nu_5 \in \{1, 19\}$ und zudem $\nu_5 \equiv 1\,19$, was nur für $\nu_5 = 1$ möglich ist. Also gibt es genau eine 5-Sylow-Gruppe, bezeichnet $P$, von $G$ und genau eine 19-Sylowgruppe von $G$, die wir $Q$ nennen. Nach einer Folgerung aus dem zweiten Sylowschen Satz sind dann, da es zu $p \in \{5, 19\}$ jeweils nur eine $p$-Sylowgruppe von $G$ gibt, $P$ und $Q$ Normalteiler von $G$. Da $|P| = 5$ und $|Q| = 19$ von teilerfremder Ordnung sind ist $P \cap Q = \{e_G\}$. Damit können wir das innere direkte Produkt $P \cdot Q \leq G$ bilden, und es gilt sogar stärker $G \simeq P \cdot Q$, da $|P \cdot Q| = |P||Q\| = 95$. Aus der Vorlesung ist bekannt, dass das innere direkte Produkt zweier Normalteiler $P, Q$ von $G$ isomorph zum äußeren direkten Produkt $P \times Q$ ist. Somit haben wir die Isomorphie $P \times Q \simeq G$. Da $P$ und $Q$ jeweils von Primzahlordnung sind, sind sie zudem zyklisch, d.h., $P \simeq \mathbb{Z}/5\mathbb{Z}$ und $Q \simeq \mathbb{Z}/19\mathbb{Z}$. Wiederum infolge Teilerfremdheit von 5 und 19 liefert uns der Chinesische Restsatz $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/19\mathbb{Z} = \mathbb{Z}/95\mathbb{Z}$. Insgesamt

haben wir somit die Isomorphie $G \simeq \mathbb{Z}/95\mathbb{Z}$, d.h., $G$ ist isomorph zur zyklischen Gruppe $\mathbb{Z}/95\mathbb{Z}$, damit selbst zyklisch. □

**Aufgabe 121 (F12T2A1)** (a) Wir untersuchen, ob $G = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ und $H = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$ isomorph sind. Mittels Chinesischem Restsatz erhalten wir zunächst $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ und $H \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. Aufgrund der Transitivität der Isomorphie zweier Gruppen stellen wir $G \simeq H$ fest.
(b) Die alternierende Gruppe $A_4$ ist nicht einfach, denn aus der Vorlesung ist bekannt, dass die Kleinsche Vierergruppe $V_4$ ein nicht-trivialer Normalteiler von $A_4$ ist.
(c) Sei $M = \{\sigma \in S_5 | \text{ord}(\sigma) = 2\}$. $M$ enthält alle Elemente von $S_5$, die die Ordnung 2 haben. Angenommen, alle Elemente der Ordnung 2 wären zueinander konjugiert. Es ist $(12) \in S_5$ ein Element der Ordnung 2 und ebenso $(12)(34) \in S_5$. Laut Annahme gibt es dann ein $\sigma \in S_5$, sodass $\sigma(12)\sigma^{-1} = (12)(34)$, was aber dem Vorlesungsresultat widerspricht, dass zwei Element der $S_n$ genau dann konjugiert sind, wenn sie vom gleichen Zerlegungstyp sind. Das ist bei (12), das Zerlegungstyp (2) hat und bei (12)(34), das Zerlegungstyp $(2, 2)$ hat, nicht der Fall.
(d) Wir behaupten, dass $(x) \subseteq \mathbb{Z}[x]$ ein Primideal ist. Dazu betrachten wir den Einsetzungshomomorphismus $\phi : \mathbb{Z}[x] \to \mathbb{Z}, f \mapsto f(0)$, von dem aus der Vorlesung bereits die Surjektivität bekannt ist. Es ist $\phi(f) = 0$ genau dann, wenn das ganzzahligen Polynom $f$ konstantes Glied hat, d.h., für ein $n \in \mathbb{N}$ und $a_1, ..., a_n \in \mathbb{Z}$ von der Form

$$f = \sum_{k=1}^{n} a_k x^k = x \left( \sum_{k=1}^{n} a_k x^{k-1} \right) \in (x) \tag{172}$$

ist. Umgekehrt lässt sich jedes $f \in (x)$ in dieser Form schreiben, sodass auch $(x) \in \ker \phi$. Nach dem Homomorphiesatz für Ring induziert $\phi$ daher $\mathbb{Z}[x]/(x) \simeq \mathbb{Z}$. $\mathbb{Z}$ ist bekanntermaßen ein Integritätsbereich, sodass das Ideal $(x)$ ein Primideal ist. □

**Aufgabe 122 (H19T3A2)** Sei $G$ eine Gruppe und $H \leq G$ eine Untergruppe vom Index $n \in \mathbb{N}$.
(a) Zu zeigen ist, dass für alle $g \in G$ ein $j \in \{1, ..., n\}$ existiert, sodass $g^j \in H$. Sei $\mathcal{M} = \{g^k H | 0 \leq k \leq n\}$. Dann ist $|\mathcal{M}| = n+1 > n = |G/H|$, wobei $G/H$ die Menge der Linksnebenklassen von $H$ in $G$ bezeichnet. Daher gibt es ohne Einschränkung $k_1, k_2 \in \{0, 1, 2, ..., n\}$ mit $k_1 < k_2$ (also insbesondere verschieden), sodass $g^{k_1} H = g^{k_2} H$. Letztere Gleichung ist äquivalent zu $g^{k_2} \in g^{k_1} H$. Damit gibt es ein $h \in H$, sodass $g^{k_2 - k_1} = h \in H$. Wegen $0 \leq k_1 < k_2 \leq n$ ist $j \equiv k_2 - k_1 \in \{1, ..., n\}$ und wir finden mit dem soeben definierten $j$ $g^j \in H$ wie behauptet.
(b) Wir zeigen, dass das in (a) gefundene $j$ nicht notwendigerweise als Teiler von $n$ gefordert werden kann. Falls $G$ abelsch ist, dann ist $H \trianglelefteq G$. Damit gilt bereits, dass $G/H$ die algebraische Struktur einer Gruppe ("Faktorgruppe") trägt, deren Neutralelement $eH$ ist. Insbesondere ist $G/H$ laut Vorlesung dann selbst abelsch. Somit ist zu beliebigem $g \in G$ $\langle gH \rangle \leq G/H$, also nach Lagrange $\text{ord}(gH) | n$. Wir bezeichnen die Ordnung von $gH$ mit $J$. Dann ist $(gH)^J = (gH)(gH) \cdots (gH) =$

$g(Hg)(Hg)\cdots(Hg)H = g^J H = eH = H$, was bedeutet, dass $g^J \in H$. Somit ist es im Falle abelschen $G$s stets möglich, $J$ als Teiler von $n$ zu wählen. Wir versuchen also eine nicht-abelsche Gruppe. Sei $G = S_3$ die Permutationsgruppe der dreielementigen Menge. Diese ist laut Vorlesung nicht-abelsch und hat Ordnung 6. Wir betrachten die Untergruppe $H = \langle(13)\rangle \leq G$. Diese hat Ordnung 2 und somit nach Lagrange den Index 3. Die einzigen Teiler von 3 sind 1 und 3. Das Element $(12) \in S_3$ erfüllt aber $(12)^3 = (12)$ und es gilt $(12) \notin H$, sondern nur $(12)^2 = \mathrm{id} \in H$. Da $2 \not| 3$ haben wir gezeigt, dass es – in der Notation von (a) – nicht immer möglich ist, einen Teiler $j$ von $n$ mit der in (a) spezifizierten Eigenschaft zu wählen. □

**Aufgabe 123 (H18T1A2(a))** Sei $G$ eine Gruppe und $H \leq G$ vom endlichen index $n$. Sei $M \equiv \{gHg^{-1} | g \in G\}$. Wir zeigen, dass $M$ endlich ist. Sei dazu $R$ ein Repräsentantensystem von $G/H$. Wir definieren $\phi : R \to M, g \mapsto gHg^{-1}$. Wir behaupten, dass diese Abbildung surjektiv ist. Sei $x \in G$ beliebig. Dann gibt es wegen der Zerlegungseigenschaft der Linksnebenklassen von $H$ in $G$ ein $g \in G$, sodass $gH = xH$. Damit finden wir ein $h \in H$, sodass $g^{-1}x = h$. Nun gilt $gHg^{-1} = ghHh^{-1}g^{-1} = (gg^{-1}x)H(x^{-1}gg^{-1}) = xHx^{-1}$. Somit ist $xHx^{-1} \in \phi(R)$ und Beliebigkeit von $x \in G$ impliziert $M \subseteq \phi(R)$, die umgekehrte Inklusion ist wegen Wohldefiniertheit von $\phi$ klar. Somit haben wir $|M| \leq n$ und $M$ ist insbesondere endlich. □

**Aufgabe 124 (H18T2A3(a))** Sei $G$ eine abelsche Gruppe und bezeichne $T(G)$ die Menge aller Elemente aus $G$, die endliche Ordnung haben. Eine Gruppe $G$ ist torsionsfrei, wenn gilt $T(G) = \{0_G\}$.
(a.i) Wir zeigen, dass es sich bei $T(G)$ in jedem Fall um eine Untergruppe von $G$ handelt. Per Definition von $T(G)$ ist bereits $T(G) \subseteq G$ klar. Da in jedem Fall gilt $1 \cdot 0_G = 0_G$, d.h., das Neutralelement von $G$ Ordnung 1 hat, ist $0_G$ in $T(G)$. Seien nun $a, b \in G$ zwei Elemente endlicher Ordnung. Wir zeigen nun, dass auch $a+b \in T(G)$. Sei $n = \mathrm{ord}(a)$ und $m = \mathrm{ord}(b)$. Da $a, b \in T(G)$ sind $n, m \in \mathbb{N}$. Wir behaupten, dass gilt $\mathrm{ord}(a+b) | n \cdot m$. Es gilt in der Tat $(n \cdot m)(a+b) = (a+b)+(a+b)+...+(a+b) = (a+a+...+a)+(b+b+...+b) = m \cdot (n \cdot a)+n \cdot (m \cdot b) = m \cdot 0_G + n \cdot 0_G = 0_G + 0_G = 0_G$, wobei wir im zweiten Schritt die Kommutativität von $G$ verwendet haben und in den folgenden Schritten vom Assoziativgesetz in $G$ Gebrauch gemacht haben, um den anfänglichen Ausdruck als Verknüpfung von (additiv geschriebenen Potenzen) von $n \cdot a = 0_G$ und $m \cdot b = 0_G$ zu schreiben. Dieser evaluierte dann zu $0_G$, weil das Neutralelement $0_G$ Ordnung 1 hat. Wir zeigen nun, dass mit $a \in T(G)$ auch $-q \in T(G)$. Für $a = 0_G$ ist das klar, denn $0_G + 0_G = 0_G$, sodass $-0_G = 0_G$. Sei also $a \neq 0_G$. Dann ist $\mathbb{N} \ni n := \mathrm{ord}(a) > 1$. Sei $-a$ das zu $a$ inverse Element in $G$. Dann ist auch $-a \neq 0_G$, denn andernfalls wäre $a + (-a) = a + 0_G = a = 0_G$, im Widerspruch zu $a \neq 0_G$. Angenommen, $\mathrm{ord}(a) \neq \mathrm{ord}(-a)$. Dann führte $a+(-a) = 0_G$ nach Potenzieren mit $m := \min\{n, \mathrm{ord}(-a)\}$ auf den Widerspruch $m \cdot a = 0_G$ bzw. $m \cdot (-a) = 0_G$ im Widerspruch zur Minimalität der Ordnung des jeweiligen Elements. Folglich ist $\mathrm{ord}(a) = \mathrm{ord}(-a)$ und die rechte Seite damit insbesondere endlich. Damit ist die Untergruppeneigenschaft von $T(G)$ nachgewiesen.
(a.ii) Wir zeigen nun, dass $G/T(G)$ torsionsfrei ist. Da $G$ laut Voraussetzung abelsch ist, ist die Untergruppe $T(G)$ automatisch ein Normalteiler von $G$. Die Menge der Linksnebenklasse $G/T(G)$ trägt also die Struktur einer Faktorgruppe. Um zu zeigen,

dass $T(G/T(G)) = \{0_{G/T(G)}\}$, wobei $0_{G/T(G)}$ das Neutralelement von $G/T(G)$ ist, betrachten wir ein beliebiges $g+T(G) \in G/T(G)$, wo $g \in G \setminus T(G)$ Repräsentant einer von $0_G + T(G) = T(G)$ verschiedenen Nebenklasse ist, und zeigen, dass das betrachtete Element nicht endliche Ordnung hat. Angenommen $n \equiv \text{ord}(g + T(G)) \in \mathbb{N}$. Dann ist $0_G + T(G) = n(g + T(G)) = n \cdot ng + T(G)$, d.h., $ng \in 0_G + T(G) = T(G)$. Das bedeutet aber gerade, dass $ng$ endliche Ordnung, bspw. $m \in \mathbb{N}$, hat. Damit gilt aber $0_G = m \cdot ng = (mn)g$, also $\text{ord}(g)|mn$, sodass $g \in T(G)$, im Widerspruch zu $g \in G \setminus T(G)$. Damit gibt es kein $g+T(G) \in G/T(G)$, das von $0_G + T(G) = 0_{G/T(G)}$ verschieden ist, sodass $g + T(G) \in T(G/T(G))$. Damit ist wegen der Gruppeneigenschaft der Torsionsgruppe nur $T(G/T(G)) = \{0_{G/T(G)}\}$ möglich. Letzteres heißt, dass $G/T(G)$ torsionsfrei ist. □

**Aufgabe 125 (F13T2A1)** Zu zeigen ist, dass alle Elemente von $\mathbb{Q}/\mathbb{Z}$ von endlicher Ordnung sind. Für $0 + \mathbb{Z}$, das Neutralelement der Faktorgruppe, ist klar, dass es endliche Ordnung hat. Sei dazu $a/b \in \mathbb{Q} \setminus \mathbb{Z}$ ein vollständig gekürzter Bruch ($\text{ggT}(a, b) = 1$). Es ist $a \in \mathbb{Z}$ und $b \in \mathbb{N}$. Es gilt nun, dass $b \cdot (a/b+\mathbb{Z}) = b \cdot (a/b)+\mathbb{Z} = a + \mathbb{Z} = \mathbb{Z}$, denn $a \in \mathbb{Z}$. Wegen $\text{ggT}(a, b) = 1$ gibt es auch kein $\mathbb{N} \ni n < b$, sodass $n(a/b+\mathbb{Z}) = \mathbb{Z}$. Wir bestimmen nun die Elemente endlicher Ordnung in $\mathbb{R}/\mathbb{Z}$. Wegen $\mathbb{Q} \subset \mathbb{R}$, ist auch $\mathbb{Q}/\mathbb{Z} \subseteq \mathbb{R}/\mathbb{Z}$. Wir zeigen nun, dass wir damit bereits alle Elemente endlicher Ordnung gefunden haben. Sei $a + \mathbb{Z} \in \mathbb{R}/\mathbb{Z}$ ein Element der endlichen Ordnung $n \in \mathbb{N}$. Dann gilt $n \cdot (a + \mathbb{Z}) = 0 + \mathbb{Z} \Leftrightarrow n \cdot a \in \mathbb{Z}$. Das bedeutet, es gibt ein $m \in \mathbb{Z}$, sodass $n \cdot a = m$. Die letzte Gleichung können wir wegen $n \neq 0$ zu $a = m/n$ umschreiben. Das bedeutet aber gerade, dass $a \in \mathbb{R}$ die Form eine Bruchs hat, d.h., dass $a \in \mathbb{Q}$. Damit haben sind alle Elemente endlicher Ordnung aus $\mathbb{R}/\mathbb{Z}$ in $\mathbb{Q}/\mathbb{Z}$ enthalten und alle in der letztgenannten Gruppe enthaltenen Elemente haben endliche Ordnung, wie oben nachgewiesen. Wir bestimmen nun die Elemente in $\mathbb{R}/\mathbb{Q}$, die von endlicher Ordnung sind. Da das Neutralelement der Faktorgruppe $\mathbb{R}/\mathbb{Q}$ von der Ordnung 1 ist, wissen wir bereits, dass $T(\mathbb{R}/\mathbb{Q}) \supseteq \{0+\mathbb{Q}\}$. Wir behaupten, dass auch die umgekehrte Inklusion gilt. Denn andernfalls gäbe es ein $a \in \mathbb{R} \setminus \mathbb{Q}$, sodass $n(a + \mathbb{Q}) = \mathbb{Q}$, wobei $n = \text{ord}(a) \in \mathbb{N}$. Das bedeutet aber, dass $n \cdot a = q$, wobei $q \in \mathbb{Q}$. Da $1/n \in \mathbb{Q}$, haben wir $a = q/n \in \mathbb{Q}$, im Widerspruch zu $a \in \mathbb{R} \setminus \mathbb{Q}$. Somit gilt $T(\mathbb{R}/\mathbb{Q}) = \{0 + \mathbb{Q}\}$. □

**Aufgabe 126 (F14T2A3)** Sei $G$ eine Gruppe und bezeichne mit $\phi_h$ für alle $h \in G$ den wie folgt definierten Gruppenhomomorphismus $\phi_h : G \to G$ mit $\phi_h(g) = hgh^{-1}$ für alle $g \in G$. Definiere $\text{Inn}(G) = \{\phi_h | h \in G\} \subseteq \text{Aut}(G)$ und $Z(G) = \{h \in G | gh = hg \, \forall g \in G\}$.
(a) Zu zeigen ist, dass $\text{Inn}(G) \trianglelefteq \text{Aut}(G)$. Zunächst prüfen wir die Untergruppeneigenschaft nach. Als bekannt vorausgesetzt wird dabei, dass $\text{Aut}(G)$ die Gruppe der Automorphismen von $G$ ist (eine Gruppe also). Wir zeigen, dass das Neutralelement $\text{id}_G$ von $\text{Aut}(G)$ auch in $\text{Inn}(G)$ liegt. Sei dazu $g \in G$ beliebig. Es gilt $\phi_e(g) = ege^{-1} = ege = g = \text{id}_G(g)$, wobei $e$ das Neutralelement in $G$ bezeichnet. Beliebigkeit von $g \in G$ impliziert $\text{id}_G = \phi_e \in G$. Seien nun $\phi_1, \phi_2 \in \text{Inn}(G)$ beliebig. Zu zeigen ist, dass $\phi_1 \circ \phi_2 \in \text{Inn}(G)$. Wegen $\phi_1, \phi_2 \in \text{Inn}(G)$ gibt es $h_1, h_2 \in G$, sodass $\phi_1 = \phi_{h_1}$ und $\phi_2 = \phi_{h_2}$. Sei $g \in G$ beliebig. Dann gilt $(\phi_1 \circ \phi_2)(g) = \phi_1(h_2 g h_2^{-1}) = h_1 h_2 g h_2^{-1} h_1^{-1} = h_1 h_2 g (h_1 h_2)^{-1} = \phi_{h_1 h_2}(g)$, also

$\phi_1 \circ \phi_2 = \phi_{h_1h_2}$. Wegen $h_1h_2 \in G$ ist auch $\phi_{h_1h_2} \in \mathrm{Inn}(G)$ und damit $\phi_1 \circ \phi_2$. Wir zeigen nun, dass für beliebiges $h \in G$ auch $\phi_h^{-1} \in \mathrm{Inn}(G)$. Es gilt für beliebiges $g \in G$ $\phi_{h^{-1}}(\phi_h(g)) = \phi_{h^{-1}}(hgh^{-1}) = h^{-1}(hgh^{-1})h = (h^{-1}h)g(h^{-1}h) = ege = g = (hh^{-1})g(hh^{-1}) = \phi_h(h^{-1}g(h^{-1})^{-1}) = \phi_h(\phi_{h^{-1}}(g))$. Somit ist $\phi_h^{-1} = \phi_{h^{-1}} \in \mathrm{Inn}(G)$. Damit ist die Untergruppeneigenschaft von $\mathrm{Inn}(G)$ nachgewiesen. Wir zeigen nun die Normalteilereigenschaft. Sei $\psi \in \mathrm{Aut}(G)$ beliebig. Dann gilt für alle $g, h \in G$, dass $(\psi \circ \phi_h \circ \psi^{-1})(g) = \psi(h\psi^{-1}(g)h^{-1}) = \psi(h)\psi(\psi^{-1}(g))\psi^{-1}(h) = \psi(h)g\psi^{-1}(h) = \psi(h)g(\psi(h))^{-1} = \phi_{\psi(h)}(g)$, also $\psi \circ \phi_h\psi \in \mathrm{Inn}(G)$ für alle $h \in G$ und somit $\psi\mathrm{Inn}(G)\psi^{-1} \subseteq \mathrm{Inn}(G)$, woraus laut Vorlesung bereits die Normalteilereigenschaft $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$ folgt.
(b) Zu zeigen ist, dass $\phi : G \to \mathrm{Inn}(G), h \mapsto \phi_h$ einen Gruppenisomorphismus $G/Z(G) \simeq \mathrm{Inn}(G)$ induziert. Wir zeigen zunächst, dass $\phi$ ein Gruppenhomomorphismus ist. Für $h_1, h_2, g \in G$ beliebig gilt $\phi(h_1h_2)(g) = \phi_{h_1h_2}(g) = h_1h_2g(h_1h_2)^{-1} = h_1(h_2gh_2^{-1})h_1^{-1} = \phi_{h_1}(\phi_{h_2}(g)) = \phi_{h_1}(\phi(h_2)(g)) = (\phi(h_1) \circ \phi(h_2))(g)$, also $\phi(h_1h_2) = \phi(h_1) \circ \phi(h_2)$. Nach Definition von $\mathrm{Inn}(G)$ gibt es ferner zu jedem $\psi \in \mathrm{Inn}(G)$ ein $h \in G$, sodass $\psi = \phi_h$. Mit diesem $h \in G$ gilt dann $\phi(h) = \phi_h = \psi$. Somit ist $\phi$ surjektiv. Wir wenden nun den Homomorphiesatz an, und sehen, dass $G/\ker\phi \simeq \mathrm{Inn}(G)$. Zum Abschluss bemerken wir, dass $h \in \ker\phi \Leftrightarrow \phi(h)(g) = \mathrm{id}_G(g) = g\,\forall g \in G \Leftrightarrow hgh^{-1} = g \Leftrightarrow hg = gh\,\forall g \in G \Leftrightarrow h \in Z(G)$. Damit haben wir $ker\psi = Z(G)$ nachgewiesen und die Isomorphie $G/Z(G) \simeq \mathrm{Inn}(G)$ gefunden, die durch den nach Homomorphiesatz von $\phi$ induziertem Isomorphismus $\bar{\phi} : G/\ker\phi \to \mathrm{Inn}(G)$ gewährleistet wird.
(c) $G := (\mathbb{Z}/7\mathbb{Z}, +)$ ist zyklisch von Ordnung 7. Laut Vorlesung gilt nun $\mathrm{Aut}(G) \simeq (\mathbb{Z}/7\mathbb{Z})^\times$, wobei $\mathbb{Z}/7\mathbb{Z}$ hier als primer Restklassenring aufzufassen ist. Es gilt $|\mathrm{Aut}(G)| = |(\mathbb{Z}/7\mathbb{Z})^\times| = \Phi(7) = 7 - 1 = 6$. Damit gibt es genau 6 Automorphismen von $G$. Angenommen, es gäbe ein $\phi_h \neq \mathrm{id}$ in $\mathrm{Inn}(G)$. Dann gibt es ein $g \in G$, sodass $h + g + (-h) \neq g$. Da aber $G$ als zyklische Gruppe abelsch ist, haben wir $h + g + (-h) = g + (h + (-h)) = g + 0 = g$, im Widerspruch zur Definition des gewählte $g$. Da $\mathrm{Inn}(G) \supseteq \{\mathrm{id}_G\}$ haben wir somit bereits nachgewiesen, dass nur die Identität ein innerer Automorphismus von $\mathbb{Z}/7\mathbb{Z}$ ist. □

**Aufgabe 127 (H19T1A1(d))** Gesucht sind $i, k \in \mathbb{N}$, sodass $\mathrm{sgn}(\sigma) = 1$, wobei $\sigma \in S_9$ gegeben ist durch

$$\sigma \equiv \sigma_{i,k} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 2 & 7 & 4 & i & 5 & 6 & k & 9 \end{pmatrix}.$$

Da $\sigma \in S_9 = \mathrm{Per}(\{1,2,3,4,5,6,7,8,9\})$, ist nur $i = 3$ und $k = 8$ oder $i = 8$ und $k = 3$ möglich. Falls $i = 3$, dann ist $k = 8$ und wir können $\sigma_{i=3,k=8}$ in (disjunkter) Zykelschreibweise als $\sigma = (3765)$ angeben. Da $\mathrm{sgn}((3765)) = (-1)^{l((3765))-1} = (-1)^3 = -1$, wobei $l(...)$ die Länge des Zykels bezeichnet, scheidet diese Option aus. Wegen $\sigma_{8,3} = (3,8) \circ \sigma_{8,3}$, liefert die Homomorphismuseigenschaft des Signumshomomorphismus sofort, dass $\mathrm{sgn}(\sigma_{8,3}) = (-1) \cdot \mathrm{sgn}(\sigma_{3,8}) = (-1) \cdot (-1) = 1$. Damit sehen wir, dass $i = 8$ und $k = 3$ die einzige Möglichkeit ist, $i$ bzw. $k$ aus $\mathbb{N}$ gemäß Anforderung zu wählen.

**Aufgabe 128** Gesucht sind $i, j, k \in \mathbb{N}$, sodass $\text{sgn}(\sigma) = 1$, wobei $\sigma \in S_9$ gegeben ist durch

$$\sigma = \sigma_{i,j,k} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 8 & i & 1 & j & 3 & 9 & 5 & k \end{pmatrix}.$$

Da $\sigma \in S_9$ sind nur die Möglichkeiten $\{i, j, k\} = \{2, 4, 6\}$ beachtlich. Wir versuchen $i = 2, j = 4, k = 6$. Dann ist

$$\sigma_{2,4,6} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 8 & 2 & 1 & 4 & 3 & 9 & 5 & 6 \end{pmatrix} = (1, 7, 9, 6, 3, 2, 8, 5, 4). \tag{173}$$

Hierbei handelt es sich um einen 9-Zykel und es gilt $\text{sgn}(\sigma_{2,4,6}) = (-1)^{l(\sigma_{2,4,6})} = (-1)^8 = 1$. Da für jede Transposition $\tau (\in S_9)$ Signum $-1$ hat, liefert uns die Homomorphismuseigenschaft des Signums von Permutation, dass gerade Permutationen von der Form $\sigma_{i,j,k}$ nur noch durch Komposition mit genau zwei Transpositionen zustande kommen können, bzw., da $|\{2, 4, 6\}| = 3$, durch Komposition mit einem 3-Zykel, dessen Träger durch die Menge $\{2, 4, 6\}$ festgelegt ist. Damit finden wir, dass neben $(i = 2, j = 4, k = 6)$ nur noch alle zyklischen Vertauschungen dieser Werte für $i$, $j$ und $k$ zulässig sind.

**Aufgabe 129 (H03T2A1)** (a) Es gilt $A_n \equiv \{\sigma \in S_n | \text{sgn}(\sigma) = 1\} = \ker(\text{sgn})$, wobei $\text{sgn} : S_n \to \{\pm 1\}$ des Signumshomomorphismus ist.
(b) Für $n \geq 2$ ist sgn surjektiv, denn es gilt $\text{sgn}(\text{id}) = 1$ und $\text{sgn}((12)) = -1$. Der Homomorphiesatz liefert nun $S_n/A_n \simeq \{\pm 1\}$. Zusammen mit der Endlichkeit von $S_n$ und dem Satz von Lagrange erhalten wir also $(S_n : A_n) = 2$.
(c) Sei $n = 4$. Wegen $|S_n| = 4! = 24$ und $(S_4 : A_4) = 2$ ist $A_4 \trianglelefteq S_4$ und $|A_4| = 12$. Sei $\nu_3$ und $\nu_2$ die Anzahl der 3- bzw. 2-Sylowgruppen von $A_4$. Nach dem dritten Sylow'schen Satz gilt $\nu_2 | 3$ und $\nu_2 = 1 \, mod(2)$, also $\nu_2 \in \{1, 3\}$. Ebenso ist $\nu_3 | 4$ und $\nu_3 \equiv 1 \, \text{mod}(3)$, also $\nu_3 \in \{1, 4\}$ Falls $\nu_2 = 3, \nu_3 = 4$ dann haben wir 1 Element der Ordnung 1 in der Vereinigungsmenge aller Sylowgruppen von $A_4$, $3 \cdot 3$ Elemente der Ordnung 2 oder 4 und $4 \cdot 2$ Elemente der Ordnung 3. Da die genannte Vereinigungsmenge aber eine Teilmenge von $A_4$ ist, die selbst nur 12 Elemente hat, scheidet dieser Fall aus. Falls $\nu_3 = 1$, dann wäre die einzige 3-Sylowgruppe von $A_4$ nach dem dritten Sylow'schen Satz ein Normalteiler von $A_4$. Aber es sind $\langle (123) \rangle, \langle (234) \rangle \leq A_4$ zwei verschiedene Untergruppen der Ordnung 3 von $A_4$, sodass $\nu_3 \neq 1$ und damit $\nu_3 = 4$. Somit bleibt nur noch die Möglichkeit, dass $\nu_2 = 1$ und wir finden, dass es genau eine 2-Sylowgruppe $V_4 \leq A_4$ gibt. $V_4$ ist die sogenannte Kleinsche Vierer-Gruppe. Laut einer Folgerung aus dem zweiten Sylow'schen Satz gilt wegen $\nu_2 = 1$, dass $V_4 \trianglelefteq A_4$. Da $|V_4| = 2^2$ von Primzahlquadratordnung ist, ist $V_4$ auflösbar. Da $|A_4/V_4| = 3$ von Primzahlordnung ist, ist $A_4/V_4$ zyklisch von Ordnung 3, also insbesondere abelsch und damit auflösbar. Laut Vorlesung folgt aus der Auflösbarkeit von $A_4/V_4$ und $V_4$ bereits die Auflösbarkeit von $A_4$. Da $S_4/A_4$ Ordnung 2 hat, ist $S_4/A_4$ wiederum zyklisch, also abelsch, also auflösbar. Zusammen mit der Auflösbarkeit von $A_4$ folgt die Auflösbarkeit von $S_4$ genauso wie beim Nachweis der Auflösbarkeit von $A_4$. □

**Aufgabe 130 (F18T3A1(c))** Die gesuchte Darstellung von $\phi \in S_9$ ist $\phi = (15487)(2936)$. Da $\phi$ das Produkt eines 5-Zykels und eines 4-Zykels ist, die dis-

jukten Träger haben, hat $\phi$ die Ordnung $\text{ord}(\phi) = \text{kgV}(\text{ord}(15487), \text{ord}(2936)) = \text{kgV}(5, 4) = 20$. □

**Aufgabe 131 (F16T1A3)** Sei $(A, +)$ eine abelsche Gruppe und $(H, \cdot)$ eine Gruppe, die einen Normalteiler $N$ vom Index 2 hat.
(a) Wir zeigen, dass $x, y \in H \setminus N$ impliziert, dass $xy \in N$. Da $N \trianglelefteq H$, ist $H/N$ eine Gruppe, deren Ordnung $|H/N| = (H : N) = 2$ erfüllt. Da $H/N$ von Primzahlordnung ist, ist $H/N$ insbesondere zyklisch. Bezeichne mit $\bar{x}$ das Bild von $x \in H$ unter dem kanonischen Epimorphismus $\pi : H \to H/N$. Dann gilt $\bar{x} \neq \bar{e}$ und $\bar{y} \neq \bar{e}$ für $x, y \in H \setminus N$. Da $H/N$ Ordnung 2 hat, folgt $\bar{x} = \bar{y}$. Somit ist $\overline{x \cdot y} = \bar{x} \cdot \bar{y} = \bar{x}^2 = \bar{e}$, d.h., $xy \in N$.
(b) Wir definieren auf $A \times H$ eine Verknüpfung wie folgt

$$(a, x) * (b, y) = \begin{cases} (a + b, xy) & x \in N \\ (a - b, xy) & x \in N \end{cases}.$$

Wir sollen zeigen, dass die oben angegebene Verknüpfung assoziativ ist. Seien $(a, x), (b, y), (c, z) \in A \times H$. Dann gilt

$$(a, x) * (b, y) = \begin{cases} (a + b, xy) & x \in N \\ (a - b, xy) & x \in H \setminus N \end{cases},$$
$$(b, y) * (c, z) = \begin{cases} (b + c, yz) & x \in N \\ (b - c, yz) & y \in H \setminus N \end{cases}.$$

Somit ist (unter Verwendung der Assoziativität der Verknüpfungen $\cdot$ und $+$ auf $H$ bzw. $A$):

$$((a, x) * (b, y)) * (c, z) = \begin{cases} (a + b + c, xyz) & x \in N, xy \in N \\ (a + b - c, xyz) & x \in N, xy \in H \setminus N \\ (a - b + c, xyz) & x \in H \setminus N, xy \in N \\ (a - b - c, xyz) & x \in H \setminus N, xy \in H \setminus N \end{cases}$$
$$(a, x) * ((b, y) * (c, z)) = \begin{cases} (a + b + c, xyz) & x \in N, y \in N \\ (a + b - c, xyz) & x \in N, y \in H \setminus N \\ (a - b - c, xyz) & x \in H \setminus N, y \in N \\ (a - b + c, xyz) & x \in H \setminus N, y \in H \setminus N \end{cases}$$

Zusammen mit Teilaufgabe (a) finden wir, dass die Fälle $x \in N, xy \in N \leftrightarrow x \in N, y \in N$, $x \in N, xy \in H \setminus N \leftrightarrow x \in N, y \in H \setminus N$, $x \in H \setminus N, xy \in N \leftrightarrow x \in H \setminus N, y \in H \setminus N, x \in H \setminus N, xy \in H \setminus N \leftrightarrow x \in H \setminus N, y \in N$ zueinander korrespondieren. In jedem der vier Fälle finden wir also $((a, x) * (b, y)) * (c, z) = (a, x) * ((b, y) * (c, z))$ und haben damit die Assoziativität von $* : (A \times H) \times (A \times H) \to A \times H$ nachgewiesen.
(c) Wir sollen nun zeigen, dass für alle $x \in H \setminus N$ von Ordnung 2 gilt, dass $(a, x)$ für beliebiges $a \in A$ ebenfalls Ordnung 2 hat. Zunächst gilt $x^2 = e_H \in N$ aus der Voraussetzung an die Ordnung von $x$. Sei nun $a \in A$ beliebig. Dann gilt $(a, x) \neq (0, e_H)$, denn $x \in H \setminus N$ aber $e_H \in N$. Somit ist die Ordnung von $(a, x)$ strikt größer als 1. Nun gilt $(a, x) * (a, x) = (a - a, x^2) = (0, e_H)$, denn $x \in H \setminus N$ nach Voraussetzung. Da 2 die kleinste natürliche Zahl $n$ ist, sodass $(a, x)^n = (0, e_H)$, ist

bereits $\mathrm{ord}_{A\times H}((a,x)) = 2$.
(d) Wir suchen eine Gruppe $G$ der Ordnung 42, sodass es in $G$ kein Element der Ordnung 6 und kein Element der Ordnung 14 gibt. Wir setzen $G$ in der Form $A \times H$ mit $A = \mathbb{Z}/21\mathbb{Z}$ und $H = \mathbb{Z}/2\mathbb{Z}$ an und wählen zusätzlich $N = \{\bar{0}\}$ als Normalteiler. Sei nun $(a,x) \in A \times H$ und $x \in N$. Dann gilt für alle $n \in \mathbb{N}$, dass $(a,x)^n = (n \cdot a, x^n)$ falls $x \neq 1$ und $\mathrm{ord}(a,x) = 2$ falls $x = 1 \notin N$. Damit sind nur die folgenden Ordnungen möglich: $\mathrm{ord}((a,x)) = 2$, falls $x = 1$, nach Teil (c) und $\mathrm{ord}(a,x) \in \{1,3,7,21\}$ falls $x = 0$. Damit haben wir die Anforderungen an $G$ hinsichtlich der Nicht-Existenz von Elementen bestimmter Ordnung implementiert. Es gilt zudem $|A \times H| = |A||H| = 21 \cdot 2 = 42$, sodass $G = A \times H$ auch von der richtigen Gruppenordnung ist. □

**Aufgabe 132 (H16T2A2)** Seien $A, B$ zwei abelsche Gruppen und $\phi : B \to \mathrm{Aut}(A)$ ein Gruppenhomomorphismus. Das innere semidirekte Produkt $A \rtimes_\phi B$ ist definiert als $A \rtimes_\phi B = \{(a,b) | a \in A, b \in B\}$ mit der Verknüpfung $(a_1,b_1) * (a_2,b_2) = (a_1\phi(b_1)(a_2), b_1b_2)$.
(a) Wir zeigen, dass $A \rtimes_\phi B$ genau dann abelsch ist, wenn $\phi(b) = \mathrm{id}_A$ für alle $b \in B$. "⇒": Sei vorausgesetzt, dass $\phi(b) = \mathrm{id}_A$ für alle $b \in B$. Seien $(a_1,b_2),(a_2,b_2) \in A \times B$ beliebig. Dann gilt $(a_1,b_1) * (a_2,b_2) = (a_1\phi(b_1)(a_2), b_1b_2) = (a_1a_2, b_1b_2) = (a_2a_1, b_2b_1) = (a_2\phi(b_2)(a_1), b_2b_1) = (a_2,b_2) * (a_1,b_1)$. "⇐": Setzen wir umgekehrt voraus, dass $A \rtimes_\phi B$ abelsch ist. Dann gilt $(a_1,0) * (a_2,b) = (a_2,b) * (a_1,0)$ für $a_1, a_2 \in A$ und $b \in B$. Explizit haben wir $(a_1\phi(0)(a_2), b) = (a_1a_2, b) = (a_2a_1, b) = (a_2\phi(b)(a_1), b)$. Insbesondere gilt in der ersten Komponente $a_2a_1 = a_2\phi(b)(a_1)$. Multiplikation mit $a_2^{-1}$ liefert, dass $a_1 = \phi(b)(a_1)$ für beliebiges $a_1 \in A$ und $b \in B$. Das bedeutet, dass $\phi(b) = \mathrm{id}_A$ für alle $b \in B$.
(b) Wir sollen eine nicht-abelsche Gruppe der Ordnung 2015 konstruieren. Es gilt $2015 = 5 \cdot 403 = 5 \cdot 13 \cdot 31$. Wir versuchen zunächst eine nicht-abelsche Gruppe der Ordnung $5 \cdot 31 = 155$ zu konstruieren, indem wir ein semidirektes äußeres Produkt von den zyklischen Gruppen $\mathbb{Z}/5\mathbb{Z}$ und $\mathbb{Z}/31\mathbb{Z}$ angeben. Es ist $\mathrm{Aut}(\mathbb{Z}/31\mathbb{Z}) \simeq (\mathbb{Z}/31\mathbb{Z})^\times \simeq \mathbb{Z}/30\mathbb{Z}$, weil 31 eine Primzahl ist. Nun ist durch $\phi(1) = 6$ ein nichttrivialer Homomorphismus $\phi : \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/30\mathbb{Z}$ erklärt, denn 6 hat Ordnung 5 in $\mathbb{Z}/30\mathbb{Z}$. Vermöge der oben angeführten Isomorphien haben wir somit einen nichttrivialen Homomorphismus $\psi : \mathbb{Z}/5\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/31\mathbb{Z})$ gefunden. Teil (a) liefert nun, dass $\mathbb{Z}/31\mathbb{Z} \rtimes_\psi \mathbb{Z}/5\mathbb{Z}$ nicht-abelsch ist. Das äußere direkte Produkt $(\mathbb{Z}/31\mathbb{Z} \rtimes_\psi \mathbb{Z}/5\mathbb{Z}) \times \mathbb{Z}/13\mathbb{Z}$ ist ebenfalls nicht-abelsch, denn der erste Faktor ist nicht-abelsch. Da $\{5,13,31\}$ eine Menge paarweise teilerfremder Primzahlen ist, gilt $|(\mathbb{Z}/31\mathbb{Z} \rtimes_\psi \mathbb{Z}/5\mathbb{Z}) \times \mathbb{Z}/13\mathbb{Z}| = 5 \cdot 13 \cdot 31 = 2015$. Damit haben wir eine nicht-abelsche Gruppe der Ordnung 2015 gefunden. □

**Aufgabe 133 (H19T2A4)** □ Sei $S_3$ die symmetrische Gruppe auf $M_3 = \{1,2,3\}$ und $G = S_3 \times S_3$. Zu einem vorgegebenen Primteiler $p$ der Gruppenordnung $|G|$ sei $\nu_p$ die Anzahl der $p$-Sylowgruppen von $G$.
(a) Gesucht ist $\nu_3$. Wir sehen zunächst, dass $|G| = |S_3 \times S_3| = |S_3| \cdot |S_3| = 3! \cdot 3! = 2^2 \cdot 3^2$. In jedem der beiden Faktoren gilt $A_3 \trianglelefteq S_3$, denn $(S_3 : A_3) = 2$. Zudem ist $|A_3| = 3$. Wegen $|S_3| = 6 = 3 \cdot 2$ ist die $A_3$ jeweils eine 3-Sylowgruppe von $S_3$. Eine aus der Vorlesung bekannte Folgerung aus dem zweiten Sylow-Satz besagt, dass ei-

ne $p$-Sylowgruppe einer Gruppe $G$ genau dann Normalteiler von $G$ ist, wenn es zur Primzahl $p$ genau eine $p$-Sylowgruppe gibt. Mithilfe dieses Resultats folgt aus der Normalteilereigenschaft von $A_3$ in $S_3$, dass $A_3$ die einzige 3-Sylowgruppe von $S_3$ ist. Sei nun $H \equiv G_1 \times G_2$ äußeres direktes Produkt der zwei Gruppen $G_1, G_2$. Zudem seien $N_1, N_2$ jeweils Normalteiler von $G_1, G_2$. Wir behaupten, dass $N_1 \times N_2 \trianglelefteq G_1 \times G_2$. Aus der Vorlesung wird als bekannt vorausgesetzt, dass zumindest $N_1 \times N_1 \leq G_1 \times G_2$ gilt. Seien nun $(g_1, g_2) \in G_1 \times G_2$ und $(n_1, n_2) \in N_1 \times N_2$ beliebig. Zu zeigen ist, dass $(g_1, g_2) \cdot (n_1, n_2) \cdot (g_1, g_2)^{-1} \in N_1 \times N_2$, d.h., die notwendige und hinreichende Bedingung dafür, dass $N_1 \times N_2 \trianglelefteq G_1 \times G_2$. Es gilt $(g_1, g_2) \cdot (n_1, n_2) \cdot (g_1, g_2)^{-1} = (g_1, g_2) \cdot (n_1, n_2) \cdot (g_1^{-1}, g_2^{-1}) = (g_1 n_1 g_1^{-1}, g_2 n_2 g_2^{-1})$, wobei jeweils die Eigenschaft von $G_1 \times G_2$ äußeres Produkt zu sein verwendet wurde. Nun gilt infolge $N_1 \trianglelefteq G_1$ und $N_2 \trianglelefteq G_2$, dass $g_1 n_2 g_1^{-1} \in N_1$ und $g_2 n_2 g_2^{-1} \in N_2$, sodass $(g_1 n_1 g_1^{-1}, g_2 n_2 g_2^{-1}) \in N_1 \times N_2$. Damit ist die Normalteilereigenschaft $N_1 \times N_2 \trianglelefteq G_1 \times G_2$ bewiesen. Es folgt im Kontext des zu bearbeitenden Beispiels direkt, dass $A_3 \times A_3 \trianglelefteq S_3 \times S_3$. Wegen $|A_3 \times A_3| = 3^2$ handelt es sich bei $A_3 \times A_3$ um eine 3-Sylowgruppe von $S_3 \times S_3$. Mit der oben zitierten Folgerung aus dem zweiten Sylow-Satz folgt nun, dass $\nu_3 = 1$.
(b) Gesucht sind drei verschiedene 2-Sylowgruppen von $G$, im Zeichen $P, Q, R$, sodass $|P \cap Q| = 1$ und $|P \cap R| > 1$. In der $S_3$ gibt es genau 3 Untergruppen der maximalen 2-Potenzordnung 2, mit anderen Worten 2-Sylowgruppen, nämlich $\langle (1,2) \rangle, \langle (1,3) \rangle$ und $\langle (2,3) \rangle$, wie man leicht mithilfe des dritten Sylow-Satzes prüft. Damit ist $P \equiv \langle (1,2) \rangle \times \langle (1,2) \rangle$ eine Untergruppe von $G$, die die Ordnung $4 = 2^2$ hat und damit 2-Sylowgruppe von $G$ ist. Ebenso sieht man, dass $R = \langle (1,2) \rangle \times \langle (1,3) \rangle$ und $Q = \langle (1,3) \rangle \times \langle (1,3) \rangle$ 2-Sylowgruppen von $G$ sind. Da die Erzeuger der zyklischen Faktoren $\langle (1,2) \rangle$ und $\langle (1,3) \rangle$ verschieden und als Transpositionen von der Ordnung 2 sind, gilt $\langle (1,2) \rangle \cap \langle (1,3) \rangle = \{\mathrm{id}\rangle$ und damit $P \cap Q = \{(\mathrm{id}, \mathrm{id})\}$, also $|P \times Q| = 1$. Zudem ist $P \cap R = \{(\mathrm{id}, \mathrm{id}), ((1,2), \mathrm{id})\}$, also $|P \cap R| = 2 > 1$. Insgesamt haben wir damit 3 2-Sylowgruppen von $G$ mit der angegebenen Eigenschaft gefunden. □

**Aufgabe 134 (H18T3A2(b))** Zu zeigen ist, dass $A_3 \times A_3$ die einzige 3-Sylowgruppe von $S_3 \times S_3$ ist. Laut einer Folgerung aus dem zweiten Sylowschen Satz, angewendet auf die vorliegende Situation, ist die Eigenschaft $A_3 \times A_3 \trianglelefteq S_3 \times S_3$ äquivalent dazu, dass $A_3 \times A_3$ die einzige 3-Sylowgruppe von $S_3 \times S_3$ ist. Da $A_3 \trianglelefteq S_3$ gilt auch $A_3 \times A_3 \trianglelefteq S_3 \times S_3$. Damit folgt die Behauptung. □

**Aufgabe 135** Sei $\mathbb{N} \ni n$ und $n \geq 3$. Zu zeigen ist, dass $D_n$ isomorph zu einer äußeren semidirekten Produkt zweier zyklischer Gruppen ist. Definiere zunächst $C_n \equiv \mathbb{Z}/n\mathbb{Z}$ und $C_2 = \mathbb{Z}/2\mathbb{Z}$ aus Notationsgründen. Wegen $n \geq 3$ ist $\Phi(n) \geq 2$ und gerade, wobei $\Phi$ die Eulersche $\Phi$-Funktion bezeichnet. Sei $\alpha : C_n^\times \to \mathrm{Aut}(C_n)$ der aus der Vorlesung bekannte, eindeutige Isomorphismus, der die Einheitengruppe $C_n^\times$ auf die Automorphismengruppe von $C_n$ abbildet. Wegen $C_n^\times \simeq C_{\Phi(n)}$ lässt sich $\alpha$ durch Komposition in einen Isomorphismus $\beta : C_{\Phi(n)} \to \mathrm{Aut}(\Phi(n))$ überführen. Durch die Wahl $\bar{1} \mapsto \Phi(n)/2$ erhalten wir einen nicht-trivialen Homomorphismus $\phi : C_2 \to C_{\Phi(n)}$, aus dem wir durch Komposition wiederum den nicht-trivialen Homomorphismus $\psi : C_2 \to \mathrm{Aut}(C_n)$ gewinnen, sodass $\bar{1} \mapsto \chi$, wobei $\chi^2 = \mathrm{id}_{C_n}$ aber $\chi \neq \mathrm{id}_{C_n}$. Wir setzen also $\chi(a) = -a$ für alle $a \in C_n$. Damit ist $C_n \rtimes_\psi C_2$ eine nicht-

abelsche Gruppe, denn $\psi$ ist nicht-trivial. Als semidirektes Produkt hat $C_n \rtimes_\psi C_2$ zudem die Ordnung $|C_n \rtimes_\psi C_2| = 2n = |D_n|$, sodass die geforderte Isomorphie von $D_n$ zu $C_n \rtimes_\psi C_2$ zumindest nicht von Vornherein ausgeschlossen ist. Laut Vorlesung ist eine Gruppe $G$ genau dann isomorph zu $D_n$, wenn es Elemente $\tau, \sigma \in G$ gibt, sodass $\operatorname{ord}(\sigma) = n$, $\operatorname{ord}(\tau) = 2$ und $\sigma\tau\sigma\tau = e_G$. Es ist $(0,1) \in C_n \rtimes_\psi C_2$ von der Ordnung 2, denn $(0,1) \neq (0,0)$ und $(0,1) *_\psi (0,1) = (0, 1+1) = (0,0)$. Für $(1,0) \in C_n \rtimes_\psi C_2$ behaupten wir, dass $n(1,0) = (n,0)$ für alle $n \in \mathbb{N}$. In der Tat gilt $1 \cdot (1,0) = (1,0) = (1 \cdot 1, 0)$. Sei die Behauptung für festes $n$ vorausgesetzt, dann gilt $(n+1)(1,0) = n(1,0) *_\psi (1,0) = (n,0) *_\psi (1,0) = (n + \psi(0)(1), 0+0) = (n + \mathrm{id}_{C_n}(1), 0) = (n+1, 0) = ((n+1) \cdot 1, 0)$. Damit ist der Induktionsbeweis abgeschlossen. Damit folgt, dass, in $C_n \rtimes_\psi C_2$, $\operatorname{ord}((1,0)) = n \Leftrightarrow \operatorname{ord}(1) = 0$ in $C_n$. Letzteres ist wahr, denn $1 \in C_n$ ist Erzeuger dieser Gruppe. Wir setzen nun $\sigma = (1,0)$ und $\tau = (0,1)$. Dann haben $\sigma$ und $\tau$ die gewünschten Ordnung und es gilt $\sigma *_\psi \tau = (1,0) *_\psi (0,1) = (1,1)$. Unter Verwendung der Assoziativität von $*_\psi$ gilt $\sigma *_\psi \tau *_\psi \sigma *_\psi \tau = (\sigma *_\psi \tau)^2 = (1,1) *_\psi (1,1) = (1 + \psi(1)(1), 1+1) = (1 + \chi(1), 0) = (\chi(\chi(1)+1), 0) = (0,0)$ mit der Wahl von $\chi$ von oben. Damit haben wir gezeigt, dass $C_n \rtimes_\psi C_2 \simeq D_n$. □

**Aufgabe 136 (F13T3A1)** Wir sollen eine nicht-abelsche Gruppe der Ordnung 2013 konstruieren. Die Quersumme von 2013 ist durch 3 dividierbar, sodass 2013 selbst durch 3 teilbar ist. Es ist $3 \cdot 671$. Ferner ist $671 = 660 + 11 = 60 \cdot 11 + 11$, sodass $2013 = 11 \cdot 61 \cdot 3$ in Primfaktorzerlegung. Seien $C_k = \mathbb{Z}/k\mathbb{Z}$ für $k \in \mathbb{N}$. Wir versuchen aus $C_3$ und $C_{61}$ zunächst eine nicht-abelsche Gruppe mithilfe des äußeren semidirekten Produkts zu konstruieren. Dazu benötigen wir einen nicht-trivialen Homomorphismen $\psi : C_3 \to \mathrm{Aut}(C_{61})$. Da 61 Primzahl ist, liefert ein bekanntes Resultat zu den Automorphismengruppen zyklischer Gruppen von Primzahlordnung, dass $\mathrm{Aut}(C_{61}) \simeq C_{\Phi(61)}$, wobei $\Phi$ die Eulersche $\Phi$-Funktion ist. Wegen $\Phi(61) = 60$ finden wir $\mathrm{Aut}(C_{61}) \simeq C_{60}$ und bezeichnen den Isomorphismus dazu mit $\alpha$. Durch $\bar{1} \mapsto \bar{20}$ ist ein nicht-trivialer Homomorphismus $\phi : C_3 \to C_{60}$ eindeutig bestimmt. Den gesuchten Homomorphismus $\psi$ erhalten wir durch $\psi := \alpha^{-1} \circ \phi$. Wegen der Automorphismeneigenschaft von $\alpha$ ist $\psi$ wohldefiniert. Da $\phi(\bar{1}) \neq \bar{0}$ ist mit $\phi$ auch $\psi$ nicht-trivial. Laut Vorlesung ist dann $C_{61} \rtimes_\psi C_3$ eine nicht-abelsche Gruppe, für deren Ordnung gilt $|C_{61} \rtimes_\psi C_3| = |C_{61}||C_3| = 61 \cdot 3 = 183$. Indem wir nun das äußere direkte Produkt von $C_{61} \rtimes_\psi C_3$ und $C_{11}$ betrachten, d.h., die Gruppe $G = (C_{61} \rtimes_\psi C_3) \times C_{11}$ setzen, erhalten wir eine Gruppe der Ordnung $|G| = |C_{61} \rtimes_\psi C_3||C_{11}| = 183 \cdot 11 = 2013$, d.h., der gewünschten Ordnung. Da der erste Faktor im äußeren direkten Produkt nicht-abelsch ist, ist auch $G$ nicht-abelsch. Somit ist $G = (C_{61} \rtimes_\psi C_3) \times C_{11}$ mit dem Homomorphismus $\psi : C_3 \to \mathrm{Aut}(C_{61})$ nach oben eine nicht-abelsche Gruppe der gesuchten Gruppenordnung. □

**Aufgabe 137** Wir sollen eine nicht-abelsche Gruppe der Ordnung 2020 konstruieren, die nicht isomorph zu $D_{1010}$ ist. Es gilt $2020 = 4 \cdot 5 \cdot 101 = 2^2 \cdot 5 \cdot 101$ in Primfaktorzerlegung. Für $k \in \mathbb{N}$ notieren wir die zyklischen Gruppen $\mathbb{Z}/k\mathbb{Z}$ als $C_k$. Wir versuchen zunächst aus $C_5$ und $C_{101}$ eine nicht-abelsche Gruppe der Ordnung 505 zu konstruieren. Dazu suchen wir einen nicht-trivialen Gruppenhomomorphismus $\psi : C_5 \to \mathrm{Aut}(C_{101})$. Da 101 prim ist, liefert uns ein bekanntes Resultat zur

Struktur der Automorphismengruppen zyklischer Gruppen, dass es einen eindeutigen Isomorphismus $\alpha : C_{\Phi(101)=100} \to \mathrm{Aut}(C_{101})$ gibt. Damit reduziert sich die Suche auf das Auffinden eines nicht-trivialen Gruppenhomomorphismus $\phi : C_5 \to C_{100}$. Dieser ist durch Angabe des Bilds des Erzeugers von $C_5$ bereits eindeutig festgelegt. Wir setzen $\phi(\bar{1}) = \bar{20}$. Es gilt $5 \cdot \bar{20} = \bar{100} = \bar{0}$ in $C_{100}$ und $1 \cdot \bar{20} = \bar{20} \neq \bar{0}$, $2 \cdot \bar{20} = \bar{40} \neq \bar{0}$, $3 \cdot \bar{20} = \bar{60} \neq \bar{0}$ und $4 \cdot \bar{20} = \bar{80} \neq \bar{0}$. Damit ist auch $\bar{20}$ von der Ordnung 5 in $C_{100}$, der Homomorphismus $\phi$ also wohldefiniert. Durch Komposition von $\phi$ und $\alpha$ zu $\psi = \alpha \circ \phi$ erhalten wir nun einen nicht-trivialen Homomorphismus $\psi : C_5 \to \mathrm{Aut}(C_{101})$. Die Homomorphismeneigenschaft ist hierbei klar, denn wohldefinierte Kompositionen von Gruppenhomomorphismen sind selbst wieder Gruppenhomomorphismen laut Vorlesung. Die Nicht-Trivialität folgt daraus, dass $\bar{1}$ auf ein Element $\chi \in \mathrm{Aut}(C_{101})$ von der Ordnung 5 abgebildet wird. Somit können wir die Gruppe $H := C_{101} \rtimes_\psi C_5$ definieren, die wegen $|H| = |C_{101}||C_5| = 505$ die Ordnung 505 hat, und die zudem wegen der Nicht-Trivialität von $\psi$ laut Vorlesung nicht-abelsch ist. Indem wir nun das äußere direkte Produkt $G := C_4 \times H$ betrachten, haben wir eine Gruppe der Ordnung $|G| = 4 \cdot 505 = 2020$ gefunden. Da $H$ nicht-abelscher Faktor im äußeren direkten Produkt ist, ist auch $G$ nicht-abelsch. Wir behaupten, dass $G$ nicht-isomorph zu $D_{1010}$ ist. Laut Vorlesung ist eine Gruppe $X$ der Ordnung 2020 genau dann isomorph zu $D_{2020}$, wenn es $\sigma, \tau \in X$ gibt, sodass $\mathrm{ord}(\sigma) = 1010$ und $\mathrm{ord}(\tau) = 2$ sowie $\sigma\tau\sigma\tau = e_X$ gilt. Insbesondere gibt es also in $X$ dann nur Elemente der Ordnung $k$, wobei $k|1010$. Angenommen, $G \simeq D_{1010}$. Dann ist $(1, 0, 0) \in G$ ein Element der Ordnung 4. Da aber $4 \not| 1010$ haben wir einen Widerspruch dazu, dass auch $(1, 0, 0)$ von einer Ordnung $k$ ist, die 1010 teilt. Somit war die Annahme falsch und es gilt $G \not\simeq D_{1010}$. □

**Aufgabe 138 (F04T2A1)** Gesucht ist eine Untergruppe der Ordnung 21 von $S_7$. Es gilt $21 = 3 \cdot 7$. Sei $\sigma = (1234567) \in S_7$. Dann ist $\langle\sigma\rangle \leq S_7$ eine Untergruppe der Ordnung 7. Wir versuchen nun ein geeignetes Element $\tau \in S_7$ der Ordnung 3 zu finden, sodass $\langle\sigma\rangle \ni \chi = \tau\sigma\tau^{-1}$. Da $\sigma \neq \mathrm{id}$ scheidet id als Wahl für $\chi$ aus. Da ferner $\mathrm{ggT}(3, 7) = 1$, scheidet auch $\chi = \sigma$ aus. Denn ansonsten wäre $\sigma\tau = \tau\sigma$, also $\langle\sigma, \tau\rangle$ abelsch. Da $\langle\tau\rangle, \langle\sigma\rangle \leq \langle\sigma, \tau\rangle$ Untergruppen von verschiedener Primzahlordnung zu einer abelschen Gruppe sind, wäre $\langle\sigma, \tau\rangle \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/\mathbb{Z} \simeq \mathbb{Z}/21\mathbb{Z}$, wobei letzteres durch den Chinesischen Restsatz für Gruppen bedingt ist. Aber in $S_7$ kann es maximal Elemente der Ordnung 12 geben, wie man leicht anhand der disjunkten Zykeldarstellung eines beliebigen Elements der $S_7$ verfiziert. Somit haben wir einen Widerspruch. Wir setzen also $\sigma^2 = \tau\sigma\tau^{-1} = (\tau(1), \tau(2), \tau(3), \tau(4), \tau(5), \tau(6), \tau(7))$. Es gilt aber $(1234567)(1234567) = (1357246)$. Setze nun $\tau = (235)(647)$. Dann hat $\tau$ als Produkt zweier 3-Zykel mit disjunktem Träger tatsächlich Ordnung 3 und es gilt $(\tau(1), \tau(2), \tau(3), \tau(4), \tau(5), \tau(6), \tau(7)) = (1357246)$. Wir betrachten nun $H = \langle\sigma, \tau\rangle$. Offenbar gilt $\langle\tau\rangle, \langle\sigma\rangle \leq H$. Wegen $\mathrm{ggT}(3, 7) = 1$ gilt auch $\langle\tau\rangle \cap \langle\sigma\rangle = \{\mathrm{id}\rangle$. Wir zeigen, dass $\langle\sigma\rangle \trianglelefteq H$. Dazu genügt es, zu zeigen, dass $\sigma\langle\sigma\rangle\sigma^{-1} \subseteq \langle\sigma\rangle$ und $\tau\langle\sigma\rangle\tau^{-1} \subseteq \langle\sigma\rangle$. Da $\langle\sigma\rangle$ zyklisch ist, reicht es aus, dass $\sigma^{-1}\sigma\sigma \in \langle\sigma\rangle$ und $\tau\sigma\tau^{-1} \in \langle\sigma\rangle$. Ersteres gilt offensichtlicherweise, das zweiteres gilt nach Wahl von $\tau$. Insgesamt haben wir $\langle\sigma\rangle \trianglelefteq H$ nachgewiesen. Somit ist das Komplexprodukt $\langle\sigma\rangle\langle\tau\rangle$ zumindest inneres semidirektes Produkt und als solches eine Untergruppe von $H$ und von der Ordnung $21 = 7 \cdot 3 = |\langle\sigma\rangle| \cdot |\langle\tau\rangle|$. Da $H$ selbst Untergruppe von $S_7$ ist, ist auch

$G := \langle\sigma\rangle\langle\tau\rangle$ eine Untergruppe von $S_7$ mit der geforderten Ordnung. □

**Aufgabe 139 (H16T2A1)** Sei $\mathbb{H} = \{z \in \mathbb{C} | \Im[z] > 0\}$ die Menge aller komplexen Zahlen aus der oberen komplexen Halbebene. Durch $\circ : \mathrm{SL}_2(\mathbb{R}) \times \mathbb{H} \to \mathbb{H}, (A, z) \to (az + b)/(cz + d)$ ist eine Gruppenoperation erklärt, wobei

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \tag{174}$$

(a) Wir sollen die Bahnen der Operation angeben. Hierzu betrachten wir zunächst die Bahn des Elements $z = i$ und evaluieren ($a \in \mathbb{R}^\times$, $b \in \mathbb{R}$)

$$A \circ z = \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \circ i = \frac{ai + b}{a^{-1}} = ba + a^2 i. \tag{175}$$

Wir behaupten, dass $\mathbb{H} = \{z = ba + a^2 i \in \mathbb{C} | b \in \mathbb{R}, a \in \mathbb{R} \setminus \{0\}\} =: M$. Zu "$\supseteq$". Seien $a \in \mathbb{R} \setminus \{0\}$ und $b \in \mathbb{R}$ beliebig vorgegeben. Dann gilt $z = ab + a^2 i \in \mathbb{C}$ mit $\Im[z] = a^2 > 0$. Also ist $z \in \mathbb{H}$. Zu "$\subseteq$". Sei umgekehrt $z \in \mathbb{H}$ vorgegeben. Dann gibt es $u \in \mathbb{R}$ und $v \in \mathbb{R}^+$, sodass $z = u + iv$. Wir definieren $a \equiv \sqrt{v} > 0$ und $b = u/\sqrt{v} \in \mathbb{R}$. Es gilt $ab + a^2 i = u + iv = z$. Somit ist $z \in M$. Damit haben wir gezeigt, dass sich vermöge der Operation mit einer geeigneten Matrix $A \in \mathrm{SL}_2(\mathbb{R})$ in oberer Dreiecksgestalt auf $i \in \mathbb{H}$ jedes $Z \in \mathbb{H}$ erhalten lässt. Damit ist $\mathrm{SL}_2(\mathbb{R})(i) = \mathbb{H}$. Aus der Vorlesung ist bekannt, dass eine Operation einer Gruppe auf einer Menge $X$ bereits dann transitiv ist, wenn es ein Element aus $X$ gibt, dessen Bahn bereits ganz $X$ ist. Somit erhalten wir, dass $\circ$ eine transitive Operation ist. Nach Definition bedeutet das, dass es genau eine Bahn der Operation $\circ$ gibt, diese ist dann $\mathbb{H}$.
(b) Wir sollen nun den Stabilisator des Elements $i \in \mathbb{H}$ in $G \equiv \mathrm{SL}_2(\mathbb{R})$ bzgl. $\circ$ bestimmen. Für $A \in G$ gilt: $A \in G_i \Leftrightarrow A \circ i = i$. In der eingangs vorgestellten Notation bedeutet das ausgeschrieben

$$i = \frac{ai + b}{ci + d} \Rightarrow i(ci + d) = ai + b \Leftrightarrow -c + id = b + ia. \tag{176}$$

Da $a, b, c, d$ insbesondere reell sind, können wir den Real- und Imaginärteil der letzten Gleichung getrennt auswerten. Das liefert $-c = b$ und $d = a$. Die Bedingung, dass $\det(A) = 1$ übersetzt sich in $\det(A) = ad - bc = a^2 + b^2 = 1$. Somit ist

$$G_i = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} | a, b \in \mathbb{R} : a^2 + b^2 = 1 \right\}. \tag{177}$$

Indem wir $a = \cos(\psi)$, $b = \sin(\psi)$ für ein $\psi \in [0, 2\pi)$ schreiben, sehen wir, dass $G_i$ gerade die Drehgruppe $\mathrm{SO}_2(\mathbb{R})$ ist, die aus den orientierungserhaltenden Rotation um den Ursprung der komplexen Zahlenebene im Winkel $\psi$ besteht. □

**Aufgabe 140** Sei $\mathbb{H} = \{z \in \mathbb{C} | \Im[z] > 0\}$ die Menge aller komplexen Zahlen aus der oberen komplexen Halbebene. Durch $\circ : \mathrm{SL}_2(\mathbb{Z}) \times \mathbb{H} \to \mathbb{H}, (A, z) \to (az + b)/(cz + d)$ ist eine Gruppenoperation erklärt, wobei

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \tag{178}$$

Wir zeigen, dass es unendlich viele Bahnen gibt. Angenommen, es gibt nur endlich viele Bahnen $B_1, ..., B_n$. Da die Zuordnung $G \to B_k, g \mapsto g \circ z$ für alle $k \in \{1, ..., n\}$ surjektiv ist, ist mit $G = \mathrm{SL}_2(\mathbb{Z})$ auch $B_k$ abzählbar. Da die Bahnen der Operation eine Zerlegung von $\mathbb{H}$ bilden, gilt

$$M := \bigcup_{k=1}^{n} B_k = \mathbb{H}. \tag{179}$$

Da $\mathbb{R} \simeq \mathbb{R} \oplus i \cdot 1 \subseteq \mathbb{H}$, d.h., $\mathbb{H}$ eine überabzählbare Menge beinhaltet, haben wir einen Widerspruch: Denn die Gleichheit implizierte, dass es eine bijektive Abbildung $\alpha : \mathbb{N} \to \mathbb{H}$ gibt. Dann wäre aber $\beta : \alpha^{-1}(\mathbb{R} \oplus i \cdot 1) \to \mathbb{R} \oplus i \cdot 1$ eine bijektive Abbildung als surjektive Einschränkung der bijektiven Abbildung, die sich vermöge $\mathbb{R} \oplus i \cdot 1 \simeq \mathbb{R}$, zu einer bijektiven Abbildung $\gamma : \alpha^{-1}(\mathbb{R} \oplus i \cdot 1) \subseteq \mathbb{N} \to \mathbb{R}$ umwandeln lässt. Da aber $\mathbb{R}$ überabzählbar ist, existiert eine solche Abbildung nicht. Damit war die Annahme, es gäbe nur endlich viele Bahnen, falsch, und es gibt unendlich, genauer (ohne Beweis hier) unendlich überabzählbar viele Bahnen der Operation $\circ$. □

**Aufgabe 141** Sei $\mathcal{U} \equiv \{U \leq \mathbb{R}^2 | \dim_{\mathbb{R}}(U) = 1\}$ die Menge der eindimensionalen Untervektorräume von $\mathbb{R}^2$ und $G \equiv \mathrm{GL}_2(\mathbb{R})$. Wir definieren $\circ : G \times \mathcal{U} \to \mathcal{U}, (A, U) \mapsto A \circ U \equiv \{Au | u \in U\}$.
(a) Wir zeigen, dass $\circ$ als Abbildung wohldefiniert ist. Sei dazu $U \in \mathcal{U}$ beliebig. Da $\dim_{\mathbb{R}}(U) = 1$, gibt es ein $u \in U \setminus \{0_{\mathbb{R}^2}\}$ mit der Eigenschaft, dass $\mathrm{lin}_{\mathbb{R}}(u) = U$. Da $A \in \mathrm{GL}_2(\mathbb{R})$ gilt auch $Au = v \neq 0_{\mathbb{R}^2}$. Ansonsten wäre $\dim \ker(A) = 1 > 0$ im Widerspruch dazu, dass durch $\mathbb{R}^2 \to \mathbb{R}^2, x \mapsto Ax$ eine bijektive lineare Abbildung erklärt ist. Nun gilt $AU = \{Au' | u' \in \mathrm{lin}(u)\} = \{A(\lambda u) | \lambda \in \mathbb{R}\} = \{\lambda(Au) | \lambda \in \mathbb{R}\} = \{\lambda v | \lambda \in \mathbb{R}\} = \mathrm{lin}_{\mathbb{R}}(v)$. Letzteres ist ein eindimensionaler Untervektorraum von $\mathbb{R}^2$, $\mathrm{lin}_{\mathbb{R}}(u) \in \mathcal{U}$. Beliebigkeit von $U \in \mathcal{U}$ impliziert nun die Wohldefiniertheit der Abbildung $\circ$. Wir zeigen nun, dass es sich bei $\circ$ um eine Gruppenoperation handelt. Zunächst ist das neutrale Element von $G$ die Einheitsmatrix $E_2$. Es gilt für beliebiges $U \in \mathcal{U}$, dass $E_2 \circ U = E_2 U = \{E_2 u | u \in U\} = \{u | u \in U\} = U$. Seien zudem $A, B \in G$ und $U \in \mathcal{U}$ beliebig. Dann ist $A \circ (B \circ U) = A \circ (BU) = A \circ \{Bu | u \in U\} = A\{Bu | u \in U\} = \{ABu | u \in U\} = \{(A \cdot B)u | u \in U\} = (A \cdot B)U = (A \cdot B) \circ U$, wobei auch die Verträglichkeit der Gruppenoperation $\circ$ mit der Gruppenverknüpfung $\circ$ (Matrixmultiplikation) auf $G$ nachgewiesen ist. Damit haben wir gezeigt, dass es sich bei $\circ$ um eine Gruppenoperation handelt.
(b) Wir zeigen, dass $\circ$ transitiv ist. Dazu reicht es aus, zu zeigen, dass es ein $U \in \mathcal{U}$ gibt, sodass $G(U) = \mathcal{U}$. Wir wählen $U = \mathrm{lin}_{\mathbb{R}}(\hat{e}_1)$, wobei $\hat{e}_1 = (1, 0)^T \in \mathbb{R}^2$. Zudem sei $\mathcal{U} \ni U = \mathrm{lin}_{\mathbb{R}}(u)$ mit einem Vektor $u \neq 0_{\mathbb{R}^2}$. Wir wählen nun die Matrix $A$ dergestalt, dass $A = (u, v)$, wobei $v \in \mathbb{R}^2 \setminus U$ beliebig ist. Dann ist $\{u, v\}$ eine Menge linear unabhängiger Vektoren, sodass $A \in \mathrm{GL}_2(\mathbb{R})$, da die Spaltenvektoren von $A$ linear unabhängig sind. Zudem gilt $A\hat{e}_1 = u$. Analog zum Beweis der Wohldefiniertheit von $\circ$ schließen wir, dass $A \circ \mathrm{lin}_{\mathbb{R}}(\hat{e}_1) = \mathrm{lin}_{\mathbb{R}}(u) = U$. Beliebigkeit von $U \in \mathcal{U}$ impliziert, dass $G(\mathrm{lin}_{\mathbb{R}}(\hat{e}_1)) = \mathcal{U}$. Damit ist $\circ$ transitiv.
(c) Seien $U_1 \equiv \mathrm{lin}_{\mathbb{R}}(\hat{e}_1)$ und $U_2 \equiv \mathrm{lin}_{\mathbb{R}}(\hat{e}_2)$. Wir bestimmen die Stabilisatoren $G_{U_1}$ und $G_{U_2}$. Zu $G_{U_1}$. Es ist $A \in G_{U_1} \Leftrightarrow A \circ U_1 = U_1 \Leftrightarrow A\hat{e}_1 = \lambda \hat{e}_1$, wo $\lambda \in \mathbb{R}^\times$. Damit ist $A = (\lambda \hat{e}_1, v)$, wo $v \in \mathbb{R}^2 \setminus U_1$. Analog sehen wir, dass $A \in G_{U_2} \Leftrightarrow A \circ U_2 = U_2 \Leftrightarrow$

$A\hat{e}_2 = \lambda\hat{e}_2$ mit $\lambda \in \mathbb{R}^\times$. Somit ist $A = (v, \lambda\hat{e}_2)$, wo $v \in \mathbb{R}^2 \setminus U_2$. Explizit finden wir die gesuchten Stabilisatoren also als

$$G_{U_1} = \left\{ \begin{pmatrix} \lambda & a \\ 0 & c \end{pmatrix} | a \in \mathbb{R}, \lambda, c \in \mathbb{R}^\times \right\}, \tag{180}$$

$$G_{U_2} = \left\{ \begin{pmatrix} c & 0 \\ a & \lambda \end{pmatrix} | a \in \mathbb{R}, \lambda, c \in \mathbb{R}^\times \right\}. \tag{181}$$

Das sind die oberen bzw. unteren Dreiecksmatrizen mit nicht-verschwindender Determinante, die aus der linearen Algebra bereits als Untergruppen der $\mathrm{GL}_2(\mathbb{R})$ bekannt sind. □

**Aufgabe 142** (a) Wir zeigen, dass eine $p$-Gruppe $G$ ein nicht-triviales Zentrum $Z(G)$ hat. Sei $|G| = p^d$ mit $d \in \mathbb{N}$. Ohne Einschränkung ist $d > 1$, denn für den Fall, dass $d = 1$ ist $G$ als Gruppe von Primzahlordnung bereits zyklisch und somit abelsch, sodass $Z(G) = G$. Sei also $d > 1$. Wir betrachten die Operation der Gruppe $G$ auf sich selbst durch Konjugation. Dann liefert die Klassengleichung

$$|G| = |Z(G)| + \sum_{g \in R} (G : C_g(G), \tag{182}$$

wobei $R$ ein Repräsentantensystem der Bahnen der Länge $> 1$ ist. $C_g(G)$ bezeichnet den Zentralisator von $g \in G$ in $G$. Da $C_g(R) < p^2$ aber $|C_g(G)||G|$ nach dem Satz von Lagrange, kann nur $(G : C_g(G)) \in \{p, p^2, ..., p^d\}$ für alle $g \in R$. Der Fall, dass $(G : C_g(G)) = p^d$ ist aber ausgeschlossen, denn dann wäre $|R| = 1$ und $|Z(G)| \geq 1$ wegen $e \in Z(G)$, sodass die Klassengleichung den Widerspruch $p^d \geq 1 + p^d$ liefert. Andererseits können wir die Klassengleichung modulo $p$ reduzieren. Dann ist $|Z(G)| \equiv 0 \bmod(p)$, woraus mit $p > 1$ folgt, dass $|Z(G)| > 1$. Damit wissen wir bereits, dass $\{e\} \subsetneq Z(G) \subseteq G$. das Zentrum von $G$ ist somit nicht-trivial.
(b) Wir zeigen, dass Gruppen der Ordnung $p^2$, wo $p$ eine Primzahl ist, abelsch sind. Aus Aufgabenteil (a) ist bereits bekannt, dass eine Gruppe $G$ der Ordnung $p^2$ als $p$-Gruppe ein nicht-triviales Zentrum hat. Falls $Z(G) = G$, dann ist $G$ nach Definition des Zentrums bereits abelsch. Dieser Fall kann im Folgenden unbeachtlich bleiben. Es gilt dann insbesondere $|Z(G)| = p$, sodass $Z(G)$ als Gruppe von Primzahlordnung zyklisch ist, $Z(G) \simeq \mathbb{Z}/p\mathbb{Z}$. Angenommen, es gäbe nun ein $g \in G$, sodass $gh \neq hg$ für ein $h \in G$. Wegen $|G| = p^2$ hat $g$ dann die Ordnung 1 oder $p$, denn $\mathrm{ord}(g) = p^2$ implizierte, dass $G$ zyklisch und damit abelsch wäre. Der Fall, dass $\mathrm{ord}(g) = 1$ ist ebenfalls ausgeschlossen, denn dann ist $g = e_G$ und das Neutralelement vertauscht mit jedem anderen Gruppenelement. Also ist $\mathrm{ord}(g) = p$. Wir betrachten nun die Untergruppe $\langle g \rangle \trianglelefteq G$. Diese kann nur $Z(G) \cap \langle g \rangle = \{e_G\}$ erfüllen, denn ansonsten wäre wegen $Z(G) \cap \langle g \rangle \leq Z(G)$ und $|Z(G)|$ bereits $\langle g \rangle = Z(G)$, was aber $g \in Z(G)$ im Widerspruch zur Wahl von $g$ implizierte. Zudem ist bekannt, dass $Z(G) \trianglelefteq G$. Zusammen mit $\langle g \rangle \leq G$ betrachten wir das innere semi-direkte Produkt $Z(G)\langle g \rangle$. Wir zeigen, dass dieses isomorph zum äußeren direkten Produkt $Z(G) \times \langle g \rangle$ ist. Da $|\langle g \rangle| = p = Z(G)$, sind beide isomorph zu $\mathbb{Z}/p\mathbb{Z}$. Wir zeigen also, dass $\mathbb{Z}/p\mathbb{Z} \cdot \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Wir schließen dazu die Existenz eines nicht-trivialen Homomorphismus $\phi : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ aus. Da ein Element $g$ aus $\mathbb{Z}/p\mathbb{Z}$ entweder Ordnung $p$

oder Ordnung 1 hat, können wir nur $\mathrm{ord}(\phi(g))|\mathrm{ord}(g)$ erreichen, indem wir $g$ auf ein Element der Ordnung 1 in $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ abbilden. Denn letzteres hat Ordnung $p-1 < p$, sodass kein Automorphismus der Ordnung $p$ existiert. Somit ist $\phi(g) = \mathrm{id}_{\mathbb{Z}/p\mathbb{Z}}$ für alle $g \in \mathbb{Z}$. Damit ist aber nach Vorlesung bereits $\mathbb{Z}/p\mathbb{Z} \cdot \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Da letzteres aber abelsch ist, da jeder der beiden Faktoren abelsch ist, haben wir den gesuchten Widerspruch: Bezogen auf das $G$ der Aufgabenstellung bedeutet das $Z(G) = G$, sodass wir ein Element $g$ wie angenommen nicht wählen können. □

**Aufgabe 143 (H13T3A4)** Sei $V = \mathbb{F}_p^n$ und $G \leq \mathrm{GL}_n(\mathbb{F}_p)$ für ein $n \in \mathbb{N}$ dergestalt, dass $|G| = p^e$ für ein $e \in \mathbb{N}$. Zu zeigen ist, dass es ein $v \in \mathbb{F}_p^n$ gibt, sodass $v \neq 0$ und $\gamma \cdot v = v$ für alle $\gamma \in G$. Hierzu bemerken wir, dass $* : G \times V \to V, (\gamma, v) \mapsto \gamma \cdot v$ eine Gruppenoperation ist. Es operiert nämlich die Gruppe der invertierbaren $n \times n$-Matrizen auf die (Spalten-)Vektoren im $n$-dimensionalen $\mathbb{F}_p$-Vektorraum $\mathbb{F}_p^n$ durch Matrixmultiplikation. Wegen Abgeschlossenheit des Körpers $\mathbb{F}_p$ unter Multiplikation ist die Abbildung wohldefiniert. Zudem gilt $E_n * v = v$, für alle $v \in V$, wo $E_n = \mathrm{diag}(1, 1, ..., 1)$ die $n \times n$-Matrix bezeichnet, die nur auf der Diagonale Einträge hat, die jeweils gleich dem Neutralelement von $\mathbb{F}_p^\times$ sind. Diese ist das Neutralelement in $\mathrm{GL}_n(\mathbb{F}_p)$, liegt mithin in $G$. Zudem gilt für $A, B \in G$ und $v \in V$, dass $A * (B * v) = A * (Bv) = A(Bv) = (AB)v = (AB) * v$, sodass die Abbildung $*$ mit der Verknüpfung auf $G$ verträglich ist. Damit ist verifiziert, dass es sich bei $*$ um eine Operation von $G$ auf $V$ handelt. Da $|V| = |\mathbb{F}_p|^n = p^n < \infty$, liefert die Bahnengleichung

$$|V| = |F| + \sum_{v \in R} (G : G_v), \tag{183}$$

wo $R \subseteq V$ ein Repräsentantensystem derjenigen Bahnen ist, die eine Länge $> 1$ haben, und $F$ die Fixpunktmenge der Operation bezeichnet. Offenbar gilt für alle $\gamma \in G$, dass $\gamma \cdot 0_{\mathbb{F}_p^n} = 0_{\mathbb{F}_p^n}$. Damit ist $0_{\mathbb{F}_p^n} \in F$, also $|F| \geq 1$. Wegen $|G(v)| > 1$ für $v \in R$ nach Definition von $R$, ist $|G(v)| = (G : G_v) > 1$ und, genauer nach dem Satz von Lagrange, $(G : G_v) = |G|/|G_v| \in \{p, p^2, ..., p^d\}$, wo $d < \min\{n, e\}$. Reduktion modulo $p$ liefert dann $|F| = 0 \bmod (p)$, was wegen $p \geq 2 > 1$ nur dann geht, wenn es mindestens ein $v \in F$ mit $v \neq 0_{\mathbb{F}_p^n}$ gibt. Nach Definition von $F$ erfüllt dieses $v$ nun die gewünschte Eigenschaft, dass $\gamma \cdot v = v$ für alle $\gamma \in G$. □

**Aufgabe 144 (H12T1A1)** Sei $p$ eine Primzahl und $\mathbb{N} \ni l > 0$ und $q = p^l$.
(a) Wir zeigen zunächst, dass $\mathrm{SL}_2(\mathbb{F}_q)$ die Ordnung $q(q^2 - 1)$ hat. Hierzu beachten wir, dass $\det : \mathrm{GL}_2(\mathbb{F}_q) \to \mathbb{F}_q^\times, A \mapsto \det(A)$ bereits aus der Vorlesung als Gruppenhomomorphismus bekannt ist. Dieser Homomorphismus ist auch surjektiv, denn für jedes $a \in \mathbb{F}_q^\times$ ist die Matrix $A = \mathrm{diag}(a, 1) \in \mathrm{GL}_2(\mathbb{F}_q)$. Zusätzlich gilt $\mathrm{SL}_2(\mathbb{F}_q) = \{A \in \mathrm{GL}_2(\mathbb{F}_q) | \det(A) = 1\} = \ker \det$. Wir bestimmen die Ordnung von $\mathrm{GL}_2(\mathbb{F}_q)$. Es ist $A \in \mathrm{GL}_2(\mathbb{F}_q)$ genau dann, wenn die Spaltenvektoren von $A$ linear unabhängig über $\mathbb{F}_q$ sind. Für den ersten Spaltenvektor haben wir $(q^2 - 1)$ Möglichkeiten (denn er muss vom Nullvektor verschieden sein). Für den zweiten Spaltenvektor haben wir nur noch $q^2 - q$ Möglichkeiten, denn er darf nicht aus der $\mathbb{F}_q$-linearen Hülle des ersten Spaltenvektors gewählt werden, da die Menge aus den

beiden Spaltenvektoren in diesem Fall linear abhängig über $\mathbb{F}_q$ ist. Insgesamt haben wir also $(q^2-1)(q^2-q)$ verschiedene Elemente in $\mathrm{GL}_2(\mathbb{F}_q)$. Zusammen mit $|\mathbb{F}_q^\times| = q-1$ wegen der Körpereigenschaft von $\mathbb{F}_q$ liefert nun der Homomorphiesatz für den surjektiven Gruppenhomomorphismus det, dass

$$\mathbb{F}_q^\times = \mathrm{GL}_2(\mathbb{F}_q)/\mathrm{SL}_2(\mathbb{F}_q). \tag{184}$$

Hierbei haben wir $\ker\det = \mathrm{SL}_2(\mathbb{F}_q)$ von oben bereits verwendet. Da $\mathrm{GL}_2(\mathbb{F}_q)$ insbesondere endlich ist, folgt mit dem Satz von Lagrange $q-1 = (q^2-q)(q^2-1)/|\mathrm{SL}_2(\mathbb{F}_q)|$, was wir zu $|\mathrm{SL}_2(\mathbb{F}_q)| = q(q^2-1)$ umformen.
(b) Für die Untergruppen $N^-$ und $B$ finden wir anhand der Definition jeweils die Ordnungen $|N^-| = q$ und $|B| = (q-1)q$. Da die Anzahl der Linksnebenklassen von $B$ in $G = \mathrm{SL}_2(\mathbb{F}_q)$ gegeben ist durch $|G/B| = (G:B) = |G|/|B|$ nach dem Satz von Lagrange, liefert Einsetzen der Ergebnisse aus (a) und des Ergebnisses für $|B|$ von vorher, dass $|G/B| = q+1$. Im Folgenden sei $\Omega = G/B$.
(c) Wir definieren nun $* : N^- \times \Omega \to \Omega, (\alpha, \beta B) \to \alpha\beta B$. Laut Aufgabenstellung ist das eine Operation. Wir sollen zeigen, dass diese einen Fixpunkt hat. Dazu verwenden wir die Bahnengleichung

$$|\Omega| = |F| + \sum_{x \in R} (N^- : N_x^-), \tag{185}$$

wo $R$ ein Repräsentantensystem all derjenigen Bahnen bezeichnet, deren Länge $> 1$ ist. Es ist $q+1 = |\Omega|$ und $N_x^- \leq N^-$, also $|N_x^-| \,|\, |N^-| = q = p^l$. Zudem $|N^-(x)| = (N^- : N_x^-) \in \{p, p^2, ..., q\}$, denn da $R$ gerade Repräsentantensystem der Bahnen der Länge $> 1$ ist, ist $(N^- : N_x^-) > 1$ für alle $x \in R$. Reduktion modulo $p$ liefert nun $|F| \equiv 1 \bmod(p)$, sodass $F$ zumindest ein Element $\phi B \in \Omega$ enthält. Dieses ist dann (einer) der gesuchte(n) Fixpunkt(e). □

**Aufgabe 145 (F13T1A5)** Sei $M$ die Menge der $3 \times 3$-Matrizen über $\mathbb{C}$ mit charakteristischem Polynom $\chi = (x-1)^3$.
(a) Zu zeigen ist, dass die Gruppe $G = \mathrm{GL}_3(\mathbb{C})$ auf $M$ durch Konjugation operiert. Wir definieren dazu die Abbildung $* : G \times M \to M, (T, A) \mapsto T * A = TAT^{-1}$ und verifizieren die Wohldefiniertheit. Sei dazu $A \in M$, $T \in G$ beliebig und setze $B = TAT^{-1} \in G$. Es gilt $\chi_{TAT^{-1}}(z) = \det(zE_3 - TAT^{-1}) = \det(T(zE_3)T^{-1} - TAT^{-1}) = \det(T)\det(zE_3 - A)\det(T^{-1}) = \det(T)\det(zE_3 - A)\det(T)^{-1} = \det(zE_3 - A) = \chi_A = (z-1)^3$. Mithin ist $\chi_B(z) = (z-1)^3$, also $TAT^{-1} = B \in M$. Damit ist $*$ wohldefiniert. Wir prüfen, dass $*$ eine Gruppenoperation ist. Es gilt nämlich $E_3 * A = E_3 A E_3^{-1} = A$ für alle $A \in M$ und für $T, S \in G$ und $A \in M$ beliebig gilt zudem: $S * (T * A) = S * (TAT^{-1}) = STAT^{-1}S^{-1} = (ST)A(ST)^{-1} = (ST) * A$. Damit handelt es sich bei $*$ in der Tat um eine Gruppenoperation.
(b) Wir sollen nun die Anzahl der Bahnen bestimmen. Da das charakteristische Polynom $\chi_A$ für alle $A \in M$ in Linearfaktoren zerfällt, ist $A$ ähnlich zu einer Matrix $J$ in Jordan-Normalform, die nur den Eigenwert 1 hat. Mit anderen Worten, es existiert ein $T \in G$, sodass $T * A = TAT^{-1} = J$. Hierbei können wir wegen der Eindeutigkeit der Jordan-Normalform (bis auf Reihenfolge der Blöcke) die folgenden Fälle haben. $A$ hat 3 Jordan-Blöcke der Länge 1, $A$ hat einen Jordan-Block der Länge 2 und damit einen der Länge 1 oder $A$ hat einen Jordan-Block der Länge 3. Da $\chi_A$

die dreifache Nullstelle 1 hat und keine weiteren Nullstellen besitzt, ist $A$ ähnlich zu genau einer der folgenden Matrizen:

$$J_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \tag{186}$$

$$J_2 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \tag{187}$$

$$J_3 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}. \tag{188}$$

Aus den obigen Überlegungen sehen wir direkt, dass $R \equiv \{J_1, J_2, J_3\}$ ein Repräsentantensystem der Menge $\mathcal{M}$ der Bahnen der Operation von $G$ auf $M$ ist. Damit gibt es genau 3 Bahnen der Operation. □

**Aufgabe 146** Sei $X \subseteq \mathrm{Mat}_2(\mathbb{R}) =: M$ die Menge aller reellen $2 \times 2$-Matrizen, die ähnlich zu einer Matrix in Jordan-Normalform ist.
(a) Wir geben eine Matrix $A$ in $M \setminus X$ an. Dieses ist dann insbesondere nicht ähnlich zu einer Matrix in Jordan-Normalform. Laut Vorlesung ist das äquivalent dazu, dass $\chi_A$ nicht über $\mathbb{R}$ in Linearfaktoren zerfällt. Für $A \in M$ gegeben durch

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \tag{189}$$

gilt $\chi_A = \det(zE_2 - A) = z^2 + 1$, welches keine reellen Nullstellen besitzt. Folglich ist $A$ nicht ähnlich zu einer Matrix in Jordan-Normalform und es gilt somit $A \in M \setminus X$.
(b) Wir zeigen, dass $* : \mathrm{GL}_2(\mathbb{R}) \times X \to X, (S, A) \mapsto SAS^{-1}$ eine Gruppenoperation ist. Dazu zeigen wir zunächst, dass die Abbildung wohldefiniert ist. Sei $S \in \mathrm{GL}_2(\mathbb{R})$ und $A \in X$. Es gibt ein $T \in \mathrm{GL}_2(\mathbb{R})$, sodass $TAT^{-1} = J$, da $A$ nach Definition von $X$ ähnlich zu einer Matrix in Jordan-Normalform ist. Das können wir zu $A = T^{-1}JT$ umformen. Da $B = SAS^{-1}$ ist $B = ST^{-1}JTS^{-1}$, sodass $(TS^{-1})B(TS^{-1}) = J$. Somit ist auch $B$ ähnlich zu einer Matrix in Jordan-Normalform, also $B \in X$. Wir zeigen nun, dass es sich bei $*$ um eine Operation von $G := \mathrm{GL}_2(\mathbb{R})$ auf $X$ handelt. Es gilt nämlich, dass $E_2 * A = E_2 A E_2^{-1} = A$ für alle $A \in X$. Zudem gilt für $T, S \in G$, dass $T * (S * A) = T * (SAS^{-1}) = TSAS^{-1}T^{-1} = (TS)A(TS)^{-1} = (TS) * A$ mit beliebigem $A \in X$. Damit ist $*$ eine Operation von $G$ auf $X$.
(c) Wir behaupten, dass

$$R = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} | a, b \in \mathbb{R} : a \geq b \right\} \cup \left\{ \begin{pmatrix} c & 1 \\ 0 & c \end{pmatrix} | c \in \mathbb{R} \right\} \tag{190}$$

ein Repräsentantensystem den Bahnen von $*$ ist. Sei dazu $B$ eine Bahn von $*$. Dann gibt es ein $A \in X$, sodass $G(A) = B$. Nach Definition von $X$, ist $A$ ähnlich zu einer Matrix in Jordan-Normalform. Hierbei können zwei Fälle auftreten. Entweder $A$ ist diagonalisierbar mit den einfach Eigenwerten $a, b \in \mathbb{R}$ (ohne Einschränkung

ist $a \geq b$) oder $A$ ist nicht diagonalisierbar und hat dann den zweifachen Eigenwert $c \in \mathbb{R}$. In ersten Fall gibt es ein $T \in G$, sodass

$$TAT^{-1} = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in R. \tag{191}$$

Im zweiten Fall gibt es ein $T \in G$, sodass

$$TAT^{-1} = \begin{pmatrix} c & 1 \\ 0 & c \end{pmatrix} \in R. \tag{192}$$

In jedem Fall enthält $B$ ein Element aus $R$. Die Bahn $B$ enthält sogar genau ein Element aus $R$. Seien nämlich $J, J' \in R$ verschieden aber $J, J' \in B$. Dann gibt es $T, T' \in G$, sodass $TAT^{-1} = J$ und $T'AT'^{-1} = J'$. $J$ und $J'$ können sich nach der Eindeutigkeit der Jordan-Normalform nur in der Reihenfolge der Jordan-Blöcke unterscheiden. Wir haben also einen Widerspruch, denn die Reihenfolge der Jordan-Blöcke in $R$ ist bereits nach Definition von $R$ festgelegt. Folglich ist $J = J'$ und jede Bahn von $*$ enthält genau ein Element aus $R$. Damit ist $R$ ein Repräsentantensystem der Menge der Bahnen von $*$. □

**Aufgabe 147 (H19T3A3)** Sei $G$ eine endliche Gruppe.
(a) Falls $U$ eine Untergruppe vom Index $k$ ist, so gibt es einen Normalteiler $N \trianglelefteq G$, sodass $N \subseteq U$, $k|(G : N)$ und $(G : N)|k!$. Wir betrachten hierzu die Operation von $G$ auf der Menge der Linksnebenklassen $G/U$ definiert durch $* : G \times G/U \to G/U, (g, g_1U) \mapsto gg_1U$. Aus der Vorlesung ist bekannt, dass es sich hierbei um eine wohldefinierte Abbildung handelt, die eine Operation von $G$ auf $G/U$ definiert. $*$ definiert einen Gruppenhomomorphismus $\phi : G \to \mathrm{Per}(G/U)$ vermöge $\phi(g)(g_1U) = g * g_1U$. Da bereits $\ker\phi \trianglelefteq G$, bleibt zu zeigen, dass $N := \ker\phi$ die Teilbarkeitsrelationen der Aufgabenstellung erfüllt und $N \subseteq U$. Sei dazu $n \in N$ beliebig. Es gilt $\phi(n) = \mathrm{id}_{G/U}$, sodass für $e_GU = U \in G/U$ gilt $\phi(n)(U) = \mathrm{id}_{G/U}(U) = U$ und $\phi(n)(U) = n * U = nU$. Zusammen gilt $nU = U$, sodass $n \in U$. Beliebigkeit von $n \in N$ liefert $N \subseteq U$. Mit dem Satz von Lagrange gilt zudem $(G : N) = |G|/|N| = |G|/|U| \cdot |U|/|N| = (G : U)(U : N)$. Damit gilt $(G : N) = k(G : U)$, also $k|(G : N)$. Da $\phi(G) =: H \leq \mathrm{Per}(G/U)$, gilt zusammen mit $\mathrm{Per}(G/U) \simeq S_{(G:U)} = S_k$, nach dem Homomorphiesatz $|G|/|N| = |\phi(G)||S_k| = k!$, also nach Lagrange $(G : N)|k!$.
(b) Wir zeigen, dass es keine einfache Gruppe der Ordnung 108 gibt. Es gilt zunächst $G = 2^2 \cdot 3^3$. Für die endliche Gruppe $G$ wissen wir zumindest, dass eine Untergruppe der Ordnung $2^2$ und eine Untergruppe der Ordnung $3^3$ existiert. Diese sind dann jeweils eine 2- bzw. 3-Sylowgruppe von $G$. Wir bezeichnen die gewählte 2- bzw. 3-Sylowgruppe mit $P_2$ bzw. $P_3$. Es gilt $(G : P_3) = 4$. Die Aussage von oben liefert uns, dass es einen Normalteiler $N$ von $G$ gibt, sodass $2^2 = 4|(G : N)$ und $(G : N)|24 = 2^3 \cdot 3$. Damit kommt nur $(G : N) \in \{4, 12, 24\}$ in Betracht. Da $|N||G|$ kommt sogar nur $(G : N) \in \{4, 12\}$ in Betracht. Im ersten Fall wäre $|N| = 27$, im zweiten Fall $|N| = 9$. In jedem Fall gilt $1 < |N| < 108$, sodass wir einen nichttrivialen Normalteiler von $G$ gefunden haben. $G$ ist somit also nicht einfach. □

**Aufgabe 148 (H13T1A3)** Gegeben sei die Matrix

$$A = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} \in \mathrm{Mat}(2 \times 2, \mathbb{C})$$

mit $\lambda \neq 0$. Wir sollen für alle natürlichen Zahlen $k \geq 1$ zeigen, dass $A^k$ die Jordan'schen Normalform

$$J(A^k) = \begin{pmatrix} \lambda^k & 1 \\ 0 & \lambda^k \end{pmatrix} \tag{193}$$

hat. Für $k = 1$ stimmt die Aussage, denn $A$ liegt bereits in Jordan'scher Normform vor. Wir berechnen

$$A^2 = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} = \begin{pmatrix} \lambda^2 & 2\lambda \\ 0 & \lambda^2 \end{pmatrix} \tag{194}$$

$$A^3 = \begin{pmatrix} \lambda^2 & 2\lambda \\ 0 & \lambda^2 \end{pmatrix} \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} = \begin{pmatrix} \lambda^3 & 3\lambda^2 \\ 0 & \lambda^3 \end{pmatrix} \tag{195}$$

$$A^4 = \begin{pmatrix} \lambda^3 & 3\lambda^2 \\ 0 & \lambda^3 \end{pmatrix} \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} = \begin{pmatrix} \lambda^4 & 4\lambda^3 \\ 0 & \lambda^4 \end{pmatrix}. \tag{196}$$

Wir behaupten, dass für $k \geq 1$ allgemein gilt

$$A^k = \begin{pmatrix} \lambda^k & k\lambda^{k-1} \\ 0 & \lambda^k \end{pmatrix}. \tag{197}$$

Für $k = 1$ stimmt die Aussage nach Definition von $A$. Wir zeigen nun, dass falls die Aussage für ein festes $k$ wahr ist, sie auch für $k + 1$ gilt. Eine kurze Rechnung bestätigt in der Tat

$$A^{k+1} = A^k A = \begin{pmatrix} \lambda^k & k\lambda^{k-1} \\ 0 & \lambda^k \end{pmatrix} \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} = \begin{pmatrix} \lambda^{k+1} & (k+1)\lambda^k \\ 0 & \lambda^{k+1} \end{pmatrix}. \tag{198}$$

Sei nun $k$ beliebig aber fest gewählt. Wir berechnen das charakteristische Polynom $\chi_{A^k}(z)$ von $A^k$. Es gilt

$$\chi_{A^k}(z) = \det(zE_2 - A^k) = \det\left(\begin{pmatrix} z - \lambda^k & -k\lambda^{k-1} \\ 0 & z - \lambda^k \end{pmatrix}\right) = (z - \lambda^k)^2. \tag{199}$$

Damit ist das charakeristische Polynom von $A^k$ separabel über $\mathbb{C}$ und der Satz über die Existenz der Jordan'schen Normlform liefert, dass $A^k$ in Jordan'sche Normalform gebracht werden kann. Damit stehen die beiden Kandidaten

$$J_1 = \begin{pmatrix} \lambda^k & 0 \\ 0 & \lambda^k \end{pmatrix} \text{ oder } J_2 = \begin{pmatrix} \lambda^k & 1 \\ 0 & \lambda^k \end{pmatrix} \tag{200}$$

zur Auswahl. Im ersten Fall hat $J_1$ zwei Jordan-Kästchen von je der Länge 1, im zweiten Fall hat $J_2$ ein Jordan-Kästchen der Länge 2. Wir berechnen das Minimalpolynom $\mu_{A^k}$. Dieses ist das kleinste Polynom $p$ mit der Eigenschaft, dass $p(A^k) = 0$.

Wegen des Satzes von Cayley-Hamilton gilt $\chi_{A^k}(A^k) = 0$, sodass $\mu_{A^k} | \chi_{A^k}$. Somit ist $\mu_{A^k}(z) \in \{z - \lambda^k, (z - \lambda^k)^2\}$. Im ersten Fall sehen wir aber, dass $\mu_{A^k}(A^k) \neq 0$, denn

$$\mu_{A^k}(A^k) = \begin{pmatrix} \lambda^k & k\lambda^{k-1} \\ 0 & \lambda^k \end{pmatrix} - \begin{pmatrix} \lambda^k & 0 \\ 0 & \lambda^k \end{pmatrix} = \begin{pmatrix} 0 & k\lambda^{k-1} \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad (201)$$

und das letzte (Un-)gleichheitszeichen gilt wegen der Voraussetzung, dass $\lambda \neq 0$. Somit bleibt nur $\mu_{A^k}(z) = (z - \lambda^k)^2$. Laut Vorlesung ist $\deg(\mu_{A^k})$ im Falle, dass $\mu_{A^k}$ nur eine Nullstelle besitzt, gleich der Länge des größten Jordan-Kästchens, das zu dem durch die Nullstelle gegebenen Eigenwert von $A^k$ gehört. Da hier $\mu_{A^k}$ die zweifache Nullstelle $\lambda^k$ besitzt, ist das größte zugehörige Jordan-Kästchen von der Länge 2. Mithin ist $J_2$ die gesuchte Jordan-Normalform von $A^k$ und die Behauptung bewiesen. □

**Aufgabe 149 (F18T3A3)** (a) Sei $G$ eine endliche Gruppe und bezeichne mit $\nu_p$ die Anzahl der $p$-Sylow-Untergruppen von $G$. Ferner seien $p, q$ zwei verschiedene Primzahlen, die die Ordnung von $G$ teilen. Angenommen, $\nu_p = 1 = \nu_q$ und es bezeichnet $P$ die einzige $p$-Sylowgruppe von $G$ und $Q$ die einzige $q$-Sylowgruppe von $G$. Wir zeigen: Dann gilt $g_P g_Q = g_Q g_P$ für alle $g_P \in P$ und $g_Q \in Q$. Aus dem zweiten Sylow'schen Satz folgt wegen $\nu_p = 1 = \nu_q$, dass $P \trianglelefteq G$ und $Q \trianglelefteq G$. Insbesondere gilt für alle $g_P \in P$ und $g_Q \in Q$, dass $g_Q g_P^{-1} g_Q^{-1} \in P$ und $g_P g_Q^{-1} g_P^{-1} \in Q$. Wegen der Abgeschlossenheit von $P$ und $Q$ bzgl. der Gruppenmultiplikation ist auch $g_P \cdot g_Q g_P^{-1} g_Q^{-1} \in P$ und $g_Q \cdot g_P g_Q^{-1} g_P^{-1} \in Q$. Wegen $(g_P \cdot g_Q g_P^{-1} g_Q^{-1})^{-1} = g_Q \cdot g_P g_Q^{-1} g_P^{-1}$ liefert die Abgeschlossenheit von $P$ bzw. $Q$, dass $g_Q \cdot g_P g_Q^{-1} g_P^{-1} \in P \cap Q$. Wegen $p \neq q$ und $p, q$ prim gilt ferner $\mathrm{ggT}(|P|, |Q|) = 1$. Da sowohl $P \leq G$ und $Q \leq G$ gilt $P \cap Q = \{e_G\}$. Somit gilt $g_Q \cdot g_P g_Q^{-1} g_P^{-1} = e_G$, was vermöge Multiplikation mit $g_P g_Q$ äquivalent zu $g_Q \cdot g_P = g_P g_Q$ ist.
(b) Sei nun $G$ eine Gruppe der Ordnung 12. Wir zeigen zuerst, dass $\nu_3 = 4$ und $\nu_2 = 3$ unmöglich ist. Angenommen, $\nu_3 = 4$ und $\nu_2 = 3$. Da je zwei $p$-Sylowgruppen von $G$ trivialen Schnitt haben, gibt es in $G$ mindestens $4 \cdot \Phi(3) = 8$ Elemente der Ordnung 3, nämlich mindestens die Elemente aus den 3-Sylowgruppen, die Ordnung 3 haben. Da 3 prim ist, gibt es in jeder 3-Sylowgruppe $\Phi(3) = 2$ Elemente der Ordnung 3. Zusammen mit $\nu_3 = 4$ folgt die angegebene untere Schranke für die Anzahl der Elemente aus $G$ von der Ordnung 3. In den 3, nach Voraussetzung paarweise verschiedenen 2-Sylowgruppen liegen mindestens $3 + 1 = 4$ Elemente der Ordnung 2 oder 4. Da $\mathrm{ggT}(3, 2^2) = 1$ sind diese von der vorher abgezählten Elementen verschieden. Damit haben wir mindestens 12 Elemente in $G$, die Ordnung $2, 3, 4$ haben. Da aber zusätzlich ein neutrales Element in der Gruppe $G$ liegt, müssen mindestens $12+1 = 13$ verschiedene Elemente in $G$ liegen, was $|G| = 12$ widerspricht. Somit kann der Fall $\nu_3 = 4$ und $\nu_2 = 3$ nicht auftreten. Wir zeigen nun, dass $G$ im Falle $\nu_3 = 1 = \nu_2$ abelsch ist. Dann ist nämlich die einzige 2-Sylowgruppe $P_2$ von $G$ nach dem zweiten Sylow'schen Satz ein Normalteiler von $G$. Analog liefert der zweite Sylowsche Satz mit $\nu_3 = 1$, dass die einzige 3-Sylowgruppe von $G$ ein Normalteiler von $G$ ist. $P_2$ ist als Gruppe von Primzahlquadratordnung abelsch, und $P_3$ ist als Gruppe von Primzahlordnung sogar zyklisch. Da $P_2, P_3 \trianglelefteq G$ und $\mathrm{ggT}(|P_2| = 4, |P_3| = 3) = 1$, ist $P_2 \cap P_3 = \{e_G\}$ und somit ist das innere direkte Produkt $P_2 \cdot P_3 \leq G$. Wegen $|P_2 \cdot P_3| = |P_2||P_3| = 12$ folgt sogar stärker $P_2 \cdot P_3 = G$.

Da $G = P_2 \cdot P_3 \simeq P_2 \times P_3$ und jeder der Faktoren aus dem rechts stehenden äußeren direkten Produkt abelsch ist, ist auch $G$ als zu einer abelschen Gruppe isomorphe Gruppe selbst abelsch. □

**Aufgabe 150 (H17T3A1)** Sei $G$ eine Gruppe der Ordnung $992 = 2^5 \cdot 31$.
(a) Nach dem dritten Sylowschen Satz gilt für die Anzahl $\nu_2$ der Sylowgruppen von $G$, dass $\nu_2 | 31$ und $\nu_2 \equiv 1 \bmod(2)$. Damit ist $\nu_2 \in \{1, 31\}$ möglich. Analog liefert der dritte Sylowsche Satz für die Anzahl $\nu_{31}$ der 31-Sylowgruppen von $G$, dass $\nu_{31} | 32$ und $\nu_{31} \equiv 1 \bmod(31)$. Damit ist $\nu_{31} \in \{1, 32\}$ möglich.
(b) Wir zeigen, dass $G$ auflösbar ist. Dazu schließen wir aus, dass $\nu_2 = 31$ und $\nu_{31} = 32$. Angenommen, $\nu_2 = 31$ und $\nu_{31} = 32$. Da 31 eine Primzahl ist und je zwei verschiedene 31-Sylowgruppen die Schnittmenge $\{e_G\}$ haben, haben wir $32 \cdot \Phi(31) = 32 \cdot 30$ verschiedene Elemente der Ordnung 31 in $G$. Zudem liegen keine Elemente von 2-Potenzordnung in einer 31-Sylowgruppe, ausgenommen das Neutralement $e_G$ von $G$. Seien $P', P''$ zwei verschiedene 2-Sylowgruppen von $G$. Da $P', P''$ verschieden sind, kann $P' \cap P''$ nur eine echte Untergruppe von $P'$ und $P''$ sein. Somit ist $|P' \cap P''| \leq 16$. Insgesamt gibt es somit in $G$ noch $|P' \cup P''| = |P'| + |P''| - |P' \cap P''| = 48$ Elemente der Ordnung $2^k$ mit $k \in \{0, 1, 2, 3, 4, 5\}$. Zusammen haben wir somit bereits $30 \cdot 32 + 48 > 30 \cdot 32 + 32 = 992$ Elemente in $G$, im Widerspruch zu $|G| = 992$. Somit kann der Fall $\nu_2 = 31$ und $\nu_{31} = 32$ nicht auftreten. Damit bleiben zwei Fälle übrig: $\nu_2 = 1$ oder $\nu_{31} = 1$.

- *Fall 1:* $\nu_2 = 1$. Dann ist die einzige 2-Sylowgruppe $P$ nach einer Folgerung aus dem zweiten Sylowschen Satz ein Normalteiler von $G$. Da $|G/P| = 31$ nach dem Satz von Lagrange und 31 eine Primzahl ist, ist $P/Q$ zyklisch, damit insbesondere auflösbar. $P$ selbst ist als $p = 2$-Gruppe nach der Vorlesung ebenfalls auflösbar. Da sowohl $G/P$ als auch $P$ auflösbar sind, liefert ein Vorlesungsresultat die Auflösbarkeit von $G$.

- *Fall 2:* $\nu_{31} = 1$. Dann ist die einzige 31-Sylowgruppe $Q$ nach einer Folgerung aus dem zweiten Sylowschen Satz ein Normalteiler von $G$. Da $|G/Q| = 32 = 2^5$ ist die Faktorgruppe $G/Q$ eine $p$-Gruppe zur Primzahl 2, laut Vorlesung also auflösbar. $Q$ wiederum ist von Primzahlordnung, somit zyklisch und damit insbesondere auflösbar. Analog zu Fall 1 folgt mithilfe eines Vorlesungsresultats, dass $G$ auflösbar ist.

Insgesamt ist somit in jedem der zulässigen Fälle $G$ auflösbar, die Behauptung somit bewiesen. □

**Aufgabe 151 (F15T1A3)** Sei $G$ eine Gruppe der Ordnung 105.
(a) Wir zeigen, dass $G$ einen Normalteiler der Ordnung 5 oder 7 hat. Zunächst gilt $105 = 3 \cdot 5 \cdot 7$ in Primfaktorzerlegung. Sei für eine Primzahl $p$ $\nu_p$ die Anzahl der $p$-Sylowgruppen von $G$. Nach dem dritten Sylowschen Satz gilt für $\nu_5$, dass $\nu_5 | 21$ und $\nu_5 \equiv 1 \bmod(5)$. Somit ist $\nu_5 \in \{1, 3, 7, 21\}$ wegen der ersten Bedingung und die zweite Bedingung schränkt die Möglichkeiten auf $\nu_5 \in \{1, 21\}$ ein. Analog liefert der dritte Sylow'sche Satz, dass für $\nu_7$ gilt $\nu_7 | 15$ und $\nu_7 \equiv 1 \bmod(7)$. Die erste Bedingung erlaubt $\nu_7 \in \{1, 3, 5, 15\}$ und die zweite Bedingung schränkt das

ein zu $\nu_7 \in \{1, 15\}$. Wir zeigen nun, dass $\nu_7 = 15$ und $\nu_5 = 21$ nicht möglich ist. Denn die paarweise Verschiedenheit der $p$-Sylowgruppen von Primzahlordnung 5 bzw. 7 impliziert zunächst, dass es in $G$ $21 \cdot \Phi(5) = 84$ Elemente der Ordnung 5 und $15 \cdot \Phi(7) = 90$ Elemente der Ordnung 7. Zusammen enthält $G$ dann bereits $84 + 90 = 174$ Elemente von der Ordnung 5 oder 7, was $|G| = 105$ widerspricht. Damit ist $\nu_5 = 1$ oder $\nu_7 = 1$. Im Fall $\nu_5 = 1$ hat $G$ nach einer Folgerung aus dem zweiten Sylowschen Satz einen Normalteiler der Ordnung 5, im zweiten Fall wegen desselben Vorlesungsresultats einen Normalteiler der Ordnung 7.
(b) Wir zeigen nun, dass $G$ auflösbar ist. Hierbei arbeiten wir mit Fallunterscheidung.

- *Fall 1:* $\nu_5 = 1$. In diesem Fall hat $G$ einen Normalteiler $P$ der Ordnung 5. Dieser ist von Primzahlordnung, also zyklisch, somit auflösbar. Die Faktorgruppe $G/P$ hat dann nach dem Satz von Lagrange die Ordnung 21. Für die Anzahl $\mu_7$ der 7-Sylowgruppen von $G/P$ gilt dann $\mu_7|3$ und $\mu_7 \equiv 1 \bmod(7)$. Somit ist nur $\mu_7 = 1$ möglich. Damit hat $G/P$ einen Normalteiler $P'$ der Ordnung 7, der, da von Primzahlordnung, zyklisch und damit auflösbar ist. Die Faktorgruppe $(G/P)/P'$ hat wiederum nach Lagrange die Ordnung 3, d.h., ist als Gruppe von Primzahlordnung zyklisch und damit auflösbar. Aus der Vorlesung ist bekannt, dass eine Gruppe $G$ genau dann auflösbar ist, wenn $G$ einen auflösbaren Normalteiler besitzt, sodass $G/N$ auflösbar ist. Das liefert uns zunächst die Auflösbarkeit von $G/P$. Nochmaliges Anwenden des zitierten Resultats auf $G/P$ und $P$ liefert dann die Auflösbarkeit von $G$.

- *Fall 2:* $\nu_7 = 1$. In diesem Fall hat $G$ einen Normalteiler $Q$ der Ordnung 7. Dieser ist als Gruppe von Primzahlordnung zyklisch und damit auflösbar. Die Faktorgruppe $G/Q$ hat die Ordnung 15. Bezeichnen wir wiederum mit $\mu_p$ für eine Primzahl $p$ die Anzahl der $p$-Sylowgruppen von $G/Q$, so liefert uns der dritte Sylowsche Satz für die Anzahl $\mu_5$ der 5-Sylowgruppen von $G/Q$ die zwei Bedingungen $\mu_5|3$ und $\mu_5 \equiv 1 \bmod(5)$. Beides zusammen erlaubt nur $\mu_5 = 1$, woraus mittels der bereits oben verwendeten Folgerung aus dem zweiten Sylowschen Satz die Normalteilereigenschaft der einzigen 5-Sylowgruppe $Q'$ von $G/Q$ folgt. $Q'$ ist als Gruppe von Primzahlordnung zyklisch und damit auflösbar und der Satz von Lagrange liefert, dass $(G/Q)/Q'$ von Ordnung $|(G/Q)/Q'| = 15/5 = 3$, also ebenfalls von Primzahlordnung ist. Also ist $(G/Q)/Q'$ ebenfalls zyklisch und damit auflösbar. Somit sind $Q'$ und $(G/Q)/Q'$ auflösbar und ein Resultat aus der Vorlesung liefert die Auflösbarkeit von $G/Q$. Zusammen mit der Auflösbarkeit von $Q$ folgt mithilfe desselben Vorlesungsergebnisses die Auflösbarkeit von $G$.

In jedem Fall ist $G$ auflösbar, womit der Beweis beendet ist. □

**Aufgabe 152** Im folgenden sind jeweils Gruppen einer vorgegebenen Ordnung im Hinblick auf Isomorphietypen zu bestimmen.
(a) Gesucht sind die Isomorphietypen aller Gruppen der Ordnung 99. Sei $G$ eine Gruppe der Ordnung 99. Wegen $99 = 3^2 \cdot 11$ hat $G$ nur nicht-triviale 3- und 11-Sylowgruppen. Für deren Anzahlen $\nu_3$ bzw. $\nu_{11}$ gilt $\nu_3|11$ und $\nu_3 \equiv 1 \bmod(3)$ bzw. $\nu_{11}|9$ und $\nu_{11} \equiv 1 \bmod(11)$, jeweils nach dem dritten Sylowschen Satz. In

beiden Fällen sehen wir, dass $\nu_3 = 1$ und $\nu_{11} = 1$ die jeweils einzige zulässige Möglichkeit sind. Bezeichne $P$ die einzige 3-Sylowgruppe von $G$ und $Q$ die einzige 11-Sylowgruppe von $G$. Eine Folgerung aus dem dritten Sylowschen Satz sagt nun, dass $P, Q \trianglelefteq G$. Zudem gilt $\mathrm{ggT}(|P| = 9, |Q| = 11) = 1$, sodass $P \cap Q = \{e_G\}$. Damit ist das innere direkte Produkt $PQ \leq G$. Für dessen Ordnung gilt $|PQ| = |P||Q| = 99$, sodass aus dem trivial geltenden $PQ \subseteq G$ bereits $PQ = G$ aus Ordnungsgründen folgt. Als inneres direktes Produkt der Gruppen $P, Q$ ist $G$ isomorph zu $G \simeq P \times Q$, dem äußeren direkten Produkt von $P, Q$. Da $P$ von Primzahlquadratordnung ist, ist $P$ abelsch und nach dem Hauptsatz über endlich erzeugte abelsche Gruppen weiterhin isomorph zu $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ oder $\mathbb{Z}/9\mathbb{Z}$. Diese sind bereits nicht isomorph, denn die erstgenannte Gruppe hat nur Elemente von Ordnung $\leq 3$, wohingegen die zweitgenannte Gruppe als zyklische Gruppe der Ordnung 9 mindestens ein Element der Ordnung 9 hat. Als Gruppe von Primzahlordnung ist $Q$ zyklisch und isomorph zu $\mathbb{Z}/11\mathbb{Z}$. Insgesamt haben wir damit die folgenden beiden Isomorphietypen, $(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \times \mathbb{Z}/11\mathbb{Z}$ bzw. $(\mathbb{Z}/9\mathbb{Z}) \times \mathbb{Z}/11\mathbb{Z}$. Die Nicht-Isomorphie der beiden eingeklammerten Faktoren liefert nun die Nicht-Isomorphie der beiden Isomorphietypen.
(b) Gesucht sind alle Isomorphietypen von Gruppen der Ordnung 45. Sei $G$ eine Gruppe der Ordnung 45. Die Primfaktorzerlegung liefert $|G| = 3^2 \cdot 5$. Wir bezeichnen wie in Teil (a) mit $\nu_3$ bzw. $\nu_5$ die Anzahlen der 3- bzw. 5-Sylowgruppen von $G$. Der dritte Sylowsche Satz liefert uns $\nu_3 | 5$ und $\nu_3 \equiv 1 \bmod(5)$ und $\nu_5 | 9$ und $\nu_5 \equiv 1 \bmod(5)$. Auch hier ist lediglich $\nu_3 = 1$ und $\nu_5 = 1$ möglich. Wir bezeichnen die einzige 3-Sylowgruppe von $G$ als $P$ und die einzige 5-Sylowgruppe von $G$ als $Q$. Dann gilt nach einer Folgerung aus dem zweiten Sylowschen Satz, dass $P, Q \trianglelefteq G$. Wegen $\mathrm{ggT}(|P| = 9, |Q| = 5) = 1$ gilt $P \cap Q = \{e_G\}$. Somit ist das innere direkte Produkt $PQ \leq G$. Wegen $|PQ| = |P||Q| = 45$ gilt sogar bereits $PQ = G$. Als inneres direktes Produkt der Gruppen $P$ und $Q$ ist $G$ isomorph zum äußeren direkten Produkt von $P$ und $Q$, $G \simeq P \times Q$. $P$ ist als Gruppe von Primzahlquadratordnung abelsch und nach dem Hauptsatz über endlich erzeugte abelsche Gruppen isomorph zu $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ oder $\mathbb{Z}/9\mathbb{Z}$. Die beiden Isomorphietypen sind verschieden, denn in der letztgenannten Gruppe gibt es ein erzeugendes Element, das dann die Ordnung 9 hat, wohingegen in der erstgenannten Gruppe lediglich Elemente der Ordnung $\leq 3$ existieren. Daher können die beiden Isomorphietyp-Gruppen nicht zueinander isomorph sein. Die Gruppe $Q$ hingegen ist als Gruppe von Primzahlordung isomorph zur zyklisch Gruppe $\mathbb{Z}/5\mathbb{Z}$. Analog zu Aufgabenteil (a) ist also $G$ isomorph zu $(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \times \mathbb{Z}/5\mathbb{Z}$ oder $(\mathbb{Z}/9\mathbb{Z}) \times \mathbb{Z}/5\mathbb{Z}$, wobei die Nicht-Isomorphie der beiden eingeklammerten Faktoren impliziert, dass $(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \times \mathbb{Z}/5\mathbb{Z} \not\simeq (\mathbb{Z}/9\mathbb{Z}) \times \mathbb{Z}/5\mathbb{Z}$.
(c) Gesucht sind nun alle Isomorphietypen von Gruppen der Ordnung 143. Sei $G$ eine Gruppe der Ordnung $143 = 11 \cdot 13$. Wir bezeichnen mit $\nu_{11}$ bzw. $\nu_{13}$ die Anzahlen der 11 bzw. 13-Sylowgruppen von $G$. Nach dem dritten Sylowschen Satz gilt $\nu_{11} | 13$ und $\nu_1 1 \equiv 1 \bmod(11)$ sowie $\nu_{13} | 11$ und $\nu_{13} \equiv 1 \bmod(13)$. Hieraus sieht man leicht, dass $\nu_{11} = 1$ und $\nu_{13} = 1$. Seien nun $P$ die 11- und $Q$ die 13-Sylowgruppe von $G$. Da $P$ und $Q$ jeweils zyklisch. da Ordnung 11 bzw. 13, sind, gilt $P \simeq \mathbb{Z}/11\mathbb{Z}$ und $Q \simeq \mathbb{Z}/13\mathbb{Z}$. Da ferner $P$ und $Q$ die einzigen 11- bzw. 13-Sylowgruppen von $G$ sind, liefert eine Folgerung aus dem zweiten Sylowschen Satz, dass $P, Q \trianglelefteq G$. Da $P$ und $Q$ Normalteiler von $G$ von teilerfremder Ordnung sind, ist das innere direkte

Produkt $PQ \leq G$ und wegen $|PQ| = |P||Q| = 143$ gilt sogar $PQ = G$. Somit ist $G \simeq P \times Q \simeq \mathbb{Z}/143\mathbb{Z}$, und die letzte Isomorphie folgt aus dem Chinesischen Restsatz für Gruppen. □

**Aufgabe 153** Sei $G$ eine Gruppe der Ordnung 12 ohne Untergruppe der Ordnung 6. Wir zeigen, dass $G \simeq A_4$. Wir bestimmen zunächst die Anzahlen $\nu_p$ der $p$-Sylowgruppen von $G$. Infolge des dritten Sylowschen Satzes gilt $\nu_3|4$ und $\nu_3 \equiv 1 \bmod(3)$. Damit sind nur die Fälle $\nu_3 \in \{1, 4\}$ beachtlich.

- *Fall 1:* $\nu_3 = 1$. Dann ist die einzige 3-Sylowgruppe, bezeichnet mit $P$, von $G$ nach dem zweiten sylowschen Satz ein Normalteiler von $G$. Zudem gibt es in $G$ ein Element $G$ der Ordnung 2, welches in einer der 2-Sylowgruppen von $G$ liegt. Diese erzeugt $\langle g\rangle$, was eine zyklische Untergruppe von $G$ von der Ordnung 2 ist. Da $\mathrm{ggT}(|\langle g\rangle| = 2, |P| = 3) = 1$, gilt $P \cap \langle g\rangle = \{e_G\}$. Damit ist das innere semidirekte Produkt $\langle g\rangle P \leq G$ und es gilt $|\langle g\rangle P| = |\langle g\rangle||P| = 6$, im Widerspruch zur Voraussetzung, dass $G$ keine Untergruppe der Ordnung 6 hat. Dieser Fall kann also ebenfalls unbeachtlich bleiben.

- *Fall 2:* $\nu_3 = 4$. In diesem Fall bezeichnen wir mit $X$ die Menge der 3-Sylowgruppen von $G$, diese ist wegen $\nu_3 = |X|$ vierelementig. Zudem ist aus der Vorlesung bekannt, dass die Gruppe $G$ auf $X$ durch Konjugation operiert, genauer ist $\cdot : G \times X \to X, (g, P) \mapsto g \cdot P = gPg^{-1}$ eine Gruppenoperation. Laut Vorlesung induziert diese einen Homomorphismus $\phi : G \to \mathrm{Per}(X)$ von Gruppen, indem $g \mapsto [\phi(g) : X \to X, P \mapsto \phi(g)(X) = gPg^{-1}]$ gesetzt wird. Wir zeigen nun, dass dieser injektiv ist. Angenommen, $\phi$ wäre nicht injektiv. Dann gibt es ein $g \in G \setminus \{e_G\}$, sodass $g \in \ker\phi$. Letzteres bedeutet, dass $\phi(g) = \mathrm{id}_X$. Damit ist $gPg^{-1} = P$ für alle $P \in X$. Sei nun $P \in X$ beliebig aber fest und so, dass $g \notin P$. Da die 3-Sylowgruppen alle von Primzahlordnung sind, ist diese Wahl möglich. Mit $gPg^{-1} = P$ ist $N_G(P) \supsetneq P$ und insbesondere $|N_G(P)| > 3$. Andererseits gilt $G \geq N_G(P)$ und $\nu_3 = (G : N_G(P))$. Lezteres können wir mit dem Satz von Lagrange umformen zu $|N_G(P)| = |G|/\nu_3 = 3 = |P|$. Das liefert uns einen Widerspruch zum vorherigen Ergebnis, dass $N_G(P) \supsetneq P$. Somit ist $\ker\phi = \{e_G\}$ und $\phi$ damit injektiv. Damit ist $\mathrm{im}(G) \leq \mathrm{Per}(X) \simeq S_4$ nach dem Homomorphiesatz isomorph zu einer Untergruppe der Ordnung 12 von $S_4$. Wir behaupten, dass $A_4$ die einzige Untergruppe der Ordnung 12 von $S_4$ ist. Angenommen, es wäre $U \leq S_4$ mit $U \neq A_4$ und $|U| = 12$. Dann gibt es ein $\sigma \in U$ mit $\mathrm{sgn}(\sigma) = -1$, denn die $A_4$ enthält nach Definition alle geraden Permutationen aus $S_4$. Wir betrachten nun die Einschränkung $\mathrm{sgn} : S_4 \to \{-1, +1\}$ des Signumshomomorphismus von $S_4$ auf $U$. Dieser ist surjektiv und der Homomorphiesatz liefert, dass $N = \ker\mathrm{sgn}|_U \trianglelefteq U$ ein Normalteiler der Ordnung $|\ker\mathrm{sgn}|_U| = |U|/|\{\pm 1\}| = 6$ ist, wobei wir den Satz von Lagrange gleich verwendet haben. Für diesen Normalteiler gilt auch $N \leq A_4$, sodass $A_4$ eine Untergruppe der Ordnung 6 hat. Dies ist aber laut Vorlesung nicht der Fall. Damit hat die $S_4$ lediglich die $A_4$ als Untergruppe der Ordnung 12, sodass $G \simeq \mathrm{im}(\phi) \simeq A_4$ und die Behauptung somit bewiesen ist.

□

**Aufgabe 154** Sei $G$ eine Gruppe der Ordnung 2020.
(a) Wir sollen zeigen, dass $G$ stets einen Normalteiler vom Index 2 besitzt. Zunächst gilt $2020 = 20 \cdot 101 = 2^2 \cdot 5 \cdot 101$. Wir bestimmen zunächst die Anzahlen $\nu_p$ der $p$-Sylowgruppen von $G$. Es gilt nach dem dritten Sylowschen Satz, dass $\nu_{101}|20$ und $\nu_{101} \equiv 1 \bmod(101)$. Damit ist nur $\nu_{101} = 1$ möglich. Für die Anzahl der 5-Sylowgruppen von $G$ gilt ebenfalls nach dem dritten Sylowschen Satz, dass $\nu_5|404$ und $\nu_5 \equiv 1 \bmod(5)$, sodass $\nu_5 \in \{101\}$. Wir behaupten nun, dass $G$ eine Untergruppe der Ordnung 20 hat. Wir fahren dazu mit Fallunterscheidung nach $\nu_5$ fort.

- *Fall 1:* $\nu_5 = 1$. Dann ist die einzige 5-Sylowgruppe $N$ von $G$ ein Normalteiler und $G$. Sei $U$ eine beliebige 2-Sylowgruppe von $G$. Es gilt $|U| = 2^2 = 4$. Da $\mathrm{ggT}(|U| = 4, |N| = 5) = 1$, ist $U \cap N = \{e_G\}$. Damit ist das innere semidirekte Produkt $V \equiv UN$ eine Untergruppe von $G$ und es gilt $|V| = |U||N| = 20$.

- *Fall 2:* $\nu_5 = 101$. Dann ist $\nu_5 = (G : N_G(P))$ für eine beliebige 5-Sylowgruppe $P$ von $G$. Nach Definition des Normalisators von $P$ in $G$ ist bereits $N_G(P) \leq G$ klar. Mit dem Satz von Lagrange folgt $|N_G(P)| = |G|/\nu_5 = 2020/101 = 20$. Damit ist $N_G(P) \leq G$ von der geforderten Ordnung 20.

Bezeichne nun $U$ eine Untergruppe der Ordnung 20 von $G$. Wegen $20 = 2^2 \cdot 5$ hat $U$ nach dem dritten Sylow'schen Satz genau eine 5-Sylowgruppe, $Q$. Bezeichne dazu $\mu_5$ die Anzahl der 5-Sylowgruppen von $U$. Nach dem dritten Sylowschen Satz gilt $\mu_5|4$ und $\mu_5 \equiv 1 \bmod(5)$, sodass $\mu_5 = 1$ die einzig zulässige Wahl ist. Nach einer Folgerung aus dem zweiten Sylow'schen Satz ist die einzige 5-Sylowgruppe $Q$ von $U$ auch ein Normalteiler von $U$. Ferner hat $U$ mindestens eine 2-Sylowgruppe, also mindestens ein Element $g'$ der Ordnung 2, welches dann in $\langle g' \rangle \leq U$ liegt. Da die Ordnung von $\langle g' \rangle$ und $Q$ teilerfremd sind, gilt $\langle g' \rangle \cap Q = \{e_G\}$. Damit ist nun durch das innere semidirekte Produkt $V = \langle g' \rangle Q$ eine Untergruppe $V \leq U$ gegeben, die die Ordnung $|V| = |\langle g' \rangle||Q| = 10$ hat. Aus $V \leq U$ und $U \leq G$ folgt nun $V \leq G$. Somit hat auch $G$ eine Untergruppe der Ordnung 10. Bezeichne nun mit $N$ die 101-Sylowgruppe von $G$, deren Normalteilereigenschaft in $G$ bereits am Anfang bewiesen wurde. Da $N$ und $V$ von teilefremder Ordnung sind, ist $V \cap N = \{e_G\}$. Damit ist $M \equiv VN \leq G$ ein inneres semidirekted Produkt von Gruppen. Dieses hat die Ordnung $|M| = |V||N| = 10 \cdot 101 = 1010$. Für den Index von $M$ in $G$ gilt nach dem Satz von Lagrange, dass $(G : M) = |G|/|M| = 2020/1010 = 2$. Damit ist auch nachgewiesen, dass $M \trianglelefteq G$. Zusammefassend haben wir also einen Normalteiler von $G$ vom gewünschten Index 2 gefunden.
(b) Wie behaupten, dass der Normalteiler von $G$ im Sinne von (a) nicht notwendigerweise zyklisch ist. Dazu betrachten wir die Gruppe $G = \mathbb{Z}/2\mathbb{Z} \times D_{505}$, wo $D_{505}$ die Diedergruppe der Ordnung 1010 ist. Diese ist nach Vorlesung nicht-abelsch. Offenbar ist $N \equiv \{e_G\} \times D_{505} \leq G$, als Produkt von jeweils trivialen Untergruppen der Faktoren im äußeren direkten Produkt. Ferner ist $N \simeq D_{505}$ vermöge des offensichtlichen Isomorphismus $\psi : N \to D_{505}, (0, x) \mapsto x$. Zudem ist $N \trianglelefteq G$, denn $(G : N) = |G|/|N| = 2$ und Untergruppen vom Index 2 sind Normalteiler. Da nun $D_{505}$ als nicht-abelsche Gruppe insbesondere nicht-zyklisch ist, ist auch $N$ nicht-zyklisch. Damit ist die Behauptung bewiesen. □

**Aufgabe 155** Wir zeigen, dass eine Gruppe $G$ der Ordnung 2002 stets einen Normalteiler der Ordnung 1001 besitzt. Zunächst sehen wir, dass es reicht, zu zeigen, dass $G$ eine Untergruppe $N$ der Ordnung 1001 besitzt. Denn diese hat nach dem Satz von Lagrange den Index 2 in $G$ und ist somit laut Vorlesung ein Normalteiler von $G$. Wir bestimmen zunächst die Primfaktorzerlegung von $|G| = 2002$. Es gilt $2002 = 2 \cdot 11 \cdot 91 = 2 \cdot 11 \cdot 13 \cdot 7$. Bezeichne nun für eine Primzahl $p$ $\nu_p$ die Anzahl der $p$-Sylowgruppen von $G$. Es ist $\nu_{11}|182$ und $\nu_{11} \equiv 1 \bmod(11)$ nach dem dritten Sylowschen Satz. Wegen $182 \equiv 110 + 66 + 5 \equiv 5 \bmod(11) \not\equiv 1 \bmod(11)$ und $91 \equiv 3 \bmod(11) \not\equiv 1 \bmod(11)$ und $26 \equiv 5 \bmod(11) \not\equiv 1 \bmod(11)$ und $14 \equiv 3 \bmod(11) \not\equiv 1 \bmod(11)$ und $7 \not\equiv 1 \bmod(11)$ und $2 \not\equiv 1 \bmod(11)$ und $13 \equiv 2 \not\equiv 1 \bmod(11)$ gibt es nur eine 11-Sylowgruppe von $G$. Diese ist dann ein Normalteiler von $G$ nach dem zweiten Sylow'schen Satz. Wir bestimmen analog die Anzahl $\nu_{13}$ der 13-Sylowgruppen von $G$. Es gilt $\nu_{13}|154$ und $\nu_{13} \equiv 1 \bmod(13)$. Also ist $\nu_{13} \in \{2, 7, 11, 14, 22, 77, 154\}$ allein infolge der ersten Bedingung. Anhand der zweiten sieht man, dass $\nu_{13} \in \{1, 14\}$ zulässig ist. Für $\nu_7$ sehen wir, dass $\nu_7|286$ und $\nu_7 \equiv 1 \bmod(7)$. Es ist infolge der ersten Bedingung $\nu_7 \in \{1, 2, 11, 13, 22, 26, 143, 286\}$. Damit sind wegen der zweiten Bedingung an $\nu_7$ nur $\nu_7 = 1$ oder $\nu_7 = 22$ zulässig. Im ersten Fall ist durch die einzige 7-Sylowgruppe $P_7$ ein Normalteiler von $G$ gegeben. Wir bezeichnen mit $P_{13}$ eine beliebige 13-Sylowgruppe von $G$. Da $|P_7| = 7$ und $|P_{13}|$, gilt $P_7 \cap P_{13} = \{e_G\}$ und wir haben mit dem inneren semidireken Produkt $P_{13} \cdot P_7$ eine Untergruppe der Ordnung $7 \cdot 13 = 91$ von $G$ gefunden. Wir nennen diese $U \equiv P_{13} \cdot P_7 \leq G$. Da die Ordnung von $U$ teilerfremd zur Ordnung 11 von der einzigen 11-Sylowgruppe $P_{11}$ von $G$ ist, gilt ebenso $P_{11} \cap U = \{e_G\}$. Damit haben wir mit dem inneren semidirekten Produkt $N := UP_{11}$ eine Untergruppe von $G$ gefunden, die die Ordnung $91 \cdot 11 = 1001$ hat. In diesem Fall sind wir also fertig. Im Falle, dass $\nu_7 = 22$ verwenden wir, dass $22 = \nu_7$ gleich dem Index des Normalisators $N_G(P_7)$ einer beliebigen 7-Sylowgruppe von $P_7$ in $G$ ist. Zusammen mit dem satz von Lagrange folgt für die Ordnung des Normalisators $N_G(P_7)$, dass $|N_G(P_7)| = 2002/22 = 91$. Damit haben wir mit dem $N_G(P_7)$ eine Untergruppe von $G$ gefunden, die die Ordnung 91 hat. Da wiederum $|N_G(P_7)| = 91$ und $|P_{11}| = 11$ teilerfremd sind, gilt für den Schnitt von $N_G(P_7)$ und der 11-Sylowgruppe $P_{11}$ von $G$, dass $N_G(P_7) \cap P_{11} = \{e_G\}$. Zudem ist $P_1 1 \trianglelefteq G$, sodass wir mit dem inneren semidirekten Produkt $N := N_G(P_7)P_{11}$ eine Untergruppe von $G$ gefunden haben, die die Ordnung $|N_G(P_7)P_{11}| = |N_G(P_7)||P_{11}| = 91 \cdot 11 = 1001$ hat. Da nun $(G : N) = |G|/|N| = 2002/1001$ nach dem Satz von Lagrange ist das oben gefundene $N$ ein Normalteiler von $G$ mit den gewünschten Eigenschaften. Zusammenfassend gesprochen haben wir gezeigt, dass jede Gruppe der Ordnung 2002 einen Normalteiler vom Index 2 hat. □

**Aufgabe 156 (H14T2A4)** Sei $G$ eine endliche Gruppe und $p$ eine Primzahl dergestalt, dass $P$ eine $p$-Sylowgruppe von $G$ ist und für eine Untergruppe $H \leq G$ gilt, dass $p||H|$.
(a) Wir zeigen, dass dann ein $g \in G$ existiert, sodass $H \cap gPg^{-1}$ eine $p$-Sylowgruppe von $H$ ist. Sei dazu $Q$ eine $p$-Sylowgruppe von $H$. Da $H \leq G$ ist $Q$ eine $p$-Untergruppe von $G$. Nach dem ersten Sylowschen Satz gibt es daher eine $p$-Sylowgruppe $P'$ von $G$ mit der Eigenschaft, dass $Q \leq P'$. Nach dem zweiten Sylowschen Satz gilt,

dass je zwei $p$-Sylowgruppen von $G$ zueinander konjugiert sind. Also gibt es ein $g \in G$, sodass $gPg^{-1} = P'$. Es gilt $gPg^{-1} \cap H \leq H$. Damit ist $Q \subseteq gPg^{-1} \cap H$, denn $Q \leq H$ und $Q \leq gPg^{-1} = P'$. Zu zeigen ist, dass auch $gPg^{-1} \cap H \subseteq Q$. Da $gPg^{-1} \cap H$ eine $p$-Untergruppe von $H$ ist, folgt die Behauptung daraus, dass $Q$ als $p$-Sylowgruppe von $H$ maximale $p$-Untergruppe von $H$ ist.
(b) Wir betrachten die $S_3$ und setzen $H = \langle(12)\rangle$. Offenbar gilt für $p = 2$, dass $p||H|$. Zudem ist $P = \langle(13)\rangle$ eine 2-Sylowgruppe von $S_3$, denn $|P| = 2$ und 2 ist die maximale 2-Potenz, die $|S_3| = 3! = 6$ teilt. Aber es gilt $H \cap P = \{\mathrm{id}\}$. Somit ist $|H \cap P| = 1$ und damit ist $H \cap P$ keine 2-Sylowgruppe von der Gruppe $H$, die die Ordnung 2 hat. □

**Aufgabe 157 (H19T1A4)** Sei $G$ eine nicht-abelsche Gruppe der Ordnung $715 = 5 \cdot 11 \cdot 13$. Bezeichne für jede Primzahl $p$ $\nu_p$ die Anzahl der $p$-Sylowgruppen von $G$.
(a) Wir zeigen, dass $p = 5$ die einzige Primzahl ist, für die $\nu_p > 1$ gilt.

- *Fall 1:* $p \notin \{5, 11, 13\}$. Dann ist $\mathrm{ggT}(p, |G|) = 1$ und somit ist die größte $p$-Potenz, die $|G|$ teilt $p^0 = 1$. Die einzige Untergruppe der Ordnung 1 von $G$ ist $\{e_G\}$, die dann auch die einzige $p$-Sylowgruppe von $G$ für eine beliebige Primzahl $p \notin \{5, 11, 13\}$ ist. Für diese $p$ gilt also $\nu_p = 1$.

- *Fall 2:* $p = 13$. Wir wenden den dritten sylowschen Satz an. Dieser liefert uns zunächst, dass $\nu_{13}||G|/13 = 55$, also $\nu_{13} \in \{1, 5, 11, 55\}$. Zudem gilt $\nu_{13} \equiv 1 \bmod(13)$. Wegen $5 \equiv 5 \bmod(13) \not\equiv 1 \bmod(13)$, $11 \equiv 11 \bmod(13) \not\equiv 1 \bmod(13)$ und $55 \equiv (4 \cdot 13 + 3), \bmod(13) \equiv 3 \bmod(13) \equiv 3 \bmod(13)$ ist nur $\nu_{13} = 1$ möglich.

- *Fall 3:* $p = 11$. Wir wenden den dritten sylowschen Satz an. Dieser liefert uns zunächst, dass $\nu_{11}||G|/11 = 65$, also $\nu_{11} \in \{1, 5, 13, 65\}$. Zudem gilt, ebenfalls nach dem dritten Sylowschen Satz, $\nu_{11} \equiv 1 \bmod(11)$. Wegen $5 \not\equiv 1 \bmod(11)$, $13 \equiv 2 \bmod(11) \not\equiv 1 \bmod(11)$ und $65 \equiv 10 \bmod(11) \not\equiv 1 \bmod(11)$ ist auch für $p = 11$ nur $\nu_{11} = 1$ möglich.

- *Fall 4:* $p = 5$, $\nu_5 > 1$. Wir müssen ausschließen, dass $\nu_5 = 1$. Angenommen, $\nu_5 = 1$. Bezeichne mit $P_5, P_{11}, P_{13}$ die jeweils einzigen 5-, 11- und 13-Sylowgruppen von $G$. Da $\nu_5 = \nu_{11} = \nu_{13} = 1$, gilt $P_5 \trianglelefteq G$, $P_{11} \trianglelefteq G$ und $P_{13} \trianglelefteq G$ nach dem zweiten sylowschen Satz. Da $P_{11}$ und $P_{13}$ die Ordnungen 11 bzw. 13 haben, gilt $\mathrm{ggT}(|P_{11}|, |P_{13}|) = 1$, somit $P_{11} \cap P_{13} = \{e_G\}$. Somit ist das Komplexprodukt $P_{11} \cdot P_{13}$ sogar eine Untergruppe von $G$, $P_{11} \cdot P_{13} \leq G$, nämlich das innere direkte Produkt. Da $P_{11}$ und $P_{13}$ beide Normalteiler von $G$ sind, ist auch $U := P_{11} \cdot P_{13} \trianglelefteq G$. Zudem ist die einzige 5-Sylowgruppe nach den obigen Ausführungen ebenfalls ein Normalteiler von $G$. Wegen $U \trianglelefteq G$ und $P_5 \trianglelefteq G$ sowie $\mathrm{ggT}(|U|, |P_5|) = \mathrm{ggT}(143, 5) = 1$ gilt $U \cap P_5 = \{e_G\}$. Somit ist $V := P_5 \cdot U \leq G$. Wegen $|U| = |P_{11}||P_{13}| = 143$ und $|V| = |P_5||U| = 5 \cdot 143 = 715$ gilt $|V| = |G|$. Zusammen mit $V \subseteq G$ folgt daraus, dass $V = G$. Aus der Vorlesung ist bekannt, dass ein inneres direktes Produkt $U_1 \cdot U_2 \simeq U_1 \times U_2$, d.h., dieses isomorph um äußeren direkten Produkt ist. Damit finden wir, dass $G = P_5 \cdot U = P_5 \cdot (P_{11} \cdot P_{13}) \simeq P_5 \cdot (P_{11} \times P_{13}) \simeq P_5 \times P_{11} \times P_{13}$. Da $P_p$ für $p \in \{5, 11, 13\}$ jeweils von Ordnung $p$, also von Primzahlordnung ist, ist

$P_p \simeq \mathbb{Z}/p\mathbb{Z}$, also jeweils isomorph zur zyklischen Gruppe der Ordnung $p$. Somit gilt für $G$, dass $G \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z} =: G'$. Da $G'$ äußeres direktes Produkt von zyklischen Gruppen ist, ist $G'$ abelsch. Da $G$ isomorph zu einer abelschen Gruppe, nämlich $G'$ ist, ist $G$ selbst abelsch. Das ist aber ein Widerspruch zur Voraussetzung, dass $G$ nicht-abelsch sei. Somit war die Annahme, $\nu_5 = 1$ falsch, es gilt also $\nu_5 > 1$.

Insgesamt ist also $\nu_5 > 1$ und $\nu_p = 1$ für jede von 5 verschiedene Primzahl.
(b) Sei $P$ eine 5-Sylowgruppe von $G$. Wir bestimmen den Isomorphietyp von $N_G(P)$. Aus der Vorlesung ist bekannt, dass die Anzahl $\nu_5$ der Sylowgruppen von $G$ gleich dem Index des Normalisators von $P$ in $G$ ist, d.h., dass $\nu_5 = (G : N_G(P))$. Da $G \geq N_G(P)$ und $G$, also auch $N_G(P)$, endlich sind, liefert uns der Satz von Lagrange, dass $\nu_5 = |G|/|N_G(P)|$. Wir bestimmen also $|N_G(P)| = |G|/\nu_5$. Dazu bestimmen wir die Anzahl der 5-Sylowgruppen von $G$. Nach dem dritten Sylowschen Satz gilt $\nu_5 | |G|/5 = 11 \cdot 13$, also $\nu_5 \in \{1, 11, 13, 143\}$. Zudem gilt ebenfalls nach dem dritten Sylowschen Satz, dass $\nu_5 \equiv 1 \bmod(5)$. Somit sind nur $\nu_5 \in \{1, 11\}$ möglich. Nach Teilaufgabe (a) können wir den Fall, dass $\nu_5 = 1$, ausschließen. Somit ist $\nu_5 = 11$. Das liefert uns nun, dass $|N_G(P)| = |G|/11 = 5 \cdot 13 = 65$. Wir bezeichnen mit $\mu_p$ für jede Primzahl $p$ die Anzahl der $p$-Sylowgruppen von $N_G(P)$. Da $P \trianglelefteq N_G(P)$ nach Definition des Normalisators und $5^1$ die maximale 5-Potenzordnung ist, die $|N_G(P)|$ teilt, ist $\mu_5 = 1$. Für $\mu_{13}$ liefert uns der dritte Sylow'sche Satz, dass $\mu_{13} | 65/13 = 5$ und $\mu_{13} \equiv 1 \bmod(13)$. Somit ist $\mu_{13} = 1$. Sei $Q_{13}$ die einzige 13-Sylowgruppe von $N_G(P)$. Nach dem zweiten sylowschen Satz gilt $Q_{13} \trianglelefteq N_G(P)$. Da $Q_{13}, P \trianglelefteq N_G(P)$ und $\mathrm{ggT}(|P|, |Q_{13}|) = \mathrm{ggT}(5, 13) = 1$, also $Q_{13} \cap P = \{e_G\}$, ist das Komplexprodukt $PQ_{13}$ sogar ein inneres direktes Produkt, $PQ_{13} \leq N_G(P)$. Da $|PQ_{13}| = |P||Q_{13}| = 65 = |N_G(P)|$, folgt zusammen mir $PQ_{13} \subseteq N_G(P)$, dass $PQ_{13} = G$. Mithilfe der aus der Vorlesung bekannten Isomorphie zwischen dem inneren und äußeren direkten Produkt zweier Gruppen finden wir $N_G(P) \simeq P \times Q_{13}$. Da $|P| = 5$, also $P$ von Primzahlordnung ist, gilt $P \simeq \mathbb{Z}/5\mathbb{Z}$. Analog ist $|Q_{13}| = 13$, also $Q_{13}$ von Primzahlordnung, sodass gilt $Q_{13} \simeq \mathbb{Z}/13\mathbb{Z}$. Damit finden wir, dass $N_G(P) \simeq P \times Q_{13} \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}$. Da 5 und 13 teilerfremd sind, sehen wir mithilfe des Chinesischen Restsatzes für Gruppen, dass $N_G(P)$ des Isomorphietyp der zyklischen Gruppe der Ordnung $5 \cdot 13 = 65$ hat. □

**Aufgabe 158 (H16T1A1)** Sei $N$ ein auflösbarer Normalteiler einer endlichen Gruppe $G$ und $H$ eine weitere auflösbare Untergruppe von $G$. Zu zeigen ist, dass $NH$ wiederum eine auflösbare Untergruppe von $G$ ist.
Zunächst ist aus der Vorlesung bekannt, dass $NH \leq G$, da $N \trianglelefteq G$ und $H \leq G$. Zu zeigen ist noch die Auflösbarkeit von $NH$. Hierfür verwenden wir, dass $NH$ genau dann auflösbar ist, wenn $N$ und die Faktorgruppe $NH/N$ auflösbar ist. $N$ ist nach Voraussetzung auflösbar. Nach dem ersten Isomorphiesatz gilt zudem, dass $NH/N \simeq H/(H \cap N)$. Da $H \cap N \trianglelefteq H$ und $H$ auflösbar ist, ist nach dem gleichen Vorlesungsresultat auch $H/(H \cap N)$ und $H \cap N$ auflösbar. Da $NH/N$ isomorph zu einer auflösbaren Gruppe, nämlich $H/(H \cap N)$, ist, ist auch $NH/N$ auflösbar. Da $NH/N$ und $N$ auflösbar sind, liefert uns das eingangs angesprochene Vorlesungsresultat, dass $NH$ auflösbar ist. Insgesamt haben wir also gezeigt, dass $NH$ eine auflösbare Untergruppe von $G$ ist. □

**Aufgabe 159 (F16T2A1)** (a) Sei $p$ eine Primzahl und sei $\mathbb{F}_p$ der Körper mit $p$ Elementen. Es sei bekannt, dass

$$G := \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} | a \neq 0 \right\} \leq \mathrm{GL}_2(\mathbb{F}_p). \tag{202}$$

Zu zeigen ist, dass $G$ auflösbar ist. Zunächst stellen wir fest, dass $G$ offenbar die Ordnung $p(p-1) = |G|$ hat. Nach Definition ist $G$ auflösbar genau dann, wenn $G$ eine Normalreihe mit abelschen Faktor hat. Wir suchen also mittels Homomorphiesatz einen Normalteiler $N \trianglelefteq G$, sodass $G/N$ abelsch ist und $N$ zudem auch abelsch ist. Dann ist $G$ auf jeden Fall auflösbar. Hierzu verwenden wir $\det : G \to \mathbb{F}_p^\times, A \mapsto \det(A)$. Da die Determinantenabbildung laut Vorlesung einen Gruppenhomomorphismus von $\mathrm{GL}_2(\mathbb{F}_p)$ nach $\mathbb{F}_p^\times$ definiert, ist auch die Einschränkung der Determinantenabbildung von $\mathrm{GL}_2(\mathbb{F}_p)$ auf $G \leq \mathrm{GL}_2(\mathbb{F}_p)$ ein Gruppenhomomorphismus. Wir zeigen, dass det wie oben definiert surjektiv ist. Sei dazu $a \in \mathbb{F}_p^\times$ beliebig. Dann ist $a \neq 0$. Betrachte $A \equiv \mathrm{diag}(a, 1)$. Dann gilt $\det(A) = a \cdot 1 - 0 \cdot 0 = a$. Somit ist $\det^{-1}(\{a\}) \neq \emptyset$ für alle $a \in \mathbb{F}_p^\times$ und det mithin surjektiv. Damit können wir den Homomorphiesatz anwenden, der uns liefert, dass

$$G/\ker\det \simeq \mathbb{F}_p^\times. \tag{203}$$

Mittels Satz von Lagrange folgern wir, dass $|\ker\det| = |G|/|F_p^\times| = p(p-1)/(p-1) = p$. Da $p$ eine Primzahl ist, ist $\ker\det \simeq \mathbb{Z}/p\mathbb{Z}$, also zyklisch, damit abelsch und damit auflösbar. Aus der Theorie der endlichen Körper ist ferner bekannt, dass $\mathbb{F}_p^\times$ zyklisch und von Ordnung $(p-1)$ ist. Also gilt $\mathbb{F}_p^\times \simeq \mathbb{Z}/((p-1)\mathbb{Z})$. Somit ist auch $\mathbb{F}_p^\times$ auflösbar, denn $\mathbb{F}_p^\times$ ist als zyklische Gruppe insbesondere abelsch. Da $G/\ker\det$ isomorph zu einer zyklischen Gruppe ist, ist $G/\ker\det$ selbst zyklisch und mit derselben Argumentation wie gerade auch auflösbar. Zusammen mit die Auflösbarkeit von $\ker\det \simeq \mathbb{Z}/p\mathbb{Z}$ als zyklische Gruppe folgt die Auflösbarkeit von $G$.
(b) Sei $G$ eine beliebige Gruppe der Ordnung $p(p-1)$, wo $p$ eine Primzahl bezeichnet. Wir zeigen, dass $G$ genau eine Untergruppe $H$ der Ordnung $p$ hat und $G$ zudem genau dann auflösbar ist, wenn $G/H$ auflösbar ist. Bezeichne für eine Primzahl $q$ mit $\nu_q$ die Anzahl der $q$-Sylowgruppen von $G$. Wir bestimmen die Anzahl $\nu_p$ der $p$-Sylowgruppen von $G$. Es gilt nach dem dritten Sylowschen Satz, dass $\nu_p | p(p-1)/p = p-1$ und zudem $\nu_p \equiv 1 \bmod(p)$. Aus der letzten Relation finden wir, dass nur $\nu_p = 1$ für die Anzahl $\nu_p$ der $p$-Sylowgruppen möglich ist, wenn wir uns auf $\nu_p \leq p-1$ beschränken. Da letzteres durch die Forderung $\nu_p | (p-1)$ bedingt ist, finden wir, dass es genau eine $p$-Sylowgruppe, im Zeichen $H$, von $G$ gibt. Das ist tatsächlich das gesuchte $H$ von Ordnung $p$, da $p^1 = p$ die maximale $p$-Potenz ist, die $|G|$ teilt. Nach dem zweiten Sylowschen Satz gilt zudem $H \trianglelefteq G$. Somit ist auch $G/H$ eine Gruppe. Aus der Vorlesung ist bekannt, dass eine Gruppe $W$ mit einem Normalteiler $N$ genau dann auflösbar ist, wenn $W/N$ und $N$ auflösbar sind. Da $H$ von Primzahlordnung ist, ist $H$ isomorph zur zyklischen Gruppe der Ordnung $p$, die als insbesondere abelsche Gruppe auflösbar ist. Also reduziert sich die oben zitierte Aussage auf die Äquivalenz, dass $G$ von der Ordnung $p(p-1)$ genau dann auflösbar ist, wenn $G/H$ auflösbar ist, wo $H \leq G$ von der Ordnung $p$.
(c) Sei $C := \mathbb{Z}/61\mathbb{Z} \times A_5$. Zunächst gilt $|C| = |\mathbb{Z}/61\mathbb{Z}||A_5| = 61 \cdot 5!/2 = 61 \cdot 60$. Da

$p = 61$ eine Primzahl ist, können wir die Aussage aus Teil (b) auf $C$ anwenden. Wir betrachten hierzu den folgenden Gruppenhomomorphismus $\pi_2 : C \to A_5$, $(a, b) \mapsto b$. Dieser ist als Projektionsabbildung auf den zweiten Faktor im äußeren direkten Produkt offenbar surjektiv, die Homomorphismuseigenschaft ist aus der Vorlesung bekannt. Es ist mit dem Homomorphiesatz und dem Satz von Lagrange leicht zu sehen, dass $|\ker \pi_2| = |C|/|A_5| = 61$. Somit ist $\ker \pi_2 \simeq \mathbb{Z}/61\mathbb{Z}$, also abelsch und damit auflösbar. Wäre $C/\ker \psi$ auflösbar, dann wäre auch $A_5$ auflösbar, da durch $\bar{\pi}_2 : C/\ker \pi_2 \to A_5$ ein Isomorphismus zu einer auflösbaren Gruppen gegeben ist. Aus der Vorlesung ist aber bekannt, dass $A_5$ nicht auflösbar ist. Somit war die Annahme falsch und $C/\ker \psi$ ist nicht auflösbar. Damit ist $C$ nicht auflösbar. □

**Aufgabe 160 (F15T3A2)** Seien $p, q, r$ Primzahlen mit den Eigenschaften, dass $q < p < r$ und $pq < r + 1$. Zu zeigen ist, dass jede Gruppe der Ordnung $pqr$ auflösbar ist. Sei $G$ eine Gruppe der Ordnung $pqr$ mit $p, q, r$ wie beschrieben und bezeichne mit $\nu_s$ für eine Primzahl $s$ die Anzahl der $s$-Sylowgruppen von $G$. Für die Primzahl $r$ gilt für $\nu_r$ nach dem dritten Sylowschen Satz, dass $\nu_r||G|/r = pq$, da $r = r^1$ die höchste $r$-Potenz ist, die $|G|$ teilt. Zudem gilt nach dem dritten Sylowschen Satz, dass $\nu_r \equiv 1 \bmod(r)$. Aus der ersten Bedingung folgt, dass nur $\nu_r \in \{1, p, q, pq\}$ zulässig ist. Da aber $p \equiv p \bmod(r) \not\equiv 1 \bmod(r)$, $q \equiv q \bmod(r) \not\equiv 1 \bmod(r)$ wegen $p < r$ bzw. $q < r$ und $pq \equiv pq \bmod(r) \not\equiv 1 \bmod(r)$, da $pq > 1$ und $pq < r + 1$, ist nur $\nu_r = 1$ möglich. Somit ist die einzige $r$-Sylowgruppe $P_r$ von $G$ nach dem zweiten Sylowschen Satz insbesondere ein Normalteiler. Da $P_r$ von Primzahlordnung ist, gilt $P_r \simeq \mathbb{Z}/r\mathbb{Z}$, d.h., $P_r$ ist zyklisch, damit abelsch und damit auflösbar. Wir betrachten nun die Faktorgruppe $G/P_r$. Diese hat nach dem Satz von Lagrange die Ordnung $pq$. Bezeichne mit $\mu_l$ für eine Primzahl $l$ die Anzahl der $l$-Sylowgruppen von $G/P_r$. Für die Primzahl $p$ finden wir für $\mu_p$ nach dem dritten Sylowschen Satz, dass $\mu_p||G/P_r|/p = q$, denn $p = p^1$ ist die höchste $p$-Potenz, die $G/P_r$ teilt. Zudem gilt nach dem dritten Sylowschen Satz, dass $\mu_p \equiv 1 \bmod(p)$. Die erste Bedingung impliziert, dass $\mu_p \in \{1, q\}$, mit der zweiten Bedingung können wir $\mu_p = q$ ausschließen, denn $q < p$ impliziert zusammen mit der Primzahleigenschaft von $q$, dass $q \equiv q \bmod(p) \not\equiv 1 \bmod(p)$. Somit ist $\mu_p \equiv 1$. Die einzige $p$-Sylowgruppe $Q_p$ von $G/P_r$ ist somit ein Normalteiler laut dem zweiten Sylowschen Satz. Da $|Q_p| = p$, also $Q_p$ von Primzahlordnung ist, ist $Q_p$ zyklisch, damit abelsch und damit auflösbar. Mithilfe des Satzes von Lagrange finden wir, dass die Faktorgruppe $(G/P_r)/Q_p$ die Ordnung $q$ hat. $q$ ist nach Voraussetzung ebenfalls prim, sodass auch $(G/P_r)/Q_p$ zyklisch, damit abelsch und damit auflösbar ist. Da $(G/P_r)/Q_p$ und $Q_p$ auflösbar sind, ist laut Vorlesung auch $G/P_r$ auflösbar. Da $P_r$ und $G/P_r$ auflösbar sind, ist laut Vorlesung auch $G$ auflösbar. Beliebigkeit von $G$ mit den beschriebenen Eigenschaften liefert nun die Behauptung. □

**Aufgabe 161 (H19T3A1)** Seien $a, b, c \in \mathbb{Z}$.
(a) Wir zeigen, dass $\mathrm{ggT}(a, bc)|\mathrm{ggT}(a, b) \cdot \mathrm{ggT}(a, c)$. Sei dazu $d_1 = \mathrm{ggT}(a, b)$. Nach dem Lemma von Bezout gibt es $x, y \in \mathbb{Z}$, sodass $d_1 = xa + yb$. Sei $d_2 = \mathrm{ggT}(a, c)$. Nach dem Lemma von Bezout gibt es $u, v \in \mathbb{Z}$, sodass $d_2 = ua + vc$. Damit gilt $d_1 d_2 = (xa+yb)(ua+vc) = (uxa^2+xvac+yuab+yvbc) = (uxa+xvc+yub)a+yv \cdot bc$. Da $d = \mathrm{ggT}(a, bc)$ die kleinste natürliche Zahl ist, die $a$ und $bc$ teilt, gibt es $X, Y \in \mathbb{Z}$,

sodass $a = Xd$ und $bc = Yd$. Einsetzen liefert $d_1 d_2 = [(uxa + xvc + yub)X + yvY] \cdot d$. Der Ausdruck in der Klammer ist ungleich 0, sodass $d | d_1 d_2$.
(b) Wir zeigen, dass $\mathrm{ggT}(a, bc) \neq \mathrm{ggT}(a, b) \cdot \mathrm{ggT}(a, c)$ im Allgemeinen. Wir setzen dazu $a = b = c = 2$. Dann gilt $\mathrm{ggT}(2, 2^2) = 2$ aber $\mathrm{ggT}(2, 2) = 2$, sodass $\mathrm{ggT}(2, 2 \cdot 2) \neq \mathrm{ggT}(2, 2) \cdot \mathrm{ggT}(2, 2)$.
(c) Seien $b, c$ als teilerfremd vorausgesetzt. Wir zeigen, dass $\mathrm{ggT}(a, bc) = \mathrm{ggT}(a, b)\mathrm{ggT}(a, c)$. Aus Aufgabenteil (a) ist bereits bekannt, dass $\mathrm{ggT}(a, bc) | \mathrm{ggT}(a, b)\mathrm{ggT}(a, c)$. Wir zeigen nun, dass auch $\mathrm{ggT}(a, b)\mathrm{ggT}(a, c) | \mathrm{ggT}(a, bc)$. Im Folgenden seien $k, l \in \mathbb{N}$. Sei nun $p^k$ eine maximale $p$-Potenz für eine Primzahl $p$, die $\mathrm{ggT}(a, b)$ teilt. Analog sei $q^l$ eine maximale $q$-Potenz für eine Primzahl $q$, die $\mathrm{ggT}(a, bc)$ teilt. Nach Definition des größten gemeinsamen Teilers gilt dann erst recht $q^l | c$ und $q^l a$ sowie $p^k | a$ und $p^k | b$. Da $b, c$ nach Voraussetzung teilerfremd sind, gilt nach Definition von $k, l$, dass $p \neq q$. Somit teilt $p^k$ sowohl $a$ als auch $b$ bzw. $q^l$ sowohl $a$ als auch $c$, $q$ teilt aber nicht $b$ und $p$ teilt nicht $b$. Damit ist $\mathrm{ggT}(\mathrm{ggT}(a, b), \mathrm{ggT}(a, c)) = 1$. Da sowohl $\mathrm{ggT}(a, c) | \mathrm{ggT}(a, bc)$ als auch $\mathrm{ggT}(a, c) | \mathrm{ggT}(a, bc)$ folgt $\mathrm{ggT}(a, c) \cdot \mathrm{ggT}(a, b) | \mathrm{ggT}(a, bc)$. □

**Aufgabe 162 (F12T1A3)** Sei $\mathbb{Q} \supseteq R = \{q \in \mathbb{Q} | \exists a, b \in \mathbb{Z} : q = a/b, 2 \nmid b, 3 \nmid b\}$. Bekannt sei, dass es sich bei $R$ um einen Unterring von $\mathbb{Q}$ handelt, der selbst $\mathbb{Z}$ als Teilring enthält.
(a) Wir bestimmen die Einheitengruppe $R^\times$. Definiere

$$T := \{a/b \in R | 2 \nmid a, b, 3 \nmid b\}. \tag{204}$$

Wir behaupten $R^\times = T$. Zu $\supseteq$. Sei $q_1 = a/b \in T$. Dann gilt $2 \nmid a$ und $3 \nmid a$. Somit ist $b/a \in R$. Da zudem $2 \nmid b$ und $3 \nmid b$ gilt sogar $b/a \in T$. Wir rechnen $b/a \cdot a/b = (b \cdot a)/(a \cdot b) = 1 = (a \cdot b)/(b \cdot a) = a/b \cdot b/a$. Somit ist $a/b$ eine Einheit, denn $2 \nmid a, b$ und $3 \nmid a, b$ impliziert $a, b \neq 0$. Zu $\subseteq$. Sei $r \in R^\times$ eine Einheit. Dann ist $r = a/b$, wo $2 \nmid b$ und $3 \nmid b$, also insbesondere $b \neq 0$. Sei $q \in R^\times$ nun dergestalt, dass $rq = 1$. Dann ist $q = c/d$ mit $2 \nmid d$ und $3 \nmid d$. Es gilt nun $1 = rq = (ac)/(bd)$. Angenommen, $2 | (ac)$. Da $\mathbb{Z}$ ein Ring ist, gilt $2 | a$ oder $2 | c$. Die obenstehende Gleichung können wir aber zu $ac = bd$ umformen. Aus $2 | (ac)$ folgte dann $2 | (bd)$, also $2 | b$ oder $2 | c$, da 2 in $\mathbb{Z}$ prim ist. Damit gilt nicht $2 | a$ oder $2 | c$, also $2 \nmid a$ und $2 \nmid c$. Analog schließen wir $3 | (ac)$ aus. Analog zu gerade finden wir also $3 \nmid a$ und $3 \nmid c$. Das bedeutet aber, dass $r = a/b$ die Eigenschaft $2 \nmid a, b$ und $3 \nmid a, b$ hat, also $r \in T$. Damit ist wegen Beliebigkeit von $r \in R^\times$ auch $R^\times \subseteq T$ nachgewiesen. Insgesamt gilt also $R^\times = T$.
(b) Wir sollen zeigen, dass 2 und 3 Primelemente in $R$ sind. Dazu müssen wir zunächst ausschließen, dass es sich bei 2 und 3 um Einheiten handelt. Angenommen, $2 \in R^\times$. Dann gäbe es ein $r = a/b \in R^\times$, sodass $1 = 2 \cdot a/b$, was wir zu $b = 2a$ umformen können. Da $r \in R^\times$, gilt $2 \nmid b$, was aber zu $2 | (2a)$ im Widerspruch steht. Analog schließt man $3 \in R^\times$ aus. Somit sind 2 und 3 also Nicht-Einheiten. Wir zeigen nun, dass für $r_1, r_2 \in R$ gilt: $2 | r_1 r_2 \Rightarrow 2 | r_1$ oder $2 | r_2$ und $3 | r_1 r_2 \Rightarrow 3 | r_1$ oder $3 | r_2$. Seien also $r_1, r_2 \in R$ beliebig. Dann sind $r_1 = a_1/b_1$ und $r_2 = a_2/b_2$ mit $a_1, a_2 \in \mathbb{Z}$ und $b_1, b_2 \in \mathbb{Z}$ mit $2 \nmid b_1, b_2$. Da $2 | r_1 r_2$ gibt es ein $r_3 = a_3/b_3 \in R$ mit $a_3, b_3 \in \mathbb{Z}$ und $2 \nmid b_3$, sodass $2a_3/b_3 = a_1 a_2/(b_1 b_2)$. Letzteres können wir umformen zu $2a_3 b_1 b_2 = a_1 a_2 b_3$. Also gilt $2 | (a_1 a_2 b_3)$ und wegen $2 \nmid b_3$ sogar stärker $2 | (a_1 a_2)$. Da 2 ein Primelement in $\mathbb{Z}$ ist, folgt aus $2 | (a_1 a_2)$, dass $2 | a_2$ oder $2 | a_1$. Falls $2 | a_1$, dann

ist auch $2|a_1/b_1 = r_1$, denn dann gibt es $r' = u_1/v_1 \in R$ sodass $2u_1/v_1 = a_1/b_1$, d.h., $2u_1b_1 = a_1v_1$, also $2|a_1$, da $2 \not| v_1$ wegen $u_1/v_1 \in R$. Analog für $2|a_2$. Analog zum Nachweis, dass 2 Primelement in $R$ ist, verfährt man für den Nachweis, dass 3 Primelement in $R$ ist. Insgesamt sind somit 2 und 3 Primelemente in $R$.
(c) Wir sollen zeigen, dass jedes Primelement $p \in R$ zu 2 oder 3 assoziiert ist. Sei dazu $p \in R$ ein Primelement und $r_1, r_2 \in R$. Da $R$ Integritätsbereich, ist $p$ insbesondere irreduzibel, kann also nicht als Produkt von zwei Nicht-Einheiten geschrieben werden. Wir schließen zunächst aus, dass $2^2|p$. Dann gäbe es ein $r \in R$ mit $p = 2^2 \cdot r = 2(2r)$. 2 ist als Primelement laut (b) eine Nicht-Einheit, ebenso ist $2r \notin R$, da $2r$ ein Vielfaches eines Primelements ist. Damit haben wir eine Zerlegung von $p$ als Produkt von zwei Nicht-Einheiten gefunden, was der Irreduzibilität von $p$ widerspricht. Ebenso schließen wir aus, dass $3^2|p$. Wir schließen nun noch aus, dass $2 \cdot 3|p$. Denn dann gäbe es ein $r = a/b \in R$, sodass $2 \cdot 3 \cdot a/b = 2 \cdot (3 \cdot a/b) = p$ und wir hätten wiederum eine Zerlegung von $p$ in zwei Nicht-Einheiten gefunden. Als Primelement ist $p$ eine Nicht-Einheit, sodass für eine Darstellung von $p$ der Form $p = a/b$ mit $a, b \in \mathbb{Z}$ und $2 \not| b$ sowie $3 \not| b$ nicht gleichzeitig gelten darf $2 \not| a$ und $3 \not| a$. Andernfalls wäre nämlich $p \in R^\times$. Somit ist $p$ in $R$ also entweder genau einmal durch 2 oder genau einmal durch 3 teilbar. Im ersteren Fall finden wir ein $r = c/d \in R$, sodass $2 \cdot c/d = p$. Da $(2 \cdot 3) \not| p$ und $2^2 \not| p$ und $2 \not| d$ sowie $3 \not| d$, ist $2 \not| c$ und $3 \not| c$. Somit ist $c/d \in R^\times$, also eine Einheit. In dem betrachteten Fall, dass $p$ nur genau einmal durch 2 teilbar ist, finden wir, dass $p$ assoziiert zu 2 ist. Analog finden wir für den Fall, dass 3 genau einmal $p$ teilt, dass $p$ assoziiert zu 3 ist. □

**Aufgabe 163 (F13T3A3)** Zu zeigen ist, dass jeder endliche Integritätsbereich $R$ ein Körper ist. Sei $R$ ein endlicher Integritätsbereich. Wir definieren die Abbildung $\phi_x : R \to R, r \mapsto rx$ für ein beliebiges $x \in R \backslash \{0_R\}$. $\phi_x$ ist injektiv, denn seien $r, s \in R$ dergestalt, dass $\phi_x(r) = \phi_x(s)$, dann gilt $rx = sx$ und wegen der Kürzungsregel in einem Integritätsbereich, folgt, dass $x = 0$ oder $r - s = 0$. Ersteres ist nach der Wahl von $x$ ausgeschlossen. Also gilt $r = s$. Damit ist $\phi_x$ injektiv. Aus den Vorlesungen ist bekannt, dass injektive Abbildungen zwischen zwei gleichmächtigen, endlichen Mengen auch surjektiv sind. Somit ist $\phi_x$ bijektiv. Damit gibt es ein $r \in R$, sodass $\phi_x(r) = rx = 1$. Beliebigkeit von $x \in R \setminus \{0\}$ impliziert, dass jedes $x \in R$ ungleich 0 invertierbar ist. Damit ist $R$ bereits ein Körper. □

**Aufgabe 164 (H12T1A4)** Gegeben sei der Ring $R = \mathbb{Z}[1/2(1 + \sqrt{-7})]$. Dieser ist bzgl. der Normfunktion $N : R \to \mathbb{N}_0$ euklidisch.
(a) Wir suchen die Einheitengruppe $R^\times$. Zunächst zeigen wir, dass

$$R = \{a/2 + b/2\sqrt{-7} | a, b \in \mathbb{Z}, a \equiv b \bmod(2)\}. \tag{205}$$

Bezeichne mit $M$ die rechts stehende Menge. Sei für "$\subseteq$" $r \in R$ beliebig. Dann gibt es $c, d \in \mathbb{Z}$, sodass $r = c + d/2(1 + \sqrt{-7}) = (2c + d)/2 + d/2\sqrt{-7}$. Definiere $a = (2c + d) \in \mathbb{Z}$ und $b = d \in \mathbb{Z}$. Dann gilt $a \equiv d \bmod(2)$ und $b \equiv d \bmod(2)$, insbesondere also $a \equiv b \bmod(2)$. Somit ist $r \in M$. Für $r \in M$ beliebig gibt es $a, b \in \mathbb{Z}$ mit $a \equiv b \bmod(2)$, sodass $r = a/2 + b/2\sqrt{-7}$. Wegen $a \equiv b \bmod(2)$ gibt es ein $c \in \mathbb{Z}$, sodass $a = 2c+b$. Damit erhalten wir $r = c+b \cdot 1/2(1+\sqrt{-7}) \in R$. Wir zeigen, dass es sich bei $N$ um eine Höhenfunktion handelt (nicht gefordert). Dazu zeigen wir zuerst,

dass $N$ multiplikativ ist, d.h., dass für $r, s \in R$ gilt $N(rs) = N(r)N(s)$. Seien dazu $a, b, c, d \in \mathbb{Z}$ mit $a \equiv b \bmod(2)$ und $c \equiv d \bmod(2)$ so gewählt, dass $r = a/2 + b/2\sqrt{-7}$, $s = c/2 + d/2\sqrt{-7}$. Dann gilt $rs = (ac + 7db)/4 + \sqrt{-7}(cb - ad)/4$, also

$$N(rs) = \frac{(ac + 7db)^2}{16} + \frac{7(cb - ad)^2}{16} \tag{206}$$

$$= \frac{a^2c^2 + 49d^2b^2 + 7b^2c^2 + 7a^2d^2}{16} \tag{207}$$

Zusätzlich ist

$$N(r)N(s) = \left(\frac{a^2 + 7b^2}{4}\right)\left(\frac{c^2 + 7d^2}{4}\right) \tag{208}$$

$$= \frac{a^2c^2 + 49d^2b^2 + 7b^2c^2 + 7a^2d^2}{16}, \tag{209}$$

also $N(rs) = N(r)N(s)$ für alle $r, s \in R$. Falls nun $r = a/2 + b/2\sqrt{-7} \neq 0$ mit $a, b \in \mathbb{Z}$ und $a \equiv b \bmod(2)$, also vom Nullelement des Rings verschieden ist, gilt $N(r) = r\bar{r} = a^2/4 + 7b^2/4$. Da $a \neq 0$ oder $b \neq 0$, ist $N(r) > 0$ und zusammen mit $N(R) \subseteq \mathbb{N}_0$ folgt die Wohldefiniertheit $N|_{R\setminus\{0\}} : R \setminus \{0\} \to \mathbb{N}$. Sei nun $r, s \in R$ beliebig aber fest mit $s \neq 0$. Dann gibt es $a, b, c, d \in \mathbb{Z}$, sodass $a \equiv b \bmod(2)$, $c \equiv d \bmod(2)$ $c \neq 0$ oder $d \neq 0$ und $r = a/2 + b/2\sqrt{-7}$ und $s = c/2 + d/2\sqrt{-7}$. Wir rechnen in $\mathbb{C}$, dass

$$\frac{r}{s} = \frac{ac + 7db + \sqrt{-7}(cb - ad)}{c^2 + 7d^2} = \frac{ac + 7db}{c^2 + 7d^2} + \sqrt{-7}\frac{cb - ad}{c^2 + 7d^2}. \tag{210}$$

Wir wählen nun $e, f \in \mathbb{Z}$ dergestalt, dass

$$\left|e - \frac{ac + 7db}{c^2 + 7d^2}\right| \leq 1 \;\&\; \left|f - \frac{cb - ad}{c^2 + 7d^2}\right| \leq \frac{1}{2}, \tag{211}$$

und zusätzlich $e \equiv f \bmod(2)$. Die erste Ungleichung stellt sicher, dass wir ein geeignetes Paar $(e, f) \in \mathbb{Z}$ finden können, das die Kongruenz erfüllt. Dann gilt, dass $q = e/2 + f/2\sqrt{-7} \in R$ und wegen Multiplikativität von $N$ (s. oben)

$$0 \leq N(r) = N(x - qy) = N(y)N(x/y - q) \leq N(y)(1/2^2 + 7/2^4) = 11/16N(y) < N(y). \tag{212}$$

Damit haben wir nachgewiesen, dass es sich bei $R$ um einen euklidischen Ring handelt. Wir wenden uns der Bestimmung der Einheitengruppe $R^\times$ zu. Hierzu zeigen wir, dass für $r \in R$ gilt: $r \in R^\times \Leftrightarrow N(r) = 1$. Sei $r$ als Einheit vorausgesetzt. Dann gibt es ein $s \in R\setminus\{0\}$, sodass $rs = 1 \in R$. Damit ist $1 = N(1) = N(rs) = N(r)N(s)$, und wegen $N(R) \subseteq \mathbb{N}_0$ können wir dies nur für $N(s) = 1 = N(r)$ erfüllen. Sei umgekehrt $r \in R$ mit $N(r) = 1$. Dann gilt $4 = a^2 + 7b^2$, wenn $a, b \in \mathbb{Z}$ mit $a \equiv b \bmod(2)$ und $r = a/2 + b/2\sqrt{-7}$. Wir sehen, dass nur $b = 0$ erlaubt, die Gleichung zu lösen. Wegen der Modulo-Relation zwischen $a$ und $b$ ist nur $a \in \{-2, 0, 2\}$ möglich, wenn wir zusätzlich $4 \geq a^2$ erfüllen. Da $r \neq 0$ scheidet $a = 0$ aus und wir finden, dass $r_1 = +1 = 2/2 \neq 0$ und $r_2 = -1 = (-2)/2 \neq 0$ Kandidaten für Einheiten sind, denn

es gilt $r_1^2 = 1$ und auch $r_2^2 = 1$. Zusammen mit der vorher gezeigten Implikationsrichtung haben wir $R^\times = \{-1, 1\}$ gezeigt.
(b) Wir sollen die Primfaktorzerlegung von $r_1 = 3 \in R$, $r_2 = 5 \in R$ und $r_3 = 7 \in R$ bestimmen.

- *Fall* $r_1$. Es gilt $N(r_1) = 3^2$, also erhalten wir eine Zerlegung in irrreduzible Nicht-Einheiten (ungleich Null) höchstens, wenn wir $r, s \in R$ mit $N(r) = 3 = N(s)$ finden können. Das bedeutet aber $12 = a^2 + 7b^2$, wenn $r = a/2 + b/2\sqrt{-7}$ mit $a, b \in \mathbb{Z}$ und $a \equiv b \bmod(2)$. Man sieht leicht, dass 12 kein Quadrat ist und für $|b| = 1$ auch 5 kein Quadrat (jeweils in $\mathbb{Z}$) ist. Somit können wir kein geeignetes $r$ mit $N(r) = 3$ bestimmen und es gibt keine Zerlegung in irreduzible Faktoren. Da jedes irreduzible Element in einem faktoriellen Ring (also in $R$, da $R$ euklidisch ist) auch prim ist, ist $r_1$ prim.

- *Fall* $r_2$. Es gilt $N(r_2) = 5^2$, also erhalten wir eine Zerlegung in irreduzible Faktoren höchstens dann, wenn wir $r, s \in R$ mit $N(r) = 5 = N(s)$ finden können. Das bedeutet aber gerade $20 = a^2 + 7b^2$, wenn $r = a/2 + b/2\sqrt{-7}$ mit $a, b \in \mathbb{Z}$ und $a \equiv b \bmod(2)$. Die Gleichung von gerade eben erfodert für ganzzahlige Lösungen $|b| \leq 1$. Für jede zulässige Wahl von $b \in \{-1, 0, 1\}$ finden wir aber kein $a \in \mathbb{Z}$, sodass $20 = a^2 + 7b^2$. Das bedeutet, dass es ein $r \in R$ mit $N(r) = 5$ nicht gibt. Damit ist $r_2$ als Element aus $R$ mit Primzahlquadratnorm irreduzibel, und da $R$ als euklidischer Ring insbesondere ein Hauptidealbereich, also insbesondere faktoriell, ist, ist $r_2$ somit bereits ein Primelement.

- *Fall* $r_3$. Es gilt $N(r_3) = 7^2$, sodass wir Elemente $r, s \in R$ suchen, die $N(r) = 7 = N(s)$ und $rs = r_3$ erfüllen. Die erste Anforderung stellt sicher, dass $r, s$ irreduzibel, und damit bereits als Element von Primzahlnorm irreduzibel und damit prim sind, da $R$ als euklidischer Ring insbesondere faktoriell ist. Die einzigen verschiedenen Elemente in $R$, die die erste Anforderung erfüllen, sind bis auf Vertauschung $r = \sqrt{-7}$ und $s = -\sqrt{-7}$. Es gilt tatsächlich $rs = 7$. Damit haben wir bis auf Reihenfolge die Primfaktorzerlegung von 7 gefunden, da diese in $R$ als insbesondere faktoriellen Ring eindeutig (bis auf Reihenfolge) ist.

Damit ist die Aufgabe zu Ende. □

**Aufgabe 165 (F12T2A3)** Gegeben sei der Ring $R = \mathbb{Z}[\sqrt{-6}] = \{a+b\sqrt{-6}|a, b\imath\mathbb{Z}\}$. Gesucht sind alle Teiler von 6 in $R$. Aus der Vorlesung ist bekannt, dass $R$ als quadratischer Zahlring insbesondere ein Integritätsbereich ist. Ferner ist auf $R$ durch $N : R \to \mathbb{N}_0, a + b\sqrt{-6} \mapsto a^2 + 6b^2$ die sog. Normfunktion definiert, die auf $R$ multiplikativ ist. Sei nun $r$ ein Teiler von 6. Dann gibt es ein $s \in R$, sodass $rs = 6$. Wegen der Multiplikativität von $N$ folgt $N(rs) = N(r)N(s) = N(6) = 36$. Wir bestimmen nun die Elemente $r \in R$, sodass $N(r)|36$. Es ist also $a^2 + 6b^2|36$ für $r = a + b\sqrt{-6}$. Die Teiler von 36 sind $1, 2, 3, 4, 6, 9, 12, 18, 36$. Elemente $r \in R$ mit $a^2 + 6b^2 = 2$ oder $a^2 + 6b^2 = 3$ gibt es nicht, da es sich bei 2 und 3 um Primzahlen, also insbesondere keine Quadrate handelt und nur $b = 0$ zulässig ist. Für $4 = N(r)$ sehen wir, dass $r \in \{\pm 2\}$. Für $6 = a^2 + 6b^2$ finden wir, dass nur $b \in \{\pm 1\}$ und $a = 0$ Lösungen $r$ der Gleichung $N(r) = 6$ definiert. Für $N(r) = 9$ haben wir $9 = a^2 + 6b^2$ für $r = a + b\sqrt{-6}$

mit $a, b \in \mathbb{Z}$ zu erfüllen. Das ist nur für $r \in \{\pm 3\}$ möglich. Für $N(r) = 12$, also $a^2 + 6b^2 = 12$ sehen wir, dass wiederum nur $b \in \mathbb{Z}$ mit $|b| \leq 1$ zulässig ist. Aber für kein derartiges $b \in \mathbb{Z}$ ist $12 - 6b^2$ ein Quadrat, sodass es kein $a \in \mathbb{Z}$ gibt, das $a^2 = 12 - b^2$ erfüllt. Ebenso verfährt man im Fall $N(r) = 18$. Im Fall $N(r) = 36$ schließlich finden wir, dass nur $a \in \{\pm 6\}$ und $b = 0$ geeignete $r \in R$ definieren. Denn es ist nur die Wahl $|b| \leq 2$ zulässig, aber weder 30 noch 12 ist ein Quadrat, sodass nur der Fall $b = 0$, d.h., $a^2 = 36$ auf ganzzahlige Lösungen $a$ zu untersuchen bleibt. Die letzte Gleichung hat die beiden Lösungen $a \in \{\pm 6\}$. Für den Fall $N(r) = 1$ finden wir noch $r \in \{\pm 1\}$ Damit finden wir, dass die Menge der Teiler von 6, $T_6$, $T_6 = \{\pm 1, \pm 2, \pm 3 \pm \sqrt{-6}, \pm 6\}$ erfüllt, denn in der Tat $1 \cdot 6 = 6$ und $(-1)(-6) = 6$ und $\sqrt{-6}(\sqrt{-6}) = 6$ sowie $(\pm 2)(\pm 3) = 6$. □

**Aufgabe 166 (H13T1A1(b))** Wir behaupten, dass $10 = (1 + i)(1 - i)(2 - i)(1 + i)$ die Primfaktorzerlegung von 10 im Ring der Gaussschen Zahlen $\mathbb{Z}[i] = R$ ist. Dazu beachten wir, dass aus der Vorlesung bereits bekannt ist, dass $R$ mit der Normfunktion $N : R \to \mathbb{N}_0, z \mapsto z\bar{z}$ zu einem euklidischen Ring wird. Die Normfunktion ist aus der Vorlesung ebenfalls als multiplikativ bekannt. Damit sehen wir, dass die obige Darstellung gerade $10 = N(1 + i)N(2 + i) = 2 \cdot 5$ bedeutet, und letzteres eine wahre Aussage ist. Wir haben also tatsächlich eine Zerlegung von 10 in $\mathbb{Z}[i]$ vorliegen. Zudem ist jeder der Faktoren in der Darstellung irreduzibel, denn $N(1 + i) = 2 = N(1 - i)$ und $N(2 + i) = 5 = N(1 - i)$, d.h., die Normen jedes dieser Faktoren evaluiert zu einer Primzahl. Laut Vorlesung ist damit bereits jeder der Faktoren irreduzibel. Da $R$ als euklidischer Ring insbesondere faktoriell ist, ist jedes irreduzible Element bereits prim. Da ferner in einem faktoriellen Ring die Primfaktorzerlegung eindeutig bis auf Reihenfolge und Assoziiertheit ist, haben wir also tatsächlich "die" Primfaktorzerlegung vorliegen. □

**Aufgabe 167 (F14T3A3)** Gegeben sei die Teilmenge $R = \{a + bi\sqrt{2} | a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$.
(a) Wir zeigen, dass $R$ ein Teilring von $\mathbb{C}$ ist. Offenbar gilt $\mathbb{C} \ni 1 = 1 + 0 \cdot i\sqrt{2} \in R$. Seien nun $r, s \in R$ vorgegeben. Wir zeigen, dass $r - s \in R$ und $rs \in R$. Da $r, s \in R$ gibt es $a, b, c, d \in \mathbb{Z}$, sodass $r = a + bi\sqrt{2}$ und $s = c + di\sqrt{2}$. Damit gilt $r - s = (a+bi\sqrt{2})-(c+di\sqrt{2}) = (a-c)+(b-d)i\sqrt{2} \in R$, da die Addition auf $\mathbb{Z}$ wohldefiniert ist. Ebenso rechnen wir $rs = (a + bi\sqrt{2})(c + di\sqrt{2}) = (ac - bd) + (ad + bc)i\sqrt{2} \in R$, da mit $a, b, c, d \in \mathbb{Z}$ auch $ad - bd \in \mathbb{Z}$ und $ad + bc \in \mathbb{Z}$. Somit ist $R$ Teilring von $\mathbb{C}$.
(b) Zu zeigen ist, dass $R$ ein euklidischer Ring bzgl. der Normfunktion $d : R \to \mathbb{N}_0, z \mapsto z\bar{z}$ ist. Es ist klar, dass $R$ ein Integritätsbereich ist, denn $R$ ist ein Teilring des Körpers $\mathbb{C}$. $d$ ist wohldefiniert, denn für alle $r = a + bi\sqrt{2} \in R$ gilt $d(r) = a^2 + 2b^2 \geq 0$ als Summe von Quadraten $a^2, b^2, b^2$. Sei nun $r \in R \setminus \{0\}$. Dann gibt es $a, b \in \mathbb{Z}$ mit $r = a^2 + bi\sqrt{2}$ und $a \neq 0$ oder $b \neq 0$. Falls $a \neq 0, b \neq 0$ ist $d(r) = a^2+2b^2 > 0$. Falls $a = 0, b \neq 0$, dann ist $d(r) = 2b^2 > 0$ und falls $a \neq 0, b = 0$, dann ist $d(r) = a^2 > 0$. Somit ist $d|_{R\setminus\{0\}} : R \setminus \{0\} \to \mathbb{N}$. Seien nun $r = a + bi\sqrt{2}$ und $d = c + di\sqrt{2}$ aus $R$ vorgegeben und $s \neq 0$ vorausgesetzt. Wir zeigen, dass $q, r \in R$ existieren, sodass $x = qy + r$ mit $d(r) < d(y)$. Dazu rechnen wir in $\mathbb{C}$, unter

Beachtung von $s \neq 0$, dass

$$\frac{r}{s} = \frac{(ac+2bd)ii\sqrt{2}(bc-ad)}{c^2+2d^2} \tag{213}$$

und wählen ganze Zahlen $m, n$, sodass

$$\left| m - \frac{ac+2bd}{c^2+2d^2} \right| \leq \frac{1}{2} \ \& \ \left| n - \frac{bc-ad}{c^2+2d^2} \right| \leq \frac{1}{2}. \tag{214}$$

Wir zeigen, dass $d$ multiplikativ ist. Seien dazu $z_1, z_2 \in R$. Dann gilt $d(z_1 z_2) = z_1 z_2 \overline{z_1 z_2} = z_1 z_2 \bar{z}_2 \bar{z}_1 = (z_1 \bar{z}_1)(z_2 \bar{z}_2) = d(z_1) d(z_2)$. Somit ist $d$ auf $R$ multiplikativ. Nun gilt weiter in $\mathbb{R}$, dass $0 \leq d(r) = d(r - qs) = d(s)|r/s - q|^2 \leq d(s)(1/2^2 + 2/2^2) = 3/3d(s)$. Damit ist nachgewiesen, dass $d$ eine Höhenfunktion auf $R$ ist. Somit ist $R$ ein euklidischer Ring.
(c) Gesucht sind alle Faktorisierungen von $r = 8 - i\sqrt{2}$ in irreduzible Element in $R$ bis auf Reihenfolge. Zunächst gilt $r \in R$ und $d(r) = 66$. Sei nun $s \in R$ ein Teiler von $s$. Dann ist $s \neq 0$, da $R$ als Integritätsbereich nullteilerfrei ist und zudem $d(s)|66$, denn es gibt ein $s' \in R \setminus \{0\}$, sodass $ss_1 = r$, und die Multplikativität der Normfunktion $d$ liefert $66 = d(ss') = d(s)d(s')$ und wegen $d(s), d(s') \neq 0$ somit $d(s)|66$. Die Teiler von 66 sind $1, 2, 3, 11, 6, 22, 33, 66$. Da $R$ zudem euklidisch ist, ist die o.g. Zerlegung eindeutig bis auf Einheiten und Reihenfolge. Da $\epsilon \in R^\times \Leftrightarrow d(\epsilon) = 1$ laut Vorlesung, sehen wir schnell, dass $R^\times = \{\pm 1\}$. Der Fall, dass $d(s) = 1$ kann außer Acht bleiben, denn dann ist $s$ bereits eine Einheit. Sei $a, bßin\mathbb{Z}$, sodass $s = a^2 + 2b^2$. Wir finden, dass $2 = a^2 + 2b^2$ nur von $b \in \{\pm 1\}$ gelöst wird, also $s \in \{i\sqrt{2}, -i\sqrt{2}\}$ liefert. Weiter liefert $3 = a^2 + 2b^2$ nur $s \in \{\pm 1 \pm i\sqrt{2}, \pm 1 \mp i\sqrt{2}\}$. Für den Fall $11 = d(s) = a^2 + 2b^2$ finden wir $s \in \{\pm 3 \pm i\sqrt{2}, \pm 3 \mp i\sqrt{2}\}$. Da die so gefundenden Elemente jeweils Primzahlnorm haben, sind sie irreduzibel. Nun gilt

$$(1 + \sqrt{2}i)(3 + i\sqrt{2}) = 1 + 4i\sqrt{2}. \tag{215}$$

Multiplikation mit $-i\sqrt{2}$ liefert $(-i\sqrt{2})(1 + \sqrt{2}i)(3 + i\sqrt{2}) = 8 - i\sqrt{2}$. Wir erhalten nun alle gesuchten Zerlegungen als

$$8 - i\sqrt{2} = (-i\sqrt{2})(1 + i\sqrt{2})(3 + i\sqrt{2}) \tag{216}$$
$$8 - i\sqrt{2} = i\sqrt{2}(-1 - i\sqrt{2})(3 + i\sqrt{2}) \tag{217}$$
$$8 - i\sqrt{2} = i\sqrt{2}(1 + i\sqrt{2})(-3 - i\sqrt{2}) \tag{218}$$
$$8 - i\sqrt{2} = (-i\sqrt{2})(-1 - i\sqrt{2})(-3 - i\sqrt{2}), \tag{219}$$

indem wir alle Fälle getestet haben, wie die drei Faktoren mit den beiden Einheiten $-1$ bzw. 1 multipliziert werden können, sodass das gewünschte $8 - i\sqrt{2}$ als Produkt resultiert. Zusammen mit den eingangs gemachten Bemerkungen ist die obige Auflistung abschließend im Sinne der Aufgabenstellung. □

**Aufgabe 168 (H16T2A5)** Sei $p$ eine Primzahl und $g_1 = x^2 + x + 1 \in \mathbb{F}_p[x], g_2 = x^3 + x^2 + x + 1 \in \mathbb{F}_p[x]$. Gesucht ist die Lösungsmenge $\mathcal{L} \subseteq \mathbb{F}_p[x]$ von $f \equiv x \bmod(g_1)$ und $f \equiv 1 \bmod(g_2)$, wo $f \in \mathbb{F}_p[x]$. $\mathbb{F}_p[x]$ ist als Polynomring über einem endlichen

Körper zusammen mit der Gradfunktion als Höhenfunktion ein euklidischer Ring. Wir stellen zunächst fest, dass $1 = (-x)g_1 + 1 \cdot g_2$ in $\mathbb{F}_p[x]$. Somit sind $g_1, g_2$ teilerfremd in $\mathbb{F}_p[x]$. Wir definieren $f_1 = 1 - (-x)g_1 = x^3 + x^2 + x + 1$ und $f_2 = 1 - 1 \cdot g_2 = -x^3 - x^2 - x$. Dann gilt $f_1 \equiv 1 \bmod(g_1)$ und $f_1 \equiv 0 \bmod(g_2)$ sowie $f_2 \equiv 0 \bmod(g_1)$ und $f_2 \equiv 1 \bmod(g_2)$. Damit ist $f \equiv x \cdot f_1 + 1 \cdot f_2 = x^4 \in \mathbb{F}_p[x]$ und es gilt $f \equiv (xf_1) \bmod(g_1) = x \bmod(f_1)$ sowie $f \equiv (1 \cdot f_2) \bmod(g_2) = 1 \bmod(g_2)$, also eine Lösung der Kongruenz. Wir behaupten nun, dass

$$\mathcal{L} = x^4 + (g_1 g_2) =: M, \tag{220}$$

wo $(g_1 g_2)$ das von $g_1 g_2 \in \mathbb{F}_p[x] =: R$ erzeugte Ideal ist. Da $g_1, g_2$ teilerfremd, gilt $(g_1) + (g_2) = \mathbb{F}_p[x]$. Zudem $(g_1)(g_2) = (g_1 g_2)$. Der Chinesische Restsatz liefert uns einen Isomorphismus

$$\Phi : R/(g_1 g_2) \to R/(g_1) \times R/(g_2), f + (g_1 g_2) \mapsto (f + (g_1), f + (g_2)). \tag{221}$$

Sei nun $f \in M$. Dann gilt $f \equiv x^4 \bmod(g_1) = x \bmod(g_1)$ und $f \equiv x^4 \bmod(g_2) \equiv 1 \bmod(g_1)$. Also ist jedes $f \in M$ auch in $\mathcal{L}$ enthalten. Sei umgekehrt $f \in L$. Dann gilt $f \equiv x \bmod(g_1) \equiv x^4 \bmod(g_1)$ und $f \equiv 1 \bmod(g_2) \equiv x^4 \bmod(g_2)$. Zusammen mit der Bijektivität von $\Phi$ folgt $f + (g_1 g_2) = x^4 + (g_1 g_2)$, also $f \in x^4 + (g_1 g_2) = M$. Damit ist durch $x^4 + (g_1 g_2)$ gerade die Lösungsmenge der simultanen Kongruenz gegeben. □

**Aufgabe 169 (H12T1A5)** (a) Wir wissen $N \in \mathbb{Z}$ und $100 \leq N \leq 200$. Zudem gilt $N \equiv 1 \bmod(11)$ und $N \equiv 3 \bmod(5)$ und $N \equiv 2 \bmod(3)$. Da $3, 5, 11$ paarweise teilerfremd sind, liefert uns der Chnesische Restsatz zunächst einen Isomorphismus

$$\Phi : \mathbb{Z}/165\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}, a + (165) \mapsto (a + (3), a + (5), a + (11)). \tag{222}$$

Wir setzen $n_1' = 55$ und $n_2' = 33$ und $n_3' = 15$. Es gilt $3 \cdot n_3' \equiv 1 \bmod(11)$, $2 \cdot n_2' \equiv 1 \bmod(5)$ und $1 \cdot 55 \equiv 1 \bmod(3)$. Damit sehen wir, dass $n \in \mathbb{Z}$ von der Form $n = 1 \cdot 3 \cdot n_3' + 3 \cdot 2 \cdot \cdot n_2' + 2 \cdot 1 \cdot n_1' + 165 \cdot k = 45 + 198 + 110 + 165k = 353 + 165k = 188 + (k+1)165$ $(k \in \mathbb{Z})$ per Konstruktion die simultane Kongruenz lösen. Da nur $n = 188$ die Bedingungen $100 \leq n \leq 200$ erfüllt, folgt, dass es 188 Tänzer gibt.
(b) Zunächst gilt $57 = 3 \cdot 19$ und 3 und 19 sind als verschiedene Primzahlen teilerfremd. Somit liefert der Chinesische Restsatz den Isomorphismus $\Phi : \mathbb{Z}/57\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/19\mathbb{Z}, (a + (57)) \mapsto (a + (3), a + (19))$. Wir behaupten, dass durch

$$\Psi : \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/19\mathbb{Z} \to \mathbb{Z}/57\mathbb{Z}, (a + (3), b + (19)) \mapsto (19a - 18b + (57)) \tag{223}$$

die Umkehrabbildung gegeben ist. Sei dazu $a + (57) \in \mathbb{Z}/57\mathbb{Z}$. Dann ist $\Phi(a + (57)) = (a + (3), a + (19))$ und $\Psi(a + (3), a + (3)) = (19a - 18a + (57)) = (a + (57))$. Zudem ist für $(a + (3), b + (19)) \in \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/19\mathbb{Z}$ $\Psi(a + (3), b + (19)) = (19a - 18b + (57))$ und $\Phi(19a - 18b + (57)) = (a + (3), -18b + (19)) = (a + (3), b + (19))$. Damit gilt $\Psi = \Phi^{-1}$. □

**Aufgabe 170 (F14T3A2(c))** Sei $R = \mathbb{Q}[x]$ und $g_1 = x^2 + 1$ sowie $g_2 = x^2 - 1$. Gesucht sind alle $f \in R$, sodass $f \equiv 1 \bmod(g_1)$ und $f \equiv x \bmod(g_2)$. Wir stellen zunächst fest, dass in $\mathbb{Q}^{\text{alg}}$ die beiden Polynome $g_1$ bzw. $g_2$ die respektiven Nullstellen $\pm i$ bzw. $\pm 1$ haben. Da sie also in Linearfaktorzerlegung keinen paarweise übereinstimmenden Faktor aufweisen, sind $g_1$ und $g_2$ teilerfremd. Wir sehen zudem, dass $1 = 0.5(x^2+1)+(-0.5)(x^2+1)$. Definiere nun $f_1 = 1-0.5(x^2+1) = 0.5-0.5x^2$ und $f_2 = 1 + 0.5(x^2 - 1) = 0.5x^2 + 0.5$. Dann gilt $f_1 \equiv 1 \bmod(x^2 + 1)$ und $f_1 \equiv 0 \bmod(x^2 - 1)$ sowie $f_2 \equiv 0 \bmod(x^2 + 1)$ und $f_2 \equiv 0 \bmod(x^2 - 1)$. Wir setzen nun $f = 1 \cdot f_1 + x \cdot f_2$. Per Konstruktion erfüllt also $f$ das System von Kongruenzen. Zudem gilt $f = 0.5 + 0.5x - 0.5x^2 + 0.5x^3$. Wir behaupten, dass $\mathcal{L} = 0.5 + 0.5x - 0.5x^2 + 0.5x^3 + (g_1 g_2 = x^4 - 1) =: M$. Hierzu bemerken wir, dass wegen $\text{ggT}(g_1, g_2) = 1$ gilt $(x^2-1)+(x^2+1) = R$ und somit der Chinesische Restsatz den Isomorphismus

$$\Phi : R/(g_1 g_2) \to R/(g_1) \times R/(g_2), f + (g_1 g_2) \mapsto (f + (g_1), f + (g_2)). \tag{224}$$

In der Tat gilt für $F \in M$, dass $F \equiv f \bmod(g_1) = 1 \bmod(g_1)$ und $F \equiv f \bmod(g_2) \equiv x \bmod(g_2)$, wobei wir verwendet haben, dass das $f$ wie oben definiert per Konstruktion eine Lösung der simultanen Kongruenz ist. Umgekehrt gilt für ein $F \in \mathcal{L}$, dass $F \equiv 1 \bmod(g_1) \equiv f \bmod(g_1)$ und $F \equiv x \bmod(g_2) \equiv f \bmod(g_2)$. Da $\Phi$ ein Isomorphismus ist, ist $\Phi$ insbesondere injektiv, sodass $F \equiv f \bmod(g_1 g_2)$, d.h., $F \in f + (g_1 g_2) = M$. Somit gilt $\mathcal{L} = M = 0.5 + 0.5x - 0.5x^2 + 0.5x^3 + (x^4 - 1)$ wie behauptet. □

**Aufgabe 171 (F11T2A1)** Gesucht sind alle ganzzahligen Lösungen der Kongruenz

$$x \equiv 1 \bmod(2) \ \& \ x \equiv 2 \bmod(3) \ \& \ x \equiv 3 \bmod(5). \tag{225}$$

$2, 3, 5$ sind paarweise teilerfremde Primzahlen. Wir setzen $n_1' = 3 \cdot 5 = 15$, $n_2' = 2 \cdot 5 = 10$, $n_3' = 2 \cdot 3 = 6$. Dann gilt $1 \cdot n_1' \equiv 1 \bmod(2)$ und $n_2' \equiv 1 \bmod(3)$ und $n_3' \equiv 1 \bmod(5)$. Wir stellen fest, dass $x_0 := 1 \cdot 1 \cdot n_1' + 2 \cdot 1 \cdot n_2' + 3 \cdot 1 \cdot n_3' = 15 + 20 + 18 = 53$ eine ganzzahlige Lösung der simultanen Kongruenz ist, denn $x_0 \equiv 1 \cdot 1 \cdot n_1' \bmod(2) \equiv 1 \bmod(2)$ und $x_0 \equiv 2 \cdot 1 \cdot n_3' \bmod(3) = 2 \bmod(3)$ und $x_0 \equiv 3 \cdot 1 \cdot n_3' \bmod(5) \equiv 3 \bmod(5)$ jeweils nach Konstruktion der $n_i'$ für $i \in \{1, 2, 3\}$. Es gilt $53 \equiv 23 \bmod(30 = 2 \cdot 3 \cdot 5)$. Bezeichne mit $\mathcal{L} \subseteq \mathbb{Z}$ die Menge aller ganzzahligen Lösungen der simultanen Kongruenz. Wir behaupten, dass $\mathcal{L} = 23 + 30\mathbb{Z} =: M$ die Menge aller ganzzahligen Lösungen der simultanen Kongruenz ist. Dazu beachten wir, dass infolge der paarweisen Teilerfremdheit von $2, 3, 5$ der Chinesische Restsatz den Isomorphismus von Ringen

$$\Phi : \mathbb{Z}/30\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}, a + 30\mathbb{Z} \to (a + 2\mathbb{Z}, a + 3\mathbb{Z}, a + 5\mathbb{Z}) \tag{226}$$

liefert. Sei nun $x \in M$. Dann gilt $x \equiv x_0 \bmod(2) \equiv 1 \bmod(2)$, $x \equiv x_0 \bmod(3) \equiv 2 \bmod(3)$, $x \equiv x_0 \bmod(5) \equiv 3 \bmod(5)$. Damit ist jedes $x \in M$ eine Lösung der simultanen Kongruenz. Sei umgekehrt $x \in \mathcal{L}$. Dann gilt $x \equiv 1 \bmod(2) \equiv x_0 \bmod(2)$, $x \equiv 2 \bmod(3) \equiv x_0 \bmod(3)$, $x \equiv 3 \bmod(5) \equiv x_0 \bmod(5)$. Da $\Phi$ als Isomorphismus insbesondere bijektiv und somit injektiv ist, folgt, dass $x \equiv x_0 \bmod(30)$. Das bedeutet aber gerade, dass $x \in x_0 + 30\mathbb{Z} = 23 + 30\mathbb{Z}$. Somit gilt $\mathcal{L} = 23 + 30\mathbb{Z}$ wie behauptet. □

**Aufgabe 172** Gesucht sind alle Lösungen der simultanen Kongruenz

$$x \equiv 11 \,\mathrm{mod}(72) \;\&\; x \equiv 83 \,\mathrm{mod}(120) \;\&\; x \equiv 173 \,\mathrm{mod}(450). \tag{227}$$

Zum einen gilt $72 = 2^3 \cdot 3^2$ und $120 = 3 \cdot 2^3 \cdot 5$ und $450 = 2 \cdot 5^2 \cdot 3^2$. Wir suchen zuerst eine Lösung der ersten beiden Kongruenzen. Es gilt $\mathrm{ggT}(72, 120) = 24$. Ferner ist $83 = 72 + 11$, also $83 \equiv 11 \,\mathrm{mod}(24)$. Wir setzen also an $x = 11 + 24 \cdot y$, sodass Einsetzen in die ersten beiden Kongruenzen zunächst liefert $y \equiv 0 \,\mathrm{mod}(3)$ und $y \equiv 3 \,\mathrm{mod}(5)$. Damit finden wir, dass $y \in 3+(15)$ eine Lösung des Kongruenzsystems in $y$ ist, also $x \in 83 + (360)$ eine Lösung der ersten beiden Kongruenzen ist. Es gilt also $x \equiv 83 \,\mathrm{mod}(360)$ und $y \equiv 173 \,\mathrm{mod}(450)$. Da gilt $\mathrm{ggT}(360, 450) = 90$ und $360 = 4 \cdot 90$ und $450 = 5 \cdot 90$, berechnen wir $173 \equiv 83 \,\mathrm{mod}(90)$ und setzen nun an $x = 83+90 \cdot z$ und setzen diese Darstellung in die beiden verbleibenden Kongruenzen von gerade eben ein. Die Kürzungsregeln für Kongruenzen liefern dann $z \equiv 0 \,\mathrm{mod}(4)$ und $z \equiv 1 \,\mathrm{mod}(5)$. Damit sehen wir sofort, dass $z \in 16 + (20)$ eine Lösung des $z$-Kongruenzsystems ist. Also $x \in 83+90 \cdot 16+(1800) = 1523+(1800)$ eine Lösung des Kongruenzsystems und $1800 = \mathrm{kgV}(72, 120, 450)$. Denn es gilt $1523 \equiv 11 \,\mathrm{mod}(72)$ und $1523 \equiv 83 \,\mathrm{mod}(120)$ und $1523 \equiv 173 \,\mathrm{mod}(450)$. Somit ist $1523+(1800) \subseteq \mathcal{L}$, wo $\mathcal{L}$ die Menge aller Lösungen des Systems von Kongruenzen bezeichnet. Umgekehrt liefert uns der Chinesischer Restsatz Isomorphismen

$$\Phi : \mathbb{Z}/15\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}, x + (15) \mapsto (x + (3), x + (5)) \tag{228}$$

$$\Psi : \mathbb{Z}/20\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}, x + (20) \mapsto (x + (4), x + (5)), \tag{229}$$

denn $\mathrm{ggT}(3, 5) = 1$ und $\mathrm{ggT}(4, 5)$. Somit liefert die Injektivität von $\Phi$ bzw. $\Psi$, dass die $y$ und $z$ als Lösungen der reduzierten Kongruenzen-Systeme $y \equiv 0 \,\mathrm{mod}(3)$ und $y \equiv 3 \,\mathrm{mod}(5)$ und $z \equiv 0 \,\mathrm{mod}(4)$ und $z \equiv 1 \,\mathrm{mod}(5)$ jeweils in $3 + (15)$ bzw. $16 + (20)$ liegen. Damit liegt $x$ bereits als in $1523 + (1800)$ fest. Also gilt $\mathcal{L} = 1523 + (1800)$.□

**Aufgabe 173 (H19T2A2)** Sei $f(x) \in \mathbb{Z}[x]$.
(a) Wir zeigen für alle $a, b \in \mathbb{Z}$ und $n \in \mathbb{N}$, dass $a \equiv b \,\mathrm{mod}(n) \Rightarrow f(a) \equiv f(b) \,\mathrm{mod}(n)$. Sei $N = \deg(f)$. Da $f \in \mathbb{Z}[x]$, gibt es $a_0, a_1, ..., a_{N-1} \in \mathbb{Z}$ und $a_N \in \mathbb{Z} \setminus \{0\}$, sodass

$f = \sum_{k=0}^{N} a_k x^k$. Es gilt dann für beliebige $a, b \in \mathbb{Z}$ und $n \in \mathbb{N}$ mit $a \equiv b \bmod(n)$

$$\begin{aligned} f(a) &\equiv \left( \sum_{k=0}^{N} a_k a^k \right) \bmod(n) \\ &\equiv \sum_{k=0}^{N} a_k (a^k) \bmod(n) \\ &\equiv \sum_{k=0}^{N} a_k (a \bmod(n))^k \\ &\equiv \sum_{k=0}^{N} a_k (b \bmod(n))^k \\ &\equiv \sum_{k=0}^{N} a_k (b^k) \bmod(n) \\ &\equiv \left( \sum_{k=0}^{N} a_k b^k \right) \bmod(n) \\ &\equiv f(b) \bmod(n), \end{aligned}$$

wie behauptet.
(b) Sei nun $f$ dergestalt, dass $f(0)$ und $f(2019)$ beide ungerade sind. Wir sollen zeigen, dass $f$ keine ganzzahligen Nullstellen hat. Angenommen, $z \in \mathbb{Z}$ ist eine ganzzahlige Nullstelle. Dann gilt $z \equiv 0 \bmod(2)$ oder $z \equiv 1 \bmod(2)$. Im ersten Fall gilt wegen $z \equiv 0 \bmod(2)$, dass $f(z) \equiv f(0) \bmod(2) \equiv 1 \bmod(2)$, da $f(0)$ nach Voraussetzung ungerade ist. Da aber $0 \not\equiv 1 \bmod(2)$ haben wir einen Widerspruch dazu, dass $z$ Nullstelle von $f$ ist. Also kann $z$ zumindest nicht gerade sein. Sei also $z \in \mathbb{Z}$ Nullstelle von $f$ und ungerade, also $z \equiv 1 \bmod(2)$. Dann gilt wegen $z \equiv 1 \bmod(2) \equiv 2019 \bmod(2)$ wiederum nach Teil (a), dass $f(z) \equiv f(2019) \bmod(2) \equiv 1 \bmod(2)$, weil $f(2019)$ laut Voraussetzung ungerade ist. Da aber $0 \not\equiv 1 \bmod(2)$ haben wir so einen Widerspruch dazu, dass $z$ als Nullstelle von $f$ angenommen war. Da jede ganze Zahl entweder gerade oder ungerade ist, haben wir insgesamt gezeigt, dass es keine ganzzahligen Nullstellen von $f$ gibt.
(c) Seien $p$ und $q$ zwei verschiedene Primzahlen und $a, b \in \mathbb{Z}$ mit der Eigenschaft, dass $p \not| f(a)$ und $q \not| f(b)$. Wir behaupten, dass es ein $c \in \mathbb{Z}$ gibt, sodass $f(c)$ weder von $p$ noch von $q$ geteilt wird. Wir zeigen, dass eine Lösung $c \in \mathbb{Z}$ für die simultane Kongruenz $c \equiv a \bmod(p)$ und $c \equiv b \bmod(q)$ existiert. Dann gilt für dieses $c$, dass $f(c) \equiv f(a) \bmod(p)$ und $f(c) \equiv f(b) \bmod(q)$ jeweils nach Teil (a). Da $f(a) \not\equiv 0 \bmod(p)$ und $f(b) \not\equiv 0 \bmod(q)$ folgt, dass $f(c) \not\equiv 0 \bmod(p)$ und $f(c) \not\equiv 0 \bmod(q)$. Mit anderen Worten teilt weder $p$ noch $q$ die ganze Zahl $f(c)$. Das $c$ hat also die gewünschte Eigenschaft. Zum Nachweis der Existenz desselben, bemerken wir, dass wegen $p \neq q$ gilt $\mathrm{ggT}(p, q) = 1$, da es sich bei beiden Zahlen um Primzahlen handelt. Der Chinesische Restsatz liefert uns nun die Existenz eines Ringisomorphismus $\Phi : \mathbb{Z}/(pq\mathbb{Z}) \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}, x + (pq) \mapsto (x + (p), x + (q))$. Da dieser als Isomorphismus surjektiv ist, existiert eine Lösung $c \in \mathbb{Z}$ des Kongruenzensystems. Wir geben diese explizit an: Nach dem Lemma von Bezout finden wir

$\alpha, \beta \in \mathbb{Z}$, sodass $\alpha p + \beta q = 1$. Dann gilt mit $c_1 = 1 - xp$ und $c_2 = 1 - yq$, dass $c_1 \equiv 1 \bmod(p)$ und $c_2 \equiv 1 \bmod(q)$, sowie $c_1 \equiv 0 \bmod(q)$ und $c_2 \equiv 0 \bmod(p)$. Somit sehen wir, dass $c := ac_1 + bc_2 \in \mathbb{Z}$ eine Lösung des gewünschten Kongruenzsystems ist. Dieses hat nach den Ausführungen von weiter oben die gewünschte Eigenschaft. □

**Aufgabe 174** Gegeben sei $R = \mathbb{Z}[i]$, von dem wir als bekannt voraussetzen, dass er euklidisch bzgl. der Normfunktion $N : R \to \mathbb{N}_0, z \mapsto z\bar{z}$ ist. Ferner sei $\alpha, \beta \in R$ gegeben durch $\beta = 2 + i$ und $\alpha = 3 - 2i$, was in der Vorlesung ggf. genau anders herum vorgeschlagen wurde. Wir zeigen, dass $\mathrm{ggT}(\alpha, \beta) = 1$. Dazu setzen wir den erweiterten euklidischen Algorithmus ein.

$$\begin{array}{c|c|cc} - & 3-2i & 1 & 0 \\ - & 2+i & 0 & 1 \\ 1-i & -i & 1 & -1+i \end{array} \tag{230}$$

Damit finden wir $1 \cdot (3 - 2i) + (-1 + i) \cdot (2 + i) = -i$, und da $-i \in R^\times = \{\pm 1, \pm i\}$, $i(3-2i)+(-1-i)(2+i) = 1$. Somit ist einerseits $\mathrm{ggT}(2+i, 3-2i) = 1$ nachgewiesen, anderseits haben wir $\gamma, \delta \in R$ gefunden, sodass $\gamma\alpha + \delta\beta = 1$, indem wir $\gamma = i$, $\delta = -1 - i$ setzen. Nun suchen wir alle $\xi \in R$, sodass $\xi \equiv (1 + i) \bmod(\alpha)$ und $\xi \equiv (5 + 2i) \bmod(\beta)$. Wir definieren zu diesem Zwecke $\xi_1 = 1 - \gamma\alpha = \beta\delta$ und $\xi_2 = 1 - \beta\delta = \alpha\gamma$, wobei wir $1 = \alpha\gamma + \beta\delta$ verwendet haben. Dann gilt $\xi_1 \equiv 1 \bmod(\alpha)$ und $\xi_1 \equiv 0 \bmod(\beta)$ sowie $\xi_1 = 0 \bmod(\alpha)$ und $\xi_2 \equiv 1 \bmod(\beta)$. Wir setzen nun $\xi = (1+i)\xi_1+(5+2i)\xi_2$. Nach dem soeben bewiesenen Eigenschaften von $\xi_1, \xi_2$ folgt, dass $\xi \equiv (1 + i) \bmod(\alpha)$ und $\xi \equiv (5 + 2i) \bmod(\beta)$, d.h., dass $\xi$ das Kongruenzensystem löst. Es gilt zudem

$$\begin{aligned} \xi &= (1+i)\xi_1 + (5+2i)\xi_2 \\ &= (1+i)(-1-3i) + (5+2i)(2+3i) \\ &= -1 - i - 3i + 3 + 10 + 4i + 15i - 6 \\ &= 6 + 15i, \ \& \\ \alpha\beta &= (3-2i)(2+i) \\ &= 6 + 2 - 4i + 3i \\ &= 8 - i. \end{aligned}$$

Da $\mathrm{ggT}(\alpha, \beta) = 1$, gilt $(\alpha) + (\beta) = (1) = R$, sodass $(\alpha), (\beta) \subseteq R$ koprime Ideale in $R$ sind. Der Chinesische Restsatz liefert uns daher einen Isomorphismus

$$\Phi : R/(\alpha\beta) \to R/(\alpha) \times R/(\beta), z + (\alpha\beta) \mapsto (z + (\alpha), z + (\beta)). \tag{231}$$

Wir behaupten nun, dass $M := \xi + (\alpha\beta) = 6 + 15i + (8 - i) = \mathcal{L}$, wo $\mathcal{L}$ die Lösungsmenge der simultanen Kongruenz bezeichnet. Einerseits gilt für $z \in M$, dass $z = \xi + \omega \cdot \alpha\beta$ für ein $\omega \in R$. Damit gilt $z \equiv \xi \bmod(\alpha) = (1 + i) \bmod(\alpha)$ und $z \equiv \xi \bmod(\beta) \equiv (5 + 2i) \bmod(\beta)$, wo verwendet worden ist, dass $\xi$ eine Lösung der simultanen Kongruenz ist. Somit ist $z \in \mathcal{L}$. Für die Umkehrung verwenden wir, dass der Isomorphismus $\Phi$ von Ringen injektiv ist. Für eine Lösung $z \in \mathcal{L}$ der simultanen Kongruenz gilt also $z \equiv (1 + i) \bmod(\alpha) \equiv \xi \bmod(\alpha)$ sowie $z \equiv (5 + 2i) \bmod(\beta) \equiv$

$\xi \bmod(\beta)$, sodass wegen der Injektivität von $\Phi$ bereits $z \equiv \xi \bmod(\alpha\beta)$ folgt. Letzteres bedeutet aber gerade, dass $z \in \xi + (\alpha\beta) = M$. Mithin gilt $M = \mathcal{L}$ und alle Lösungen der simultanen Kongruenz liegen in $M = 6 + 15i + (8 - i)$. □

**Aufgabe 175 (H19T2A1)** (a) Seien $k, l \in \mathbb{N}_0$ mit $k < l$. Betrachte $f, g \in \mathbb{Q}[x]$ definiert durch $f \equiv x^{2^k} + 1$ und $g \equiv x^{2^l} - 1$. Zu zeigen ist, dass $f|g$. Seien dazu $k$ und $l$ aus $\mathbb{N}_0$ beliebig mit $k < l$. Wir fixieren $k$. Es gilt $f|g \Leftrightarrow g \in 0 + (f) \in \mathbb{Q}[x]/(f)$, wo $(f)$ das von $f$ in $\mathbb{Q}[x]$ erzeugte (Haupt-)ideal bezeichnet. Es gilt $(x^{2^k} + 1) \equiv 0 \bmod(f)$, sodass $x^{2^k} \equiv -1 \bmod(f)$. Wir beweisen die Behauptung per Induktion über $l$. Für $l = k + 1$ gilt $x^{2^{k+1}} - 1 \equiv (x^{2^k} - 1)(x^{2^k} + 1) \bmod(f) \equiv (-1 - 1)(-1 + 1) \bmod(f) \equiv 0 \bmod(f)$. Setzen wir nun voraus, dass für ein festes aber beliebiges $l > k$ die zu beweisende Aussage gilt. Setze $g_l = x^{2^l} - 1$. Wir zeigen, dass dann auch $g_{l+1} = x^{2^{l+1}} - 1 \equiv 0 \bmod(f)$. Denn $g_{l+1} = (x^{2^l} + 1) g_l \bmod(f) \equiv \left[(x^{2^l} + 1) \bmod(f)\right] [g_l \bmod(f)] \equiv \left[(x^{2^l} + 1) \bmod(f)\right] [0 \bmod(f)] \equiv 0 \bmod(f)$. Damit ist die Aussage für alle $l > k$ bewiesen.
(b) Setze für $m \in \mathbb{N}$ $n := 2^{2^m} + 1$. Wir zeigen, dass $2^{n-1} \equiv 1 \bmod(n)$. Sei $m ß in \mathbb{N}$ mit $n = 2^{2^n} + 1$ gegeben. Es ist $2^{n-1} \equiv 1 \bmod(n) \Leftrightarrow (2^{2^{2^m}} - 1) \equiv 0 \bmod(2^{2^m} + 1)$. Wir definieren nun die Polynome $f_k := x^{2^k} + 1 \in \mathbb{Q}[x]$ für $k := m$ und $g_l := x^{2^l} - 1 \in \mathbb{Q}[x]$ für $l := 2^m$. Dann gilt $f_k(2) = 2^{2^m} + 1$ und $g_l(2) = 2^{2^{2^m}} - 1$. Wenn wir also allgemein $f_k|g_l$ in $\mathbb{Q}[x]$ zeigen können, dann folgt auch $2^{2^m} + 1 | 2^{2^{2^m}} - 1$ für das fixierte aber beliebige $m$. Um Teil (a) anwenden zu können, zeigen wir, dass $k < l$, also $m < 2^m$ für beliebiges $m \in \mathbb{N}$. Definiere die reellwertige, glatte Funktion $h : \mathbb{R} \to \mathbb{R}, x \mapsto 2^x - x$. Es gilt nun $h(1) = 2^1 - 1 = 1 > 0$ und $h'(x) = \ln(2) \cdot 2^x - 1$, $h''(x) = (\ln(2))^2 2^x > 0$. Da $h'(1) > 0$ und $h''(x) > 0$ für alle $x \geq 1$ ist auch $2^m > m$ für alle $m \in \mathbb{N}$. Teil (a) liefert also $f_k|g_l$, sodass die zu beweisende Aussage gemäß den obenstehenden Ausführungen folgt. □

**Aufgabe 176 (H16T1A4)** Sei $a \in \mathbb{N}_0$. Zu zeigen ist für die Folge $(x_n)_{n \in \mathbb{N}_0}$ definiert durch $x_n = a^{2^n} + 1$ für alle $n \in \mathbb{N}$: (a) Für $n < m$ gilt $x_n | x_m - 2$. Seien $n, m \in \mathbb{N}_0$ mit $n < m$. Wir definieren das Polynom $f_n := x^{2^n} + 1 \in \mathbb{Q}[x]$ und $g_m := x^{2^m} - 1 \in \mathbb{Q}[x]$. Es gilt dann für das oben genannte $a \in \mathbb{N}_0$ $f_n(a) = a^{2^n} + 1 = x_n$ und $g_m(a) = a^{2^m} - 1 = (a^{2^m} + 1) - 2 = x_m - 2$. Wenn wir $f_n|g_m$ zeigen können, dann folgt $x_n|(x_m - 2)$, also die zu zeigende Behauptung. Wir zeigen $f_n|g_m$ durch Fixierung von $n \in \mathbb{N}$ und Induktion über $m > n$. Sei $m = n + 1$ zunächst. Dann gilt $g_m(x) = (x^{2^m} - 1) = x^{2^{n+1}} - 1 = (x^{2^n} + 1)(x^{2^n} - 1) = (x^{2^n} - 1) f_n(x)$, sodass $f_n|g_{m=n+1}$, denn $x^{2^n} - 1 \in \mathbb{Q}[x]$. Wir setzen nun für ein festes aber beliebiges $m > n$ die Gültigkeit von $f_n|g_m$ voraus, und zeigen, dass dann auch $f_n|g_{m+1}$. Denn $g_{m+1}(x) = x^{2^{m+1}} - 1 = (x^{2^m} - 1)(x^{2^m} + 1) = (x^{2^m} + 1) g_m(x)$. Da $f_n|g_m$, gilt erst recht $f_n|(x^{2^m} + 1) g_m$, also $f_n|g_{m+1}$. Damit ist $f_n|g_m$ für $m > n$ gezeigt. Nach den obenstehenden Bemerkungen ist damit auch die Behauptung bewiesen.
(b) Wir bestimmen $0 < d_{m,n} := \mathrm{ggT}(x_m, x_n)$ für $m > n$. Da $x_n|(x_m - 2)$ und $x_n, x_m \neq 0$, gibt es ein $0 \neq y \in \mathbb{Z}$, sodass $x_m - 2 = y \cdot x_n$. Das können wir umformen zu $x_m - y \cdot x_n = 2$. Somit ist $d_{m,n}|2$, also $d_{m,n} \in \{1, 2\}$. Falls $a$ ungerade ist, dann ist $x_n, x_m$ für alle $n, m \in \mathbb{N}$ offenbar gerade. Damit gilt $2|d_{m,n}$ und zusammen mit $d_{m,n} \in \{1, 2\}$ folgt $d_{m,n} = 2$. Falls $a$ gerade ist, dann ist $x_n, x_m$ ungerade. Damit

gilt $2 \nmid x_m$ und $2 \nmid x_n$. Somit ist auch $2 \nmid d_{m,n}$, denn andernfalls hätten wir einen Widerspruch dazu, dass $x_n, x_m$ ungerade sind. Für den Fall, dass $a$ gerade ist, gilt also $d_{n,m} = 1$.
(c) Setze $a = 2$. Dann ist $x_n$ ungerade für alle $n$, wie in Teil (b) beobachtet, und $x_0 = 5$, eine Primzahl. Nach Teil (b) gilt $\mathrm{ggT}(x_n, x_m) = 1$ für alle $m < n$. Indem wir $p_m$ als den größten Primteiler von $x_m$ für alle $m \in \mathbb{N}_0$ definieren, erhalten wir so eine Folge $(p_m)_{m\in\mathbb{N}_0}$ von Primzahlen. Diese hat paarweise verschiedene Glieder, denn andernfalls gäbe es zwei $M, N \in \mathbb{N}_0$ mit $M > N$, sodass $p_M = p_N =: p$. Damit wäre aber $p|x_N$ und $p|x_M$ nach Definition der Folge $(p_m)_{m\in\mathbb{N}_0}$, was $\mathrm{ggT}(x_M, x_N) = 1$ wegen $a$ gerade nach Teil (b) widerspricht. Somit ist $(p_m)_{m\in\mathbb{N}_0}$ eine (unendliche) Folge von (verschiedenen) Primzahlen. Es gibt also auf jeden Fall unendlich viele Primzahlen. □

**Aufgabe 177 (F19T3A1)** Sei $p$ eine Primzahl und definiere $\mathbb{Z}_{(p)} = \{a/b \in \mathbb{Q} | a, b \in \mathbb{Z}, p \nmid b\}$. Es gilt, dass $\mathbb{Z}_{(p)}$ ein Teilring von $\mathbb{Q}$ ist.
(a) Zu zeigen ist, dass $\bar{\Phi} : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}$ definiert durch $\bar{\Phi}(a+p\mathbb{Z}) = a+p\mathbb{Z}_{(p)}$ ein Ringisomorphismus ist. Hierzu definieren wir die Abbildung $\Phi : \mathbb{Z} \to \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}, a \mapsto a+p\mathbb{Z}_{(p)}$. Diese ist wohldefiniert, denn $\mathbb{Z} \subseteq \mathbb{Z}_{(p)}$. Wir zeigen, dass es sich bei $\Phi$ sogar um einen Ringhomomorphismus handelt. Zunächst ist $\Phi(1) = 1+p\mathbb{Z}_{(p)}$. Für $a, b \in \mathbb{Z}$ gilt $\Phi(a+b) = (a+b)+p\mathbb{Z}_{(p)} = (a+p\mathbb{Z}_{(p)}) + (b+p\mathbb{Z}_{(p)}) = \Phi(a) + \Phi(b)$. Zudem gilt $\Phi(a)\Phi(b) = (a+p\mathbb{Z}_{(p)})(b+p\mathbb{Z}_{(p)}) = ab+(a+b)p\mathbb{Z}_{(p)}+(p\mathbb{Z}_{(p)})2 = ab+p\mathbb{Z}_{(p)} = \Phi(ab)$. Somit ist $\Phi$ ein Ringhomomorphismus. Wir zeigen, dass $\Phi$ zudem surjektiv ist. Sei dazu $a/b+p\mathbb{Z}_{(p)}$ mit $a, b \in \mathbb{Z}$ und $p \nmid b$ vorgegeben. Da $p$ eine Primzahl ist und $p \nmid b$ gilt sogar $\mathrm{ggT}(b, p) = 1$. Nach dem Lemma von Bezout gibt es dann $x, y \in \mathbb{Z}$, sodass $xb + yp = 1$. Das können wir umformen in $\mathbb{Q}$, sodass $x + py/b = 1/b$. Damit ist $a/b + p\mathbb{Z}_{(p)} = a(1/b + p\mathbb{Z}_{(p)}) = a(x + py/b + p\mathbb{Z}_{(p)}) = ax + p\mathbb{Z}_{(p)} = \Phi(ax)$. Damit ist der Nachweis der Surjektivität von $\Phi$ abgeschlossen. Der Homomorphiesatz für Ringe liefert nun, dass $\Phi$ einen Isomorphismus von Ringen, $\bar{\Phi} : \mathbb{Z}/\ker\Phi \to \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}$ induziert. Es gilt zudem für $a \in \mathbb{Z}$ die Äquivalenz $a \in \ker\Phi \Leftrightarrow \Phi(a) = 0 \Leftrightarrow a + p\mathbb{Z}_{(p)} = 0 + p\mathbb{Z}_{(p)} \Leftrightarrow a \in p\mathbb{Z}_{(p)} \Leftrightarrow p|a \Leftrightarrow a \in p\mathbb{Z}$, sodass $\ker\Phi = p\mathbb{Z}$. Damit ist nachgewiesen, dass es sich bei $\bar{\Phi}$ tatsächlich um den angegebenen Isomorphismus $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}$ handelt.
(b) Sei nun $p = 5$. Wir sollen ein $y \in \{0, 1, 2, 3, 4\}$ bestimmen, sodass $\Phi(y) = (2/3 + 5\mathbb{Z}_{(5)}) + (1/7 + 5\mathbb{Z}_{(5)})$. Zunächst gilt $2/3 + 1/7 \equiv 17/21 \bmod (5\mathbb{Z}_{(5)})$. Wie im Nachweis der Surjektivität von $\bar{\Phi}$ für allgemeine Primzahlen $p$, bestimmen wir $(-4)\cdot 5 + 21 = 1$, sodass $1/21 = 1 + 5 \cdot (-4)/21$. Damit ist für $\bar{\Phi} : \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}_{(5)}/5\mathbb{Z}_{(5)}$, gegeben wie in Teil (a) spezifiziert, dass $\bar{\Phi}(2 + 5\mathbb{Z}) = \bar{\Phi}(17 + 5\mathbb{Z}) = 17\bar{\Phi}(1 + 5\mathbb{Z}) = 17/21 + 5\mathbb{Z}_{(5)}$. Damit erfüllt $y = 2$ die geforderte Eigenschaft. □

**Aufgabe 178 (H17T1A4)** (a) Sei $\omega = -1/2 + i\sqrt{3}/2$. Betrachte $\phi : \mathbb{Q}[x] \to \mathbb{C}, f \mapsto f(\omega)$. Das ist ein Ringhomomorphismus. Wir suchen $\dim_{\mathbb{Q}} \mathrm{Bild}(\phi)$. Zunächst ist $|\omega| = \sqrt{\Re[\omega]^2 + \Im[\omega]^2} = 1$ und $\sin(2\pi/3) = \sqrt{3}/2, \cos(2\pi/3) = -1/2$. $\omega$ ist also eine dritte Einheitswurzel, d.h., eine Nullstelle von $\Phi_3(x) = x^2 + x + 1$. Dieses ist nach dem Reduktionskriterium für $p = 2$ irreduzibel über $\mathbb{Q}$ und wegen zusätzlicher Normiertheit das Minimalpolynom von $\omega$. Somit gilt $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$. Wir zeigen nun, dass $\mathrm{Bild}(\phi) = \mathbb{Q}(\omega)$. Es ist $\phi(\mathbb{Q}[x]) = \{f(\omega) | f \in \mathbb{Q}[x]\} = \mathbb{Q}[\omega]$ und $\mathbb{Q}(\omega) =$

$\{f(\omega)|f \in \mathbb{Q}[x], \deg(f) \leq 1\}$, wobei die zusätzliche Einschränkung aus $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$ folgt. Damit ist klar, dass $\mathbb{Q}(\omega) \subseteq \mathbb{Q}[\omega]$, denn $\mathbb{Q}(\omega)$ ist als Teilkörper von $\mathbb{C}$ insbesondere Teilring von $\mathbb{C}$. Andererseits ist $\mathbb{Q}[\omega]$ definitionsgemäß der kleinste Teilring von $\mathbb{C}$, der $\omega$ und $\mathbb{Q}$ enthält. Wegen $\mathbb{Q} \cup \{\omega\} \subseteq \mathbb{Q}(\omega)$ folgt $\mathbb{Q}[\omega] \subseteq \mathbb{Q}(\omega)$. Insgesamt haben wir also Gleichheit, $\mathbb{Q}(\omega) = \mathbb{Q}[\omega]$.
(b) Da $\Phi_3$ als drittes Kreisteilungspolynom insbesondere Minimalpolynom von $\omega$ ist, gilt die Äquivalenz $f \in \ker\phi \Leftrightarrow f(\omega) = 0 \Leftrightarrow g|\Phi_3 \Leftrightarrow f \in (\Phi_3)$. Somit ist $\ker\phi = (\Phi_3)$.
(c) Da $\Phi_3$ als Minimalpolynom von $\omega$ ein über $\mathbb{Q}$ irreduzibles Polynom ist, und $\mathbb{Q}[x]$ als Polynomring über eine Körper ein Hauptidealring ist, ist $(\Phi_3)$ maximales Ideal in $\mathbb{Q}[x]$. Zusammen mit $\ker\phi = (\Phi_3)$ aus Teil (b) folgt, dass $\ker\phi$ maximales Ideal in $\mathbb{Q}[x]$ ist. □

**Aufgabe 179 (F16T2A2)** Sei $R = \mathbb{Z}[i]$ und $R \supseteq I = (25, 7 + i)$.
(a) Zu zeigen ist, dass $\phi : \mathbb{Z} \to R/I, a \mapsto a+I$ surjektiv ist. Zunächst gilt $7+i+I = 0+I$, sodass $i+I = -7+I$. Sei nun $z \in R/I$ vorgegeben. Dann gibt es $x, y \in \mathbb{Z}$, sodass $z = x+yi+I = (x-7y)+I$ und $x-7y \in \mathbb{Z}$. Damit ist $\phi(x-7y) = x-7y+I = x+iy+I$. Beliebigkeit von $z$ impliziert nun die Surjektivität. Wir bestimmen nun $\ker\phi$. Es gilt die Äquivalenz $a \in \ker\phi \Leftrightarrow \phi(a) = 0 \Leftrightarrow a + I = 0 + I \Leftrightarrow a \in I \Leftrightarrow \exists x, y \in \mathbb{Z} : \mathbb{Z} \ni a = x \cdot 25 + (7 + i)y \Leftrightarrow \exists x \in \mathbb{Z} : a = 25x \Leftrightarrow a \in 25\mathbb{Z}$. Damit ist $\ker\phi = 25\mathbb{Z}$.
(b) Wir sollen zeigen, dass $(R/I)^\times$ zyklisch und von Ordnung 20 ist. Da $\phi$ surjektiv ist, und als Komposition der (Ring-)Inklusion $\iota : \mathbb{Z} \to \mathbb{Z}[i]$, die aus der Vorlesung als Homomorphismus bekannt ist, und des kanonischen Epimorphismus $\pi_I : \mathbb{Z}[i] \to \mathbb{Z}[i]/I$ selber ein Homomorphismus ist, können wir den Homomorphiesatz für Ringe anwenden. Dieser liefert uns einen von $\phi = \pi_I \circ \iota$ induzierten Isomorphismus $\bar{\Phi} : \mathbb{Z}/\ker\phi \to R/I$. Wegen $\ker\phi = 25\mathbb{Z}$ finden wir $\bar{\Phi} : \mathbb{Z}/25\mathbb{Z} \to R/I$. Daher gilt auch für die Einheitengruppen $(R/I)^\times \simeq (\mathbb{Z}/25\mathbb{Z})^\times$ als Gruppen. Da $(\mathbb{Z}/25\mathbb{Z})^\times \simeq \mathbb{Z}/\Phi(5^2)\mathbb{Z}$ mit der Euler'schen $\Phi$-Funktion laut Vorlesung, und $\Phi(5^2) = 5 \cdot (5-1) = 20$, finden wir $(\mathbb{Z}/5^2\mathbb{Z})^\times \simeq \mathbb{Z}/20\mathbb{Z}$. Die Einheitengruppe von $\mathbb{Z}/25\mathbb{Z}$, und damit auch $(R/I)^\times$, ist also zyklisch von Ordnung 20.
(c) Da $(R/I)^\times \simeq \mathbb{Z}/20\mathbb{Z}$ langt es, die Anzahl der erzeugenden Elemente für die rechts stehende Gruppe zu bestimmen. Laut Vorlesung ist deren Anzahl gegeben durch $\Phi(20) = \Phi(4)\Phi(5) = (2-1) \cdot 2 \cdot (5-1) = 8$. Es gibt also 8 erzeugende Elemente von $(R/I)^\times$. □

**Aufgabe 180 (F19T2A4)** Wir sollen jeweils entscheiden, ob es sich bei den vorliegenden Faktorringen um Körper handelt.
(a) Wir behaupten, $\mathbb{Q}[x]/(x^5 - 2, x^6 + x^5 - x - 2)$ ist ein Körper. Zunächst gilt $x^6 + x^5 - 2x - 2 = (x + 1)(x^5 - 2)$. Da $(x^5 - 2) \subseteq (x^5 - 2, x^6 + x^5 - x - 2)$ und auch $(x^5 - 2, x^6 + x^5 - x - 2) \subseteq (x^5 - 2)$, weil $x^6 + x^5 - x - 2 \in (x^5 - 2)$ wegen der eingangs gemachten Rechnung ist $(x^5 - 2) = (x^6 + x^5 - x - 2, x^5 - 2)$. Wir müssen also nur zeigen, dass $\mathbb{Q}[x]/(x^5 - 2)$ ein Körper ist. Dazu beachten wir, dass $x^5 - 2$ sogar in $\mathbb{Z}[x]$ und primitiv ist. Mittels Eisenstein-Kriterium zur Primzahl $p = 2$ sehen wir, dass $x^5 - 2$ über $\mathbb{Z}$ und, nach Gauss, auch in $\mathbb{Q}[x]$ irreduzibel ist. Da $\mathbb{Q}[x]$ als Polynomring über einem Körper ein Hauptidealring ist, ist $(x^5 - 2)$ maximal. Das bedeutet aber, dass $\mathbb{Q}[x]/(x^5 - 2)$ ein Körper ist.

(b) Wir zeigen, dass $\mathbb{Z}[x]/(5, x^3 - 2x^2 + 4)$ ein Körper ist. Zunächst zeigen wir, dass $\mathbb{Z}[x]/(5, x^3 - 2x^2 + 4) \simeq \mathbb{F}_5[x]/(x^3 - 2x + 4)$. Hierzu definieren wir $\phi : \mathbb{Z}[x] \to \mathbb{F}_5[x]/(x^3 - 2x^2 + 4), f \mapsto \bar{f} \bmod(\bar{g})$, wo $\bar{g} = x^3 - 2x^2 + 4 \in \mathbb{F}_5[x]$ und $\bar{f}$ das modulo 5 reduzierte $f$ ist. Wegen $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$, da 5 prim ist, ist $\phi$ als Komposition des Reduktionsepimorphismus auf Polynomringen, $\mathrm{mod}(5) : \mathbb{Z}[x] \to \mathbb{Z}/5\mathbb{Z}[x]$, und des kanonischen Epimorphismus $\pi_{(\bar{g})} : \mathbb{F}_5[x] \to \mathbb{F}_5[x]/(\bar{g})$ ebenfalls ein surjektiver Homomorphismus von Ringen. Der Homomorphiesatz liefert also $\mathbb{Z}[x]/\ker\phi \simeq \mathbb{F}_5[x]/(\bar{g})$. Wir zeigen nun, dass $\ker\phi = (5, x^3 - 2x^2 + 4)$. Sei $g = x^3 - 2x^2 + 4 \in \mathbb{Z}[x]$ und $\bar{g} = x^3 - 2x^2 + 4 \in \mathbb{F}_5[x]$ gesetzt. Betrachte dazu die Äquivalenz: $f \in \ker\phi \Leftrightarrow \phi(f) = 0 + (\bar{g}) \Leftrightarrow \exists h \in \mathbb{F}_5[x] : \bar{h}\bar{g} \equiv f \bmod(5) \Leftrightarrow \exists \bar{h} \in \mathbb{F}_5[x] : (f - \bar{h}\bar{g}) \equiv 0 \bmod(5) \Leftrightarrow \exists h, H \in \mathbb{Z}[x] : f - hg = 5H \Leftrightarrow \exists h, H \in \mathbb{Z}[x] : f = 5 \cdot H + g \cdot H \Leftrightarrow f \in (5, x^3 - 2x^2 + 4)$. Damit haben wir in der Tat $\mathbb{Z}[x]/(5, x^3 - 2x^2 + 4) \simeq \mathbb{F}_5[x]/(x^3 - 2x + 4)$. Wir zeigen nun, dass $\bar{g} = x^3 - 2x^2 + 4$ irreduzibel in $\mathbb{F}_5[x]$ ist. Da $\deg(\bar{g}) = 3$, ist $\bar{g}$ keine Einheit ist, und es reicht, zu zeigen, dass $\bar{g}$ keine Nullstelle in $\mathbb{F}_5$ hat. Denn wäre $\bar{g}$ reduzibel, so wäre einer der irreduzibel Faktoren ein Polynom vom Grad 1 in $\mathbb{F}_5[x]$, was hieße, dass $\bar{g}$ eine Nullstelle in $\mathbb{F}_5$ hat. Es gilt aber $\bar{g}(0) = 4 \neq 0$, $\bar{g}(1) = 3 \neq 0, \bar{g}(2) = 4 \neq 0, \bar{g}(3) = 13 = 3 \neq 0, \bar{g}(4) = 36 = 1 \neq 0$. Damit ist $\bar{g}$ als Polynom vom Grad 3 irreduzibel in $\mathbb{F}_5[x]$. Da $\mathbb{F}_5[x]$ als Polynomring über einem Körper ein Hauptidealring ist, ist das vom irreduziblen Element $\bar{g}$ erzeugte Ideal $(\bar{g}) = (x^3 - 2x^2 + 4)$ maximal. Damit ist der Faktorring $\mathbb{F}_5[x]/(\bar{g})$ bereits ein Körper. Somit ist auch $\mathbb{Z}[x]/(5, x^3 - 2x^2 + 4)$ als zu einem Körper isomorpher (bzgl. eines Ringisomorphismus) Ring ein Körper. □

**Aufgabe 181 (F18T3A4)** (a) Wir sollen zeigen, dass $\mathbb{Q}[x]/(x^4 - 12x + 2)$ ein Integritätsbereich ist. Dazu bemerken wir, dass $x^4 - 12x + 4 \in \mathbb{Z}[x] \subseteq \mathbb{Q}[x]$ als normiertes Polynom insbesondere primitiv ist. Nach dem Eisensteinkriterium zur Primzahl 2 ist $x^4 - 12x + 4$ irreduzibel über $\mathbb{Z}$, somit laut dem Lemma von Gauss also auch über $\mathbb{Q}$. Da $\mathbb{Q}[x]$ als Polynomring über einem Körper ein Hauptidealring ist, ist $(x^4 - 12x + 4)$ ein maximales Ideal, da von einem irreduziblen Element aus $\mathbb{Q}[x]$ erzeugt. Das bedeutet aber, dass $\mathbb{Q}[x]/(x^4 - 12x + 2)$ ein Körper ist. Da jeder Körper ein Integritätsbereich ist, haben wir die Behauptung gezeigt.
(b) Wir sollen zeigen, dass $\mathbb{Z}[x]/(2, x^2 + x + 1)$ ein Körper ist und bestimmen, wie viele Elemente er hat. dazu zeigen wir zunächst, dass $\mathbb{Z}[x]/(2, x^2 + x + 1) \simeq \mathbb{F}_2[x]/(x^2 + x + 1)$, wo $\mathbb{F}_2$ den Körper mit zwei Elementen bezeichnet. Sei dazu $\phi : \mathbb{Z}[x] \to \mathbb{F}_2[x]/(x^2 + x + 1), f \mapsto \bar{f} \bmod(x^2 + x + 1)$. $\bar{f}$ bezeichnet hierbei die Reduktion von $f$ modulo 2. Da $\phi$ die Komposition des Reduktionsepimorphismus $\mathrm{mod}(2) : \mathbb{Z}[x] \to \mathbb{Z}/2\mathbb{Z}[x]$ und $\mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2$ sowie des kanonischen Epimorphismus $\pi_{(x^2+x+1)} : \mathbb{F}_2[x] \to \mathbb{F}_2[x]/(x^2 + x + 1)$ ist, ist $\phi$ ein Homomorphismus und surjektiv. Wir zeigen, dass $\ker\phi = (2, x^2 + x + 1)$. Es gilt: $f \in \ker\phi \Leftrightarrow \phi(f) = 0 + (x^2 + x + 1) \leftrightarrow x^2 + x + 1 | \bar{f} \Leftrightarrow \exists \bar{h} \in \mathbb{F}_2[x] : \bar{f} = \bar{h}(x^2 + x + 1) \Leftrightarrow \exists h \in \mathbb{Z}[x] : f \equiv h(x^2 + x + 1) \bmod(2) \Leftrightarrow \exists h, h \in \mathbb{Z}[x] : f = h(x^2 + x + 1) + 2H \Leftrightarrow f \in (2, x^2 + x + 1)$. Somit ist $\ker\phi = (2, x^2 + x + 1)$. Da $x^2 + x + 1$, wie man durch Einsetzen sieht, keine Nullstelle in $\mathbb{F}_2$ hat, ist es als Polynom vom Grad 2 irreduzibel über $\mathbb{F}_2$. Da $\mathbb{F}_2[x]$ als Polynomring über einem Körper bereits ein Hauptidealring ist, ist $(x^2 + x + 1)$ ein maximales Ideal in $\mathbb{F}_2[x]$. Laut Vorlesung ist dann der Faktorring $\mathbb{F}_2[x]/(x^2 + x + 1)$ ein Körper. Sei nun $\omega \in \mathbb{F}_2^{\mathrm{alg}}$, einem algebraischen Abschluss von $\mathbb{F}_2$, eine Nullstelle von $x^2 + x + 1$.

Da $x^2 + x + 1$ normiert und irreduzibel ist, ist $x^2 + x + 1$ das Minimalpolynom von $\omega$. Da $\deg(x^2 + x + 1) = 2$, ist auch $[\mathbb{F}_2(\omega) : \mathbb{F}_2] = 2$. Wir betrachten nun den Einsetzungshomomorphismus $\chi : \mathbb{F}_2[x] \to \mathbb{F}_2[\omega]$. Dieser ist als surjektiv bekannt, und zudem ist $\ker \chi = (x^2 + x + 1)$. Damit ist $\mathbb{F}_2[\omega] \simeq \mathbb{F}_2[x]/\ker \chi$. Da $\mathbb{F}_2[\omega] \subseteq \mathbb{F}_2(\omega)$ als kleinster Teilring, der $\mathbb{F}_2$ und $\omega$ enthält und $\mathbb{F}_2(\omega) = \{f(\omega) | f \in \mathbb{F}_2[x] : \deg(f) \leq 1\}$, folgt $\mathbb{F}_2[x]/(x^2 + x + 1) \simeq \mathbb{F}_2(\omega)$, wobei $\ker \chi = (x^2 + x + 1)$ erinnert wurde. Als $\mathbb{F}_2$-Vektorraum vom Grad 2 enthält $\mathbb{F}_2(\omega)$ und damit $\mathbb{F}_2[x]/(x^2 + x + 1)$ $2^2 = 4$ Elemente. □

**Aufgabe 182** Wir sollen jeweils untersuchen, ob es sich bei den folgenden Faktorringen um Körper handelt.
(a) Wir behaupten, dass $\mathbb{Z}[x]/(5, x^2 + 2)$ ein Körper ist. Dazu zeigen wir zuerst, dass $\mathbb{Z}[x]/(5, x^2 + 2) \simeq \mathbb{F}_5[x]/(x^2 + 2)$. Definiere $\phi : \mathbb{Z}[x] \to \mathbb{F}_5[x]/(x^2 + 2), f \mapsto \bar{f} \bmod(x^2 + 2)$, wo $\bar{f}$ die Reduktion von $f$ modulo 5 anzeigt. Es ist klar, dass $\phi$ als Komposition des Reduktionsepimorphismus $\mathrm{mod}(5) : \mathbb{Z}[x] \to \mathbb{F}_5[x]$ und des kanonischen Epimorphismus $\pi_{(x^2+2)} : \mathbb{F}_5[x] \to \mathbb{F}_5[x]/(x^2 + 2)$ ein Homomorphismus ist, der überdies surjektiv ist. Damit können wir den Homomorphiesatz für Ringe anwenden, der einen Isomorphismus $\bar{\phi} : \mathbb{Z}[x]/\ker \phi \to \mathbb{F}_5[x]/(x^2 + 2)$ liefert. Es verbleibt zu zeigen, dass $\ker \phi = (5, x^2 + 2)$. Dazu beachten wir folgende Äquivalenz: $f \in \ker \phi \Leftrightarrow \phi(f) = 0 \Leftrightarrow \bar{f} \in (x^2 + 2) \Leftrightarrow \exists \bar{h} \in \mathbb{F}_5[x] : \bar{f} = (x^2 + 2)\bar{h} \Leftrightarrow \exists h \in \mathbb{F}_5[x] : \bar{f} \equiv (x^2+2)\bar{h} \bmod(5) \Leftrightarrow \exists h, H \in \mathbb{Z}[x] : f = (x^2+2)h+5\cdot H \Leftrightarrow f \in (x^2+2, 5)$. Damit ist $\ker \phi = (5, x^2 + 2)$ nachgewiesen und wir haben die Isomorphie $\mathbb{F}_5[x]/(x^2 + 2) \simeq \mathbb{Z}[x]/(5, x^2 + 2)$ nachgewiesen. Da $x^2 + 2$ ein Polynom vom Grad 2 in $\mathbb{F}_5[x]$ ist, reicht es, nachzuweisen, dass $x^2 + 2$ keine Nullstellen in $\mathbb{F}_5$ hat, um zu schließen, dass $x^2 + 2$ irreduzibel ist. In der Tat ist mit $\bar{g} = x^2 + 2 \in \mathbb{F}_5[x]$, dass $\bar{g}(0) = 2 \neq 0$, $\bar{g}(1) = 3 \neq 0$, $\bar{g}(2) = 6 = 1 \neq 0$, $\bar{g}(3) = 11 = 1 \neq 0$, $\bar{g}(4) = 17 = 2 \neq 0$. Damit hat $\bar{g}$ keine Nullstelle in $\mathbb{F}_5$, ist also als Polynom vom Grad 2 über dem Körper $\mathbb{F}_5$ irreduzibel. Da $\mathbb{F}_5[x]$ als Polynomring über dem Körper $\mathbb{F}_5$ ein Hauptidealring ist, ist das vom irreduziblen Element $x^2 + 2 \in \mathbb{F}_5[x]$ erzeugte Ideal $(x^2 + 5)$ maximal. Damit ist $\mathbb{F}_5[x]/(x^2+2)$ laut Vorlesung ein Körper, also auch der zum erstgenannten Faktorring vermöge $\bar{\phi}$ isomorphe $\mathbb{Z}[x]/(5, x^2 + 2)$.
(b) Wir zeigen, dass $\mathbb{Z}[x]/(5, x^2 + 1)$ kein Körper ist. Dazu zeigen wir zuerst, dass $\mathbb{Z}[x]/(5, x^2+1) \simeq \mathbb{F}_5[x]/(x^2+1)$. Wir definieren hierzu $\phi : \mathbb{Z}[x] \to \mathbb{F}_5[x]/(x^2+1), f \mapsto \bar{f} \bmod(x^2 + 1)$, wo $\bar{f}$ die Reduktion von $f$ modulo 5 anzeigt. Da $\phi$ die Komposition des Reduktionsepimorphismus $\mathrm{mod}(5) : \mathbb{Z}[x] \to \mathbb{F}_5[x], f \mapsto \bar{f}$ und des kanonischen Epimorphismus $\pi_{(x^2+1)} : \mathbb{F}_5[x] \to \mathbb{F}_5[x]/(x^2+1), \bar{f} \mapsto \bar{f} \mathrm{mod}(x^2+1)$ ist, ist $\phi$ ein Ringhomomorphismus und surjektiv, also auch ein Epimorphismus. Der Homomorphiesatz liefert nun, dass $\mathbb{Z}[x]/\ker \phi \simeq \mathbb{F}_5[x]/(x^2+1)$. Wir zeigen, dass $\ker \phi = (5, x^2+1)$. Dazu beachten wir: $f \in \ker \phi \Leftrightarrow \phi(f) = 0 \Leftrightarrow \bar{f} \in (x^2 + 2) \Leftrightarrow \exists \bar{h} \in \mathbb{F}_5[x] : f = (x^2 + 2)\bar{h} \Leftrightarrow \exists h, H \in \mathbb{Z}[x] : f = h(x^2 + 2) + H \cdot 5 \Leftrightarrow f \in (5, x^2 + 2)$. Damit ist die postulierte Gleichung nachgewiesen. Nun ist $\mathbb{Z}[x]/(5, x^2 + 1)$ ein Körper, wenn $\mathbb{F}_5[x]/(x^2+1)$ ein Körper ist. Das ist dann der Fall, wenn $(x^2+1)$ ein maximales Ideal in $\mathbb{F}_5[x]$ ist. Da $\mathbb{F}_5[x]$ ein Polynomring über einem Körper ist, ist $(x^2 + 1)$ maximal, wenn $x^2 + 1$ irreduzibel über $\mathbb{F}_5$ ist. Da $x^2 + 1$ die Nullstelle $x = 2$ hat, ist $x^2 + 1$ als Polynom vom Grad 2 über $\mathbb{F}_5$ reduzibel. Damit ist $(x^2 + 1) \subseteq (x - 2)$, insbesondere also nicht maximal. Damit ist $\mathbb{Z}[x]/(5, x^2 + 1)$ wie ausgeführt kein Körper.

(c) Wir zeigen, dass $\mathbb{Z}[x]/(5, x^2+4, x^3+7x^2+2x+1)$ ein Körper ist. Wir zeigen hierzu zunächst, dass $\mathbb{Z}[x]/(5, x^2+4, x^3+7x^2+2x+1) \simeq \mathbb{F}_5[x]/(x^2+4, x^3+2x+2x+1)$. Wir definieren $\phi : \mathbb{Z}[x] \to \mathbb{F}_5[x]/(x^2+4, x^3+2x^2+2x+1), f \mapsto \bar{f} \bmod(x^2+4, x^3+2x^2+2x+1)$, wo $\bar{f}$ die Reduktion von $f$ modulo 5 ist. Als Komposition des Reduktionsepimorphismus $\mathrm{mod}(5) : \mathbb{Z}[x] \to \mathbb{F}_5[x]$ und des kanonischen Epimorphismus $\pi_{(x^2+2, x^3+2x+2x+1)} : \mathbb{F}_5[x] \to \mathbb{F}_5[x]/(x^2+4, x^3+2x^2+2x+1)$ ist $\phi$ ein surjektiver Ringhomomorphismus. Der Homomorphiesatz für Ringe liefert $\mathbb{Z}[x]/\ker\phi \simeq \mathbb{F}_5[x]/(x^2+4, x^3+2x^2+2x+1)$. Wir zeigen noch, dass $\ker\phi = (x^2+4, x^3+2x^2+2x+1)$. Wir beachten hier zu die Äquivalenz, dass $f \in \ker(\phi) \Leftrightarrow \phi(f) = 0 \bmod(x^2+4, x^3+2x^2+2x+1) \Leftrightarrow \bar{f} \in (x^2+4, x^3+2x^2+2x+1) \leftrightarrow \exists \bar{h}_1, \bar{h}_2 \in \mathbb{F}_5[x] : \bar{f} = \bar{h}_1(x^2+4) + \bar{h}_2(x^3+2x^2+2x+1) \Leftrightarrow \exists h_1, h_2 \in \mathbb{Z}[x] : (f - h_1(x^2+4) - h_2(x^3+2x^2+2x+1)) \equiv 0 \bmod(5) \leftrightarrow \exists h_1, h_2, H \in \mathbb{Z}[x] : f = 5 \cdot H + (x^2+4) \cdot h_1 + (x^3+7x^2+2x+1) \cdot h_2 \Leftrightarrow f \in (5, x^2+4, x^3+7x^2+2x+1)$. Damit ist insgesamt $\mathbb{Z}[x]/(5, x^2+4, x^3+7x^2+2x+1) \simeq \mathbb{F}_5[x]/(x^2+4, x^3+7x^2+2x+1)$. Da $\mathbb{F}_5$ ein Körper ist, ist $\mathbb{F}_5[x]$ ein Hauptidealring. Es ist $x^2+4 = (x+1)(x+4)$ in $\mathbb{F}_5[x]$. Da $4^3+2\cdot4^2+2\cdot4+1 = 64+32+8+1 = 0$ und $1^3+2\cdot1^3+2\cdot1+1 = 1$ ist 4, nicht aber 1 eine Nullstelle von $x^3+2x^2+2x+1$ in $\mathbb{F}_5$. Damit ist $\mathrm{ggT}(x^3+2x^2+2x+1, x^2+4) = x+1$ und somit $(x^2+4, x^3+2x^2+2x+1) = (x+1)$. Da $x+1$ als Polynom vom Grad 1 irreduzibel ist, ist $(x+1)$ maximal im Hauptidealring $\mathbb{F}_5[x]$. Damit ist laut Vorlesung $\mathbb{F}_5[x]/(x+1) = \mathbb{F}_5[x]/(x^2+4, x^3+2x^2+2x+1)$ ein Körper, also auch $\mathbb{Z}[x]/(5, x^3+7x^2+2x+1, x^2+4)$ wegen der etablierten Isomorphie. □

**Aufgabe 183 (H14T3A2)** Gesucht ist die Anzahl der Quadrate im Ring $R = \mathbb{Z}/2014\mathbb{Z}$. Es gilt $2014 = 2 \cdot 1007 = 2 \cdot 19 \cdot 53$ in Primfaktorzerlegung. Da $2, 19, 53$ paarweise verschiedene Primzahlen sind, liefert der Chinesische Restsatz den Isomorphismus

$$\begin{aligned} \Phi : \mathbb{Z}/2014\mathbb{Z} &\to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/19\mathbb{Z} \times \mathbb{Z}/53\mathbb{Z} \\ \bar{a} &\mapsto (\bar{a} \bmod(2), \bar{a} \bmod(19), \bar{a} \bmod(53)) =: (\bar{b}, \bar{c}, \bar{d}). \end{aligned} \tag{232}$$

Sei nun $\bar{a}$ ein Quadrat in $R$. Dann gibt es ein $\bar{a}_1 \in R$ mit $\bar{a} = \bar{a}_1^2$. Damit finden wir $(\bar{b}, \bar{c}, \bar{d}) = \Phi(\bar{a}) = \Phi(\bar{a}_1^2) = \Phi(\bar{a}_1)^2 = (\bar{b}_1, \bar{c}_1, \bar{d}_1)^2 = (\bar{b}_1^2, \bar{c}_1^2, \bar{d}_1^2)$, wo $\Phi(\bar{a}_1) = (\bar{b}_1, \bar{c}_1, \bar{c}_1)$. Damit ist das Bild jedes Quadrats in $R$ wiederum ein Quadrat in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/19\mathbb{Z} \times \mathbb{Z}/53\mathbb{Z} =: R'$. Wir zeigen, dass auch die Umkehrung gilt. Sei dazu $R' \ni (\bar{b}, \bar{c}, \bar{d})$ Quadrat. Dann gibt es ein $(\bar{b}_1, \bar{c}_1, \bar{d}_1) \in R'$, sodass $(\bar{b}_1, \bar{c}_1, \bar{d}_1)^2 = (\bar{b}, \bar{c}, \bar{d})$. Es ist $\Phi$ bijektiv, sodass wir $\bar{a} = \Phi^{-1}((\bar{b}, \bar{c}, \bar{d}))$, $\bar{a}_1 = \Phi^{-1}((\bar{b}_1, \bar{c}_1, \bar{d}_1))$ setzen können. Es gilt dann $\bar{a} = \Phi^{-1}((\bar{b}, \bar{c}, \bar{d})) = \Phi^{-1}((\bar{b}_1^2, \bar{c}_1^2, \bar{d}_1^2)) = \Phi^{-1}((\bar{b}_1, \bar{c}_1, \bar{d}_1))^2 = \bar{a}_1^2$. Mit anderen Worten, jedes Quadrat in $R'$ wird vermöge $\Phi^{-1}$ auf ein Quadrat in $R$ abgebildet. Damit haben wir gezeigt, dass $\Phi(Q_R) = Q_{R'}$, wo $Q_X$ für einen Ring $X$ die Menge der Quadrate in $X$ bezeichnet. Es reicht also aus, die Anzahl der Quadrate in $R'$ zu bestimmen, wozu wir die Anzahlen der Quadrate in den einzelnen Faktoren des Produkts von Ringen bestimmen.

- *Fall 1.* $\mathbb{Z}/2\mathbb{Z}$. In $\mathbb{Z}/2\mathbb{Z}$ gibt es zwei Quadrate, denn $0 = 0^2$ und $1 = 1^2$. Somit ist $|Q_{\mathbb{Z}/2\mathbb{Z}}| = 2$.
- *Fall 2.* $\mathbb{Z}/p\mathbb{Z}$, *p ungerade Primzahl.* Dann ist $\mathbb{Z}/p\mathbb{Z}$ bereits ein Körper und es gilt, dass $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{Z}/(p-1)\mathbb{Z}$. Sei $Q_p^\times = Q_p \setminus \{0\}$ die Menge der Quadrate in

$\mathbb{Z}/p\mathbb{Z}$ ausgenommen die 0. Da die Einheitengruppe $(\mathbb{Z}/p\mathbb{Z})^\times$ zyklisch und von der Ordnung $p-1 \in 2\mathbb{N}$ ist, gibt es ein $\alpha \in (\mathbb{Z}/p\mathbb{Z})^\times$, sodass $(\mathbb{Z}/p\mathbb{Z})^\times = \langle\alpha\rangle$. Da $2|\mathrm{ord}(\alpha)$ ist $\langle\alpha^2\rangle$ eine Untergruppe der Ordnung $(p-1)/2$ von $(\mathbb{Z}/p\mathbb{Z})^\times$. Diese enthält gerade alle $\beta \in Q_p^\times$, denn $\beta$ ist eine Einheit und Quadrat, d.h., es gibt ein $0 \leq k < (p-1)/2$, sodass $\beta = (\alpha^k)^2 = (\alpha^2)^k \in \langle\alpha^2\rangle$. Umgekehrt ist klar, dass jedes $\gamma \in \langle\alpha^2\rangle$ in $Q_p^\times$ liegt. Da stets $0 = 0^2$ gilt und $0 \notin Q_p^\times$, ist $|Q_p| = |Q_p^\times| + |\{0\}| = (p-1)/2 + 1 = (p+1)/2$. Somit ist die Anzahl von Quadraten im primen Restklassenring $\mathbb{Z}/p\mathbb{Z}$ für ungerade Primzahlen $p$ genau $(p+1)/2$. Indem wir die soeben bewiesene Aussage auf $\mathbb{Z}/19\mathbb{Z}$ bzw. $\mathbb{Z}/53\mathbb{Z}$ anwenden, erhalten wir $|Q_{19}| = 10$ und $|Q_{53}| = 27$.

Damit finden wir wegen Bijektivität von $\Phi$, dass $|Q_R| = |Q_{R'}| = |Q_2||Q_{19}||Q_{53}| = 2 \cdot 10 \cdot 27 = 540$. Es gibt also 540 Quadrate in $R = \mathbb{Z}/2014\mathbb{Z}$. □

**Aufgabe 184** Wir bestimmen die Anzahl der Quadrate im Ring $R = \mathbb{Z}/2020\mathbb{Z}$. Es gilt $2020 = 20 \cdot 101 = 4 \cdot 5 \cdot 101$ in Primfaktorzerlegung. Laut Chinesischem Restsatz gibt es dann einen Isomorphismus

$$\begin{aligned} \Phi : \mathbb{Z}/2020\mathbb{Z} &\to \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/101\mathbb{Z} \\ a &\mapsto (b,c,d) = (a \bmod(4), a \bmod(5), a \bmod(101)) \end{aligned} \tag{233}$$

Sei $R' = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/101\mathbb{Z}$ und bezeichne mit $Q_X$ die Menge der Quadrate in einem Ring $X$. Wir zeigen, dass $\Phi(Q_R) = Q_{R'}$. Sei dazu zunächst $a \in R$ ein Quadrat. Dann gibt es ein $a_1 \in R$, sodass $a = a_1^2$. Es gilt $(b,c,d) = \Phi(a) = \Phi(a_1^2) = \Phi(a_1)^2 = (b_1,c_1,d_1)^2 = (b_1^2, c_1^2, d_1^2)$, wo $(b,c,d) = \Phi(a)$ und $(b_1,c_1,d_1) = \Phi(a_1)$. Somit bildet $\Phi$ jedes Quadrat in $R$ auf ein Quadrat in $R'$ ab. Wir zeigen, dass zusätzlich jedes Quadrat in $R'$ vermöge $\Phi^{-1}$ auf ein Quadrat in $R$ abgebildet wird. Sei dazu $(b,c,d) \in R'$ Quadrat. Es gibt also ein $(b_1,c_1,d_1) \in R'$ mit $(b,c,d) = (b_1,c_1,d_1)^2$. Da mit $\Phi$ auch $\Phi^{-1}$ ein Ringisomorphismus ist, $a = \Phi^{-1}((b,c,d)) = \Phi^{-1}((b_1,c_1,d_1)^2) = \Phi^{-1}((b_1,c_1,d_1))^2 = a_1^2$, wo $a_1 = \Phi^{-1}(b_1,c_1,d_1)$. Damit wird auch jedes Quadrat aus $R'$ auf ein Element aus $Q_R$ abgebildet, vermöge $\Phi^{-1}$. Damit haben wir $\Phi(Q_R) = Q_{R'}$ nachgewiesen. Da $(b,c,d) \in R'$ genau dann ein Quadrat in $R'$ ist, wenn $b,c,d$ in jeweils $\mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/5\mathbb{Z}, \mathbb{Z}/101\mathbb{Z}$ Quadrate sind, reicht es, die Quadrate in den o.g. Ringen zu zählen.

- *Fall 1:* $\mathbb{Z}/4\mathbb{Z}$. Es gilt $0^2 = 0$, $1^2 = 1$, $2^2 = 4 = 0$, $3^2 = 9 = 1$ in $\mathbb{Z}/4\mathbb{Z}$. Damit gibt es in $\mathbb{Z}/4\mathbb{Z}$ genau 2 Quadrate.

- *Fall 2:* $\mathbb{Z}/5\mathbb{Z}$. Es ist $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 9 = 4$, $4^2 = 16 = 1$ in $\mathbb{Z}/5\mathbb{Z}$. Somit haben wir in $\mathbb{Z}/5\mathbb{Z}$ genau 3 Quadrate.

- *Fall 3:* $\mathbb{Z}/101\mathbb{Z}$. Da 101 eine Primzahl ist, ist $\mathbb{Z}/101\mathbb{Z}$ bereits ein Körper. Für diesen gilt $(\mathbb{Z}/101\mathbb{Z})^\times \simeq \mathbb{Z}/\Phi(101)\mathbb{Z} = \mathbb{Z}/100\mathbb{Z}$, wo $\Phi$ die eulersche $\Phi$-Funktion bezeichnet. Wir notieren ferner mit $Q^\times$ die Menge aller Quadrate in $\mathbb{Z}/101\mathbb{Z}$ ungleich 0, d.h., da $\mathbb{Z}/101\mathbb{Z}$ ein Körper ist, genau die Quadrate aus $(\mathbb{Z}/101\mathbb{Z})^\times \simeq \mathbb{Z}/100\mathbb{Z}$. Da die soeben genannte Einheitengruppe zyklisch und von Ordnung 100, also insbesondere gerader Ordnung, ist, gibt es ein $\alpha \in (\mathbb{Z}/101\mathbb{Z})^\times$ mit der Eigenschaft, dass $(\mathbb{Z}/101\mathbb{Z})^\times = \langle\alpha\rangle$. Wir betrachten die

(eindeutige) Untergruppe $\langle\alpha^2\rangle \leq \langle\alpha\rangle$. Offenbar ist jedes $\beta \in \langle\alpha\rangle$ ein Quadrat $\neq 0$. Andersherum ist jedes $\gamma \in Q^\times$ auch eine Einheit, sodass ein $0 \leq k < 51$ existiert, sodass $\gamma = (\alpha^k)^2 = (\alpha^2)^k \in \langle\alpha^2\rangle$. Also ist $\langle\alpha^2\rangle = Q^\times$ und da $\mathrm{ord}(\alpha^2) = 50$ finden wir, dass es in $\mathbb{Z}/101\mathbb{Z}$ 50 Quadrate ungleich 0 gibt. Da $0 = 0^2$, also 0 ebenfalls ein Quadrat ist, gilt $|Q| = |Q^\times| + |\{0\}| = 51$. Somit gibt es genau 51 Quadrate in $\mathbb{Z}/101\mathbb{Z}$.

Insgesamt haben wir somit $2 \cdot 3 \cdot 51 = 306$ Möglichkeiten, Quadrate in $R'$ zu finden. Da die Anzahl der Quadrate in $R'$ nach dem weiter oben bewiesenen mit der Anzahl der Quadrate in $R$ übereinstimmt, gibt es genau 306 Quadrate in $R = \mathbb{Z}/2020\mathbb{Z}$. □

**Aufgabe 185 (H12T3A4)** Gesucht ist die Anzahl der Lösungen von $x^2 + 46x + 1 = 0$ in $\mathbb{Z}/2012\mathbb{Z}$. Es gilt $2012 = 4 \cdot 503$. Der Chinesische Restsatz liefert wegen $\mathrm{ggT}(4, 503) = 1$ einen Ringisomorphismus

$$\Phi : \mathbb{Z}/2012\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/503\mathbb{Z}, a \mapsto (a \bmod(4), a \bmod(503)). \tag{234}$$

Bezeichne mit $L_x = \{\alpha \in \mathbb{Z}/x\mathbb{Z} | \alpha^2 + 46\alpha + 1 \equiv 0 \bmod(x)\}$. Wir zeigen, dass $\Phi(L_{2012}) = L_4 \times L_{503}$, sodass wegen der Bijektivität von $\Phi$ und der Endlichkeit der involvierten Mengen folgt $|L_{2012}| = |L_4||L_{503}|$. Es gilt mit $(\beta, \gamma) = \Phi(\alpha)$ $(\alpha \in \mathbb{Z}/2012\mathbb{Z})$

$$\begin{aligned}
\alpha \in L_{2012} &\Leftrightarrow \alpha^2 + 46\alpha + 1 \equiv 0 \bmod(2012) \\
&\Leftrightarrow \Phi(\alpha^2 + 46\alpha + 1) \equiv (0 \bmod(4), 0 \bmod(503)) \\
&\Leftrightarrow \Phi(\alpha)^2 + 46\Phi(\alpha) + \Phi(1) \equiv (0 \bmod(4), 0 \bmod(503)) \\
&\Leftrightarrow (\beta^2 + 46\beta + 1, \gamma^2 + 46\gamma + 1) \equiv (0 \bmod(4), 0 \bmod(503)) \\
&\Leftrightarrow (\beta, \gamma) \in L_4 \times L_{503} \\
&\Leftrightarrow \Phi(\alpha) \in L_4 \times L_{503}
\end{aligned}$$

Es gilt $\beta^2 + 2\beta + 1 \equiv 0 \bmod(4) \Rightarrow \beta \in \{1, 3\}$, wie man über Einsetzen alle $\beta \in \mathbb{Z}/4\mathbb{Z}$ verifiziert. In $\mathbb{Z}/503\mathbb{Z}$ gilt zunächst

$$\begin{aligned}
\gamma^2 + 46\gamma + 1 &\equiv 0 \bmod(503) \\
\Leftrightarrow \gamma^2 + 46\gamma &\equiv -1 \bmod(503) \\
\Leftrightarrow \gamma^2 + 46\gamma + 23^2 &\equiv (23^2 - 1) \bmod(503) \\
\Leftrightarrow (\gamma + 23)^2 &\equiv 528 \bmod(503) \\
\Leftrightarrow (\gamma + 23)^2 &\equiv 25 \bmod(503) \\
\Leftrightarrow ((\gamma + 23)^2 - 5^2) &\equiv 0 \bmod(503) \\
\Leftrightarrow (\gamma + 23 - 5)(\gamma + 23 + 5) &\equiv 0 \bmod(503) \\
\Leftrightarrow (\gamma + 18)(\gamma + 28) &\equiv 0 \bmod(503),
\end{aligned}$$

sodass $L_{503} = \{-18, -28\} \subsetneq \mathbb{Z}/503\mathbb{Z}$. Damit hat die angegebene quadratische Gleichung genau 2 Lösungen modulo 4 und genau zwei Lösungen modulo 503. Zusammen mit dem oben bewiesenen Resultat folgt, dass $x^2 + 46x + 1 \equiv 0 \bmod(2012)$ genau $2 \cdot 2 = 4$ Lösungen hat. □

**Aufgabe 186 (H15T1A1)** Gesucht sind alle Lösungen von $x^6 - 2x + 4 = 0$ in $\mathbb{Z}/64\mathbb{Z}$. Zunächst gilt $64 = 2^6$. Sei $\alpha \in \mathbb{Z}$ Repräsentant der Lösung von $x^6 - 2x + 4 = 0$. Dann gilt auch, wegen $2|64$, dass $\alpha \bmod(2)$ eine Lösung von $x^6 - 2x + 4 \equiv x^6 \bmod(2) \equiv 0 \bmod(2)$ ist. Damit ist $\alpha = 2 \cdot \gamma$. Ferner ist $\alpha^6 - 2\alpha + 4 \equiv 64\gamma - 4\gamma + 4 \equiv 0 \bmod(64)$, sodass $-\gamma + 1 \equiv 0 \bmod(16)$. Umformen liefert $\gamma \equiv 1 \bmod(16)$. Also ist $\gamma \bmod(64) \in \{17, 33, 49, 1\}$. Damit finden wir $\alpha \equiv 2\gamma \bmod(64) \in \{2, 34\}$. Damit ist jede Lösung der Gleichung in $\{2, 34\} \subseteq \mathbb{Z}/64\mathbb{Z}$ enthalten. Umgekehrt ist $2^6 - 2 \cdot 2 + 4 \equiv 64 \bmod(64) \equiv 0 \bmod(64)$ sowie $34^6 - 2 \cdot 34 + 4 \equiv 2^6 \cdot 17^6 - 64 \bmod(64) \equiv 0 \bmod(64)$, sodass $2, 34 \in \mathbb{Z}/64\mathbb{Z}$ auch Lösungen der Gleichung sind. Damit haben wir insgesamt alle gesuchten Lösungen gefunden und die Lösungsmenge der Gleichung ist gerade $\{2, 34\} \subseteq \mathbb{Z}/64\mathbb{Z}$. □

**Aufgabe 187** Wir suchen die Anzahl der Lösungen von $x^2 + 3x + 10 \equiv 0 \bmod(2020)$. Zunächst gilt $2020 = 4 \cdot 5 \cdot 101$. Da $4, 5, 101$ paarweise teilerfremd sind, liefert uns der Chinesische Restsatz für $\mathbb{Z}$ zunächst den Isomorphismus

$$\begin{aligned} &\Phi : \mathbb{Z}/2020\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/101\mathbb{Z} \\ &a \bmod(2020) \mapsto (a \bmod(4), a \bmod(5), a \bmod(503)) \end{aligned} \tag{235}$$

Sei $L_x$ für $x \in \mathbb{N}$ die Lösungsmenge der angegebenen quadratischen Gleichung in $\mathbb{Z}/x\mathbb{Z}$. Wir zeigen, dass $\Phi(L_{2020}) = L_4 \times L_5 \times L_{101}$, sodass wegen der Isomorphismuseigenschaft, genauer Bijektivität, von $\Phi$ gilt, $|L_{2020}| = |L_5||L_4||L_{101}|$. Notiere $(\beta, \gamma, \delta) = \Phi(\alpha)$ für $\alpha \in \mathbb{Z}/2020\mathbb{Z}$. Es gilt die Äquivalenz

$$\begin{aligned} \alpha \in L_{2020} &\Leftrightarrow \alpha^2 + 3\alpha + 10 \equiv 0 \bmod(2020) \\ &\Leftrightarrow \Phi(\alpha)^2 + 3\Phi(\alpha) + 10\Phi(1) \equiv (0 \bmod(4), 0 \bmod(5), 0 \bmod(503)) \\ &\Leftrightarrow (\beta, \gamma, \delta)^2 + 3(\beta, \gamma, \delta) + 10(1, 1, 1) \equiv (0, \bmod(4), 0 \bmod(5), 0 \bmod(101)) \\ &\Leftrightarrow \beta^2 + 3\beta + 10 \equiv 0 \bmod(4),\ \gamma^2 + 3\gamma + 10 \equiv 0 \bmod(5), \\ &\quad \delta^2 + 3\delta + 10 \equiv 0 \bmod(101) \\ &\Leftrightarrow (\beta, \gamma, \delta) \in L_4 \times L_5 \times L_{101} \\ &\Leftrightarrow \Phi(\alpha) \in L_4 \times L_5 \times L_{101} \end{aligned}$$

Es gilt zunächst für $\beta \in \mathbb{Z}/4\mathbb{Z}$, dass $\beta^2 + 3\beta + 10 \equiv \beta^2 + 3\beta + 2 \bmod(4) \equiv 0 \bmod(4)$. Wir sehen, dass diese Gleichung für $\beta \in \{2, 3\}$ gelöst wird, durch Einsetzen. Für $\gamma \in \mathbb{Z}/5\mathbb{Z}$ finden wir, dass $\gamma^2 + 3\gamma + 10 \equiv \gamma^2 + 3\gamma \equiv 0 \bmod(5)$, sodass $\gamma \in \{0, 2\}$ jeweils eine Lösung der Gleichung ist. Durch Einsetzen sehen wir, dass dies auch alle Lösungen sind. Für $\delta \in \mathbb{Z}/101\mathbb{Z}$ betrachten wir zunächst den Repräsentanten $d \in \mathbb{Z}$, der die Gleichung $d^2 + 3d + 10 \equiv 0 \bmod(101)$ löse. Dies ist äquivalent zu $d^2 - 98d + (49)^2 \equiv 49^2 - 10 \bmod(101)$, bzw., weiter $(d - 49)^2 \equiv 2391 \equiv 101 \equiv 68 \equiv 101$. Wir untersuchen mittels Legendre-Symbol, ob 68 ein quadratischer Rest

modulo 101 ist. Es ist unter Zuhilfenahme des Quadratischen Reziprozitätsgesetzes

$$\begin{aligned}\left(\frac{68}{101}\right) &= \left(\frac{2}{101}\right)^2 \left(\frac{17}{101}\right) \\ &\overset{101\nmid 2}{=} 1 \cdot (-1)^{(101-1)/2}(-1)^{(17-1)/2} \left(\frac{101}{17}\right) \\ &= \left(\frac{16}{17}\right) \\ &= \left(\frac{4}{17}\right)^2 \\ &= 1,\end{aligned} \tag{236}$$

denn $16 \equiv 4^2 \bmod(17)$. Sei also $\kappa \in \mathbb{Z}/101\mathbb{Z}$, sodass $\kappa^2 \equiv 68 \bmod(101)$. Dann ist $(d-49)^2 \equiv \kappa^2 \bmod(101)$ und wir finden die beiden Lösungen $d \equiv (49+\kappa) \bmod(101)$ und $d \equiv (49-\kappa) \bmod(101)$. Damit ist $\delta \in \{(49-\kappa) \bmod(101), (49+\kappa) \bmod(101)\}$. Es gibt auch keine weiteren Lösungen, denn $\mathbb{Z}/101\mathbb{Z}$ ist wegen der Primzahleigenschaft von 101 ein Körper und $x^2+3x+10 \in \mathbb{F}_{101}[x]$ hat dann höchstens zwei Nullstellen in $\mathbb{F}_{101}$ laut Fundamentalsatz der Algebra. Somit ist $|L_5| = |L_4| = |L_{101}| = 2$. Mithin $|L_{2020}| = |L_4||L_5||L_{101}| = 2 \cdot 2 \cdot 2 = 8$. Die betrachtete Gleichung hat also genau 8 Lösungen in $\mathbb{Z}/2020\mathbb{Z}$. □

**Aufgabe 188 (H19T1A1(a))** Gesucht sind alle rationalen Nullstellen des Polynoms $f(x) = x^3 - 2x + 1 \in \mathbb{Q}[x]$. Durch Inspektion sieht man, dass $x_1 = 1$ eine Nullstelle des Polynoms ist, denn $f(1) = 1^3 - 2 \cdot 1 + 1 = 0$. Polynomdivision liefert

$$x^3 - 2x + 1 = (x-1)(x^2 + x - 1). \tag{237}$$

Wir behaupten, dass $g(x) := x^2+x-1 \in \mathbb{Q}[x]$ keine rationalen Nullstellen hat. Denn es ist $g$ Polynom vom Grad 2 mit ganzzahligen Koeffizienten. Da $g$ darüber hinaus normiert ist, ist jede rationale Nullstelle von $g$ sogar ganzzahlig und ein Teiler von $-1$. Man sieht aber, dass $g(1) = 1 \neq 0$ und $g(-1) = -1 \neq 0$, sodass die einzigen Teiler von $-1$, nämlich 1 und $-1$ keine Nullstellen von $g$ sind. Folglich hat $g$ keine rationalen Nullstellen. Damit ist die Menge $N_Q$ der rationalen Nullstellen von $f$ gegeben durch $N_Q = \{1\}$. □

**Aufgabe 189 (H13T1A5(a))** Sei $f(x) = x^3 + x - 1 \in \mathbb{Q}[x]$. Wir zeigen, dass $f$ irreduzibel ist. Es ist $f$ keine Einheit und, da $\deg(f) = 3$, reicht es zu zeigen, dass $f$ keine Nullstellen in $\mathbb{Q}$ hat. Da $f$ normiert ist, ist jede rationale Nullstelle von $f$ sogar ganzzahlig und ein Teiler des konstanten Gliedes. Eine Nullstelle $x_0$ von $f$ ist also $x_0 \in \{-1, 1\}$. Allerdings gilt $f(x_0 = 1) = 1 \neq 0$ und $f(x_0 = -1) = -1 \neq 0$, sodass keiner beiden Nullstellenkandidaten tatsächlich eine Nullstelle ist. Infolge der anfänglichen Bemerkungen impliziert die Nullstellenfreiheit von $f$ dessen Irreduzibilität über $\mathbb{Q}$. □

**Aufgabe 190 (F18T2A2(a))** Sei $a \in \mathbb{Z}$ und $f(x) = x^3 + ax^2 - (3+a)x + 1 \in \mathbb{Q}[x]$. Da $f$ ein Polynom vom Grad 3, insbesondere also eine Nicht-Einheit, ist,

langt es, zu zeigen, dass $f$ keine rationalen Nullstellen hat. Da $f$ wegen $a \in \mathbb{Z}$ sogar ganzzahlige Koeffizienten hat und überdies normiert ist, ist laut Vorlesung jede rationale Nullstelle von $f$ bereits eine ganze Zahl, die 1 teilt. Die einzigen Teiler von 1 in $\mathbb{Z}$ sind $\{-1, 1\}$. Es gilt $f(1) = 1 + a - (3 + a) + 1 = -1 \neq 0$ und $f(-1) = -1 + a + (3 + a) - 1 = 1 + 2a \neq 0$, denn $1 + 2a = 0$ erfordert $a = -0.5$, was der Ganzzahligkeit von $a$ laut Voraussetzung widerspricht. Somit hat $f$ keine rationale Nullstelle, ist also als Polynom von Grad 3 in $\mathbb{Q}[x]$ irreduzibel. □

**Aufgabe 191 (F13T3A4(a))** Wir suchen alle normierten, irreduziblen Polynome vom Grad $\leq 2$ in $\mathbb{F}_3[x]$. Sei $f$ ein solches. Da $f$ eine Nicht-Einheit ist und zudem normiert sein soll, ist nur $\deg(f) = 1$ oder $\deg(f) = 2$ möglich. Da $\mathbb{F}_3$ ein Körper ist, sind alle Polynome der Form $x+a$ ($a \in \mathbb{F}_3$), d.h., alle normierten Polynome vom Grad 1 irreduzibel über $\mathbb{F}_3$. Wir finden also

$$f_0 = x,\ f_1 = x + 1,\ f_2 = x + 2 \tag{238}$$

als normierte irreduzible Polynome vom Grad 1 in $\mathbb{F}_3[x]$. Ein normiertes und irreduzibles Polynom vom Grad 2 ist automatisch von der Form $f(x) = x^2 + ax + b$ mit $a, b \in \mathbb{F}_3$. Es ist $b \neq 0$ für ein irreduzibles Polynom, denn andernfalls wäre $f(0) = 0$, also $f(x) = x(x + a)$ und somit nicht irreduzibel. Wir setzen $b = 1$, dann ist $f \in \{x^2 + 1, x^2 + x + 1.x^2 + 2x + 1\}$. Wegen $x^2 + 2x + 1 = (x + 1)^2$ kann $f$ nicht $x^2 + 2x + 1$ sein. Zudem sehen wir, dass $f(x) = x^2 + x + 1$ die Nullstelle $x = 1$ hat, denn $f(1) = 1 + 1 + 1 = 0$ in $\mathbb{F}_3$. Als Polynom vom Grad 3 wäre $f$ dann reduzibel. Zuletzt sehen wir, dass $f(x) = x^2 + 1$ keine Nullstelle in $\mathbb{F}_3$ hat, denn $f(0) = 1 \neq 0$, $f(1) = 2 \neq 0, f(2) = 2 \neq 0$ in $\mathbb{F}_3$. Als Polynom vom Grad 2 ist somit $x^2 + 1$ irreduzibel in $\mathbb{F}_3[x]$. Wir setzen nun $b = 2$. Dann ist nur $f \in \{x^2 + 2, x^2 + x + 2, x^2 + 2x + 2\}$ möglich. Dass $f(x) = x^2 + 2$ scheidet aus, denn $f(1) = 1+2 = 0$. Die Polynome $f_a(x) = x^2+x+2$ und $f_b(x) = x^2+2x+2$ hingegen haben keine Nullstellen in $\mathbb{F}_3$, denn $f_a(0) = 2 = f_b(2)$ und $f_a(1) = 1 \neq 0, f_a(2) = 2 \neq 0$ sowie $f_b(1) = 2 \neq 0$ und $f_b(2) = 1 \neq 0$. Als Polynome vom Grad 2 sind $x^2 + x + 2$ und $x^2 + 2x + 2$ somit irreduzibel über $\mathbb{F}_3$. Insgesamt haben wir also die folgenden irreduziblen Polynome in $\mathbb{F}_3[x]$:

$$x,\ x + 1,\ x + 2,\ x^2 + 1,\ x^2 + x + 2,\ x^2 + 2x + 2. \tag{239}$$

□

**Aufgabe 192 (H13T3A2)** Sei $f(x) = x^4 - x - 1 \in \mathbb{Q}[x]$ (a) Wir zeigen, dass $f$ genau 2 reelle Nullstellen hat. Es gilt $f(0) = -1 < 0$, $f(2) = 13 > 0$ und $f(-2) = 13 > 0$, sodass uns der Zwischenwertsatz liefert, dass in $(-2, 0)$ und $(0, 2)$ je mindestens eine Nullstelle von $f$, aufgefasst als Funktion von $\mathbb{R}$ nach $\mathbb{R}$ liegt. Somit hat $f$ mindestens zwei reelle Nullstellen. Es gilt $f'(x) = 4x^3 - 1$. $f'$ hat nur die reelle Nullstelle $\sqrt[3]{1/4} \in (0, 2)$. Da nach dem Satz von Rolle zwischen je zwei Nullstellen von $f$ eine Nullstelle von $f'$ liegt, können wir schließen, dass zwischen den beiden Nullstellen $x_1, x_2$ von oben keine weitere Nullstelle liegt und zudem gilt $-2 < x_1 < 0 < \sqrt[3]{1/4} < x_2 < 2$. Ebenso sehen wir, dass es keine Nullstelle $x_2 < -2$ geben kann, denn dann müsste $f'$ eine Nullstelle im Bereich $(x_3, x_2)$ haben, was aber

der vorherigen Feststellung widerspricht, dass $\sqrt[3]{1/4}$ die einzige reelle Nullstelle von $f'$ ist. Analog schließt man aus, dass es eine Nullstelle $x_4 > 2$ gibt. Insgesamt haben wir damit gezeigt, dass $f$ genau zwei reelle Nullstellen hat.
(b) Wir zeigen nun, dass $f$ irreduzibel über $\mathbb{Q}$ ist. Offenbar ist $f$ ein normiertes, damit primitives, Polynom und hat ferner ganzzahlige Koeffizienten. Laut Vorlesung ist dann bereits jede rationale Nullstelle von $f$ ganzzahlig und ein Teiler von $-1$. Andererseits stellen wir fest, dass $f(-1) = 1 \neq 0$ und $f(1) = -1 \neq 0$. Damit hat $f$ keine Nullstellen in $\mathbb{Q}$ und es kommt lediglich in Betracht, dass $f = gh$ mit zwei normierten Polynomen $g, h \in \mathbb{Q}[x]$. Wir reduzieren nun $f$ modulo 2, dann ist $\bar{f} = x^4 + x + 1$ und offenbar ebenfalls nullstellenfrei in $\mathbb{F}_2$. Das einzige irreduzible Polynom vom Grad 2 in $\mathbb{F}_2[x]$ ist $x^2 + x + 1$, und es gilt $(x^2 + x + 1)(x^2 + x + 1) = x^4 + x^2 + 1 \neq \bar{f}$. Damit ist $\bar{f}$ irreduzibel in $\mathbb{F}_2[x]$, laut Reduktionskriterium also $f$, aufgefasst als Polynom in $\mathbb{Z}[x]$. Da $f$ als normiertes Polynom insbesondere primitiv ist, ist nach dem Lemma von Gauss $f$ irreduzibel in $\mathbb{Q}[x]$.
(c) Sei $g(x) = x^3 + 4x - 1$ und $a \in \mathbb{C}$. Wir zeigen, dass $b, c, d \in \mathbb{C}$ mit $f(x) = (x^2 + ax + b)(x^2 + cx + d)$ genau dann existieren, wen $g(a^2) = a^6 + 4a^2 - 1 = 0$. Es ist $f(x) = (x^2+ax+b)(x^2+cx+d) = x^4+(a+c)x^3+(d+b+ac)x^2+(ad+bc)x+bd$, sodass Koeffizientenvergleich liefert $bd = -1$, $ad+bc = -1$, $0 = d+b+ac$ und $0 = a+c$, also $a = -c$. Einsetzen von letzterem in die zweite und dritte Gleichung liefert $b-d = 1/a$, wobei wir bemerkt haben, dass $a \neq 0$ gelten muss, da sonst $ad + bc = 0 \neq -1$. Zudem ist $b + d = a^2$. Nun gilt $-4 = 4bd = (b + d)^2 - (b - d)^2 = a^4 - 1/a^2$, sodass $-4a^2 = (a^3)^2 - 1$, also $0 = (a^3)^2 + 4a^2 - 1 = g(a^2)$. Umgekehrt liefert $g(a^2) = 0$ ein $a \neq 0$ und wir können $c = -a$, $b = 0.5((b + d) + (b - d)) = 0.5(a^2 + a^{-1})$ und $d = b - 1/a = 0.5(a^2 - a^{-1})$ setzen, was gerade die oben hergeleiteten Gleichungen für die Koeffizienten $b, c, d \in \mathbb{C}$ befriedigt. Diese sind dann nach ihrer Definition zu Beginn dergestalt, dass $f(x) = (x^2 + ax + b)(x^2 + cx + d)$.
(d) Wir zeigen, dass $g$ irreduzibel in $\mathbb{Q}[x]$ ist. Da $f$ normiert und vom Grad 3 ist, reicht es zu zeigen, dass $f$ keine Nullstelle $x_0 \in \mathbb{Z}$ hat, sodass $x_0| - 1$. In der Tat gilt, $f(1) = 4 \neq 0$ und $f(-1) = -6 \neq 0$. Somit ist $g$ irreduzibel in $\mathbb{Q}[x]$.
(e) Zu zeigen ist, dass für $a \in \mathbb{R}$ mit $g(a^2) = 0$ gilt $a \in \mathbb{Q}[x_1, x_2]$, wo $x_1, x_2$ die beiden (einzigen) reellen Nullstellen von $f$ nach (a) sind. Da $g(a^2) = 0$, gibt es $b, c, d \in \mathbb{C}$, sodass $f(x) = (x^2 + ax + b)(x^2 + cx + d)$. Insbesondere sind laut (b) auch $b, c, d \in \mathbb{R}$. Angenommen, $x^2+ax+b = (x-x_1)(x-x_2)$, dann ist $a = x_1+x_2$, also $a \in \mathbb{Q}[x_1, x_2]$. Angenommen, $x^2 + cx + d = (x - x_1)(x - x_2)$, dann ist $c = (x_1 + x_2) \in \mathbb{Q}[x_1, x_2]$, somit also $a = -c = -(x_1 + x_2) \in \mathbb{Q}[x_1, x_2]$. Der Fall, dass $x - x_i|(x^2 + ax + b)$ aber $x - x_k \not| x^2 + ax + b$ für verschiedene $i, k \in \{1, 2\}$ kann nun nicht auftreten. Denn dann wären einer der beiden (echt komplexen) Nullstellen $x_3, x_4$ ($\Im[x_3], \Im[x_4] \neq 0$) von $f$, ohne Einschränkung $x_3$ dergestalt, dass $(x - x_i)(x - x_3) = x^2 + ax + b$, was aber für $x \in \mathbb{R}$ der Tatsache widerspricht, dass $0 = \Im[x^2 + ax + b]$ und $\Im[(x - x_i)(x - x_3)] = -\Im[x_3]\Re[x - x_i]$, was zu einem Widerspruch führt, wenn wir $x = x_k$ bspw. setzen.
(f) Die Aussage lautet, dass weder $x_1$ noch $x_2$ mit Zirkel und Lineal konstruierbar sei. Es ist $x_1, x_2 \in \mathrm{Zerf}(f)$ und $f$ ist als normiertes, irreduzibles Polynom Minimalpolynom von $x_1$ und $x_2$ jeweils über $\mathbb{Q}$. Da $\mathbb{Q}[x_1, x_2] \subseteq \mathrm{Zerf}(f)$, gilt $a^2 \in \mathrm{Zerf}(f)$. Da $g$ normiert und irreduzibel ist, ist $g$ das Minimalpolynom von $a^2$ über $\mathbb{Q}$. Ferner ist $\mathbb{Q}(a^2)$ Zwischenkörper von $\mathrm{Zerf}(f)|\mathbb{Q}$ und es gilt $[\mathbb{Q}(a^2) : \mathbb{Q}] = \deg(g) = 3|[\mathrm{Zerf}(f) :$

$\mathbb{Q}]$ nach der Gradformel. Damit ist aber ausgeschlossen, dass $[\mathrm{Zerf}(f):\mathbb{Q}]$ eine Potenz von 2 ist. Das bedeutet, dass $x_1, x_2 \in \mathrm{Zerf}(f)$ beide nicht mit Zirkel und Lineal konstruierbar sind. □

**Aufgabe 193 (F19T1A1(b))** Wir bestimmen eine Zerlegung von $f(X) = 2X^4 + 2X^3 + 2X^2 + 2X$ in $\mathbb{Z}[X]$ in irreduzible Faktoren. Zunächst ist $2 \notin (\mathbb{Z}[X])^\times = \mathbb{Z}^\times = \{\pm 1\}$ und 2 ist als Primzahl irreduzibel in $\mathbb{Z}$ und auch in $\mathbb{Z}[X]$. Damit ist $f(X) = 2g(X)$ mit $g(X) = X^4+X^3+X^2+X$. Da $g(0) = 0$, ist $g(X) = X(X^3+X^2+X+1) =: Xh(X)$. Das Polynom $X \in \mathbb{Z}[X]$ ist als normiertes Polynom vom Grad 1 irreduzibel in $\mathbb{Z}[X]$. Wir stellen fest, dass $h(-1) = -1 + 1 - 1 + 1 = 0$, sodass $h$ als Polynom vom Grad 3 nicht irreduzibel ist, und wir den Linearfaktor $X + 1$ abspalten können. Dieser ist aber als normiertes Polynom vom Grad 1 irreduzibel in $\mathbb{Z}[X]$. Es gilt $X^3 + X^2 + X + 1 = (X^2 + 1)(X + 1)$. Sei $\bar{X}^2 + \bar{1} \in \mathbb{F}_3[X]$ das Bild von $X^2 + 1$, was wegen Normiertheit primitiv ist, unter der Reduktionsabbildung modulo 3. Durch Einsetzen sieht man, dass $\bar{X}^2 + \bar{1}$ irreduzibel in $\mathbb{F}_3[X]$ ist, weil es ein Polynom vom Grad 2 ist und keine Nullstellen in $\mathbb{F}_3$ hat. Das Reduktionskriterium liefert nun, dass $X^2 + 1$ irreduzibel in $\mathbb{Z}[X]$ ist. Sammeln wir die Ergebnisse, so haben wir die folgende Zerlegung von $f$ in irreduzible Faktoren in $\mathbb{Z}[X]$ gefunden,

$$f(X) = 2 \cdot X \cdot (X + 1) \cdot (X^2 + 1), \tag{240}$$

die wir jeweils durch explizites Ausschreiben von "$\cdot$" voneinander abgegrenzt haben. □

**Aufgabe 194** Wir bestimmen eine Zerlegung von $f(X, Y) = 5XY+10X-5Y-10$ in irreduzible Faktoren in $\mathbb{Z}[X, Y]$. Es ist $f(X, Y) = 5(Y + 2)(X - 1)$ und 5 ist als Primzahl irreduzibel in $\mathbb{Z}$ und somit auch in $\mathbb{Z}[X, Y]$. Da $Y + 2 \in \mathbb{Z}[Y]$ und $X - 1 \in \mathbb{Z}[X]$ irreduzibel sind, sind sie das aus Gradgründen erst recht in $\mathbb{Z}[X, Y]$. Somit haben wir eine Zerlegung von $f$ in irreduzible Faktoren gefunden. □

**Aufgabe 195 (H19T3A5(a))** Sei $a \in \mathbb{N}$ beliebig. Es gilt $f(X) = X^{2a} - X^{a+1} - X^{a-1} + 1 \in \mathbb{Q}[X]$ und durch geschicktes Ausklammern erhalten wir $X^{2a} - X^{a+1} - X^{a-1} + 1 = (X^{a+1} - 1)(X^{a-1} - 1)$. Somit ist $X^{a+1} - 1 | f$ und $f(X)/(X^{a+1} - 1) = (X^{a-1} - 1)$. □

**Aufgabe 196 (H19T1A1(b))** Sei $f(X) = X^5 + 18X^2 - 15 \in \mathbb{Q}[X]$. Da $f$ ganzzahlige Koeffizienten hat und zudem als normiertes Polynom primitiv ist, reicht es nach dem Lemma von Gauss, die Irreduzibilität in $\mathbb{Z}[X]$ nachzuweisen. Da für die Primzahl $p = 3$ gilt, $3|18, 3|15$ aber $3^2 \nmid 15$ und $3 \nmid 1$ (Leitkoeffizient 1), ist $f$ nach Eisenstein irreduzibel in $\mathbb{Z}[X]$. Das Lemma von Gauss liefert dann wie beschrieben die Irreduzibilität von $f$ in $\mathbb{Q}[X]$. □

**Aufgabe 197 (H18T1A1(a))** Sei $f(X) = X^7 + 3X + 3 \in \mathbb{Q}[X]$. Dieses Polynom ist normiert und hat ganzzahlige Koeffizienten, sodass es nach dem Lemma von Gauss reicht, die Irreduzibilität in $\mathbb{Z}[X]$ nachzuweisen. Da 3 ein Primelement in $\mathbb{Z}$ als Primzahl ist, und gilt $3 \nmid 1$, $3^2 \nmid 3$ aber $3|3$, liefert das Eisensteinkriterium, dass

$f$ in $\mathbb{Z}[X]$ irreduzibel ist. Da $f$ als normiertes Polynom insbesondere primitiv ist, liefert das Lemma von Gauss die gewünschte Irreduzibilität von $f$ in $\mathbb{Q}[X]$. □

**Aufgabe 198 (H12T3A5)** Sei $f(X) = X^5 - 7X^3 + 503X^2 + 12X - 2012 \in \mathbb{Q}[X]$. Es ist $2012 = 2^2 \cdot 503$ in Primfaktorzerlegung. Da $f$ ganzzahlig und normiert ist, ist jede rationale Nullstelle von $f$ ein Teiler von 2012. Wir stellen also fest, dass nur $x_0 \in \{\pm 1, \pm 2, \pm 4, \pm 503, \pm 1006, \pm 2012\}$ als Kandidaten für Nullstellen in Frage kommen. Es gilt $f(-2) = -32 + 7 \cdot 8 + 503 \cdot 4 - 12 \cdot 2 - 2012 = -32 - 24 + 56 = 0$, sodass wir eine Nullstelle von $f$ gefunden haben. Polynomdivision liefert

$$X^5 - 7X^3 + 503X^2 + 12X - 2012 = (X + 2)(X^4 - 2X^3 - 3X^2 + 509X - 1006). \tag{241}$$

Zudem gilt $f(2) = 2^5 - 7 \cdot 2^3 + 503 \cdot 2^4 + 12 \cdot 2 - 2012 = 0$, sodass auch 2 eine Nullstelle von $f$ ist. Da $2 + 2 = 4 \neq 0$, kann dies nur eine Nullstelle vom zweiten Faktor auf der rechten Seite sein. Offenbar ist

$$X^4 - 2X^3 - 3X^2 + 509X - 1006 = (X - 2)(X^3 - 3X + 503). \tag{242}$$

Nun ist aber leicht zu sehen, dass $X^3 - 3X + 503$ irreduzibel ist, denn $X^3 - 3X + 503 =: h(X)$ ist normiert, also primitiv, und, da normiert, hat ganzzahlige Nullstellen, die ein Teiler von der Primzahl 503 sind. Man sieht nun leicht, dass $h(1) = 501 \neq 0$, $h(-1) = 505 \neq 0$, $h(503) = (503^2 - 2) \cdot 503 > 0$ und $h(-503) = -(503^2 - 4) \cdot 503 > 0$. Damit hat $h$ keine Nullstellen in $\mathbb{Q}$ und ist als Polynom vom Grad 3 in $\mathbb{Q}[X]$ bereits irreduzibel. Die gesuchte Zerlegung von $f$ in irreduzible Faktoren lautet also

$$f(X) = (X - 2)(X + 2)(X^3 - 3X + 503), \tag{243}$$

und die Irreduzibilität der Faktoren $X \pm 2$ folgt daraus, dass diese Polynome vom Grad 1 in $\mathbb{Q}[X]$ sind. □

**Aufgabe 199 (H17T1A5)** Sei $K = \mathbb{C}(t)$ und $P(X) = X^3 - 2tX + t \in K[X]$. Wir zeigen, dass $P$ irreduzibel in $K[X]$ ist. Es ist $\mathbb{C}(t)$ der Quotientenkörper von $\mathbb{C}[t]$. Mit dem Lemma von Gauss folgt wegen Normiertheit, also Primitivität von $P$, dass $P$ irreduzibel über $K$ genau dann ist, wenn $P$ irreduzibel über $\mathbb{C}[t][X]$ ist. Wir zeigen, dass $t$ ein Primelement in $\mathbb{C}[t]$ ist. Es ist $\mathbb{C}[t] \to \mathbb{C}, p \mapsto p(0)$ ein surjektiver Homomorphismus von Ringen, nämlich der aus der Vorlesung bekannte Einsetzungshomomorphismus. Nun gilt, dass dessen Kern gerade $(t)$ ist. Mittels Homomorphiesatz für Ringe folgt $\mathbb{C}[t]/(t) \simeq \mathbb{C}$ und $\mathbb{C}$ ist als Körper ein Integritätsbereich, sodass $(t)$ ein Primideal in $\mathbb{C}[t]$, $t$ also ein Primelement in $\mathbb{C}[t]$ ist. Damit können wir das Eisensteinkriterium anwenden: Es ist $t \nmid 1$ aus Gradgründen, $t | -2t$ offensichtlicherweise und $t | t$ aber $t^2 \nmid t$ wiederum aus Gradgründen. Das besagte Kriterium von Eisenstein liefert uns nun die Irreduzibilität von $P(X) \in (\mathbb{C}[t])[X]$, und mit dem Lemma von Gauss folgt auch die Irreduzibilität von $P(X)$ über dem Quotientenkörper $\mathbb{C}(t) = K$. □

**Aufgabe 200 (H11T3A5)** (a) Sei $\mathbb{F}_2$ der Körper mit 2 Elementen und $f(X) = X^5 + X^2 + 1 \in \mathbb{F}_2[X]$. Zunächst gilt $f(0) = 1 \neq 0$ und $f(1) = 1 + 1 + 1 = 1 \neq 0$, sodass $f$ keine Nullstelle in $\mathbb{F}_2$ hat. Ist $f$ reduzibel, so kommt lediglich eine Zerlegung der Form $f = gh$ mit $g, h \in \mathbb{F}_2[X]$ mit Grad 2 und 3 respektive in Betracht. Beide Faktoren müssen irreduzibel sein, denn sonst hätte einer der Faktoren, und damit auch $f$ eine Nullstelle in $\mathbb{F}_2$, was wir vorher ausgeschlossen haben. Das einzige irreduzible Polynom vom Grad 2 in $\mathbb{F}_2[X]$ ist $X^2 + X + 1$, also ist dieses einer der Faktoren in der oben besprochenen Zerlegung. Polynomdivision liefert. Andererseits ist $X^5+X^2+1+(X^2+X+1) = (X+1)^2X+X+(X^2+X+1) = X^3 + X + X + (X^2 + X + 1) = X(X + 1) + (X^2 + X + 1) = 1 + (X^2 + X + 1)$ in $\mathbb{F}_2[X]/(X^2 + X + 1)$, sodass der Rest der Polynomdivision $1 \neq 0$ in $\mathbb{F}_2$ ist. Damit gibt es keinen irreduziblen Faktor von $f$ mit Grad 2, also keine Zerlegung von $f$ als Produkt eines irreduziblen Faktors vom Grad 2 und eines vom Grad 3. Zusammen mit der Nullstellenfreiheit von $f$ folgt die Irreduzibilität.
(b) Sei $R = \mathbb{Q}[X, Y]$ und $g(X, Y) = X^5 + X^2Y^3 + X^3 + Y^3 + X^2 + 1$. Wir zeigen, dass $g$ reduzibel ist, d.h., dass $g$ als Produkt zweier Nicht-Einheiten in $R$ geschrieben werden kann. Eine Rechnung zeigt:

$$\begin{aligned} g(X, Y) &= X^5 + X^2Y^3 + X^3 + Y^3 + X^2 + 1 && (244)\\ &= X^3(X^2 + 1) + Y^3(X^2 + 1) + (X^2 + 1) && (245)\\ &= (X^3 + Y^3 + 1)(X^2 + 1). && (246) \end{aligned}$$

Offenbar ist bereits $X^2 + 1$ und $X^3 + Y^3 + 1$ aus Gradgründen jeweils eine Nicht-Einheit, sodass $g$ nicht irreduzibel ist, und als Nicht-Einheit somit reduzibel ist. □

**Aufgabe 201 (F10T2A4)** (a) Sei $f(X) = X^4 + a_1X^3 + a_2X^2 + a_3X + a_4 \in \mathbb{Z}[X]$ mit $a_1, a_4$ beide ungerade und $a_2, a_3$ beide entweder gerade oder beide ungerade. Wir zeigen, dass $f$ irreduzibel in $\mathbb{Z}[X]$ ist. $f$ ist primitiv, da normiert. Betrachte dazu das Bild $\bar{f}$ von $f$ modulo 2.

- *Fall* 1*:* $a_2, a_3$ *ungerade.* Dann ist $\bar{f} = X^4 + X^3 + X^2 + X + 1 \in \mathbb{F}_2[X]$. Durch Einsetzen sehen wir, dass $\bar{f}$ keine Nullstellen in $\mathbb{F}_2$ hat, sodass lediglich eine Zerlegung von $\bar{f}$ als Produkt zweier irreduzibler Polynom vom Grad 2 den Nachweis der Irreduzibilität hindern könnte. Andererseits ist das einzige irreduzible Polynom vom Grad 2 in $\mathbb{F}_2[X]$ aus der Vorlesung zu $(X^2 + X + 1)$ bekannt. Es gilt nun $(X^2 + X + 1)^2 = X^4 + X^2 + 1 \in \mathbb{F}_2[X]$ und wir stellen fest, dass $(X^2 + X + 1)^2 = X^4 + X^2 + 1 \neq X^4 + X^3 + X^2 + X + 1 = \bar{f}$. Damit ist $\bar{f}$ über $\mathbb{F}_2$ irreduzibel. Nach Reduktionskriterium ist also $f$ irreduzibel in $\mathbb{Z}[X]$.

- *Fall* 2*:* $a_2, a_3$ *gerade.* Dann ist $\bar{f} = X^4 + X^3 + 1 \in \mathbb{F}_2[X]$. Durch Einsetzen sieht man, dass $\bar{f}$ auch in diesem Fall keine Nullstelle in $\mathbb{F}_2$ hat und somit aus Gradgründen nur einer Zerlegung von $\bar{f}$ in zwei irreduzible Faktoren vom Grad 2 beachtlich wäre. Analog zu Fall 1 findet man dann aber $(X^2 + X + 1)^2 = X^4 + X^2 + 1 \neq X^4 + X^3 + 1$, sodass $\bar{f}$ tatsächlich über $\mathbb{F}_2$ irreduzibel ist. Mithilfe des Reduktionskriteriums ergibt sich somit die Irreduzibilität von $f$ in $\mathbb{Z}[X]$.

In jedem Fall ist also $f$ über $\mathbb{Z}$ irreduzibel.
(b) Sei $K$ ein Körper. Wir untersuchen, ob $f(X,Y) = Y^3 + XY^2 + X^3 + X^2Y + X$ irreduzibel in $\mathbb{K}[X,Y]$ ist. Da $K$ Körper ist, ist $K[X]$ ein euklidischer Ring mit der Gradfunktion als Höhenfunktion, also ein Hauptidealbereich und somit ein faktorieller Ring. Es ist $K[X]/(X) \simeq K$ und $K$ ist als Körper ein Integritätsbereich, sodass $X$ ein Primelement in $K[X]$ ist. Umordnen der Summanden liefert $f(X,Y) = Y^3 + XY^2 + XY^2 + (X^3 + X) \in K[X][Y]$. Da $f$ normiert ist als Polynom in $Y$ mit Koeffizienten in $K[X]$, ist $f$ insbesondere primitiv. Wenden wir nun das Eisensteinkriterium auf $f$ mit dem Primelement $X \in K[X]$ an, erhalten wir wegen $X|X^3 + X$ aber $X^2 \not| X^3 + X$ und $X \not| 1$ sowie $X|X$, dass $f$ irreduzibel in $K[X][Y] = K[X,Y]$ ist. □

**Aufgabe 202 (F09T1A4)** Gesucht ist ein normiertes und irreduzibles Polynom $f$ vom Grad 2 aus $\mathbb{Z}[X]$, sodass $f(x + d)$ für alle $d \in \mathbb{Z}$ keine Primzahl $p$ das Eisensteinkriterium erfüllt. Wir setzen also an $f(X) = X^2+4$. $f$ ist offenbar normiert und erfüllt nicht das Eisensteinkriterium für $p = 2$, denn $2|4$ aber auch $2^2|4$. Für ungerade Primzahlen $p$ ist das Eisensteinkriterium wegen $p \not| 4$ nicht erfüllt. Sei nun $d \in \mathbb{Z}$ beliebig, dann ist $f(X + d) = X^2 + 2dX + (d^2 + 4)$. Für die Primzahl 2 gilt, dass $2|2d$ und $2|(d^2 + 4)$. Ist nun $d$ gerade, dann gilt $d = 2e$ für ein $e \in \mathbb{Z}$ und $d^2 + 4 = 4(e^2 + 1)$, also ist $d^2 + 4$ durch 4 teilbar, was das Eisestein-Kriterium unanwendbar macht. Ist $d$ hingegene ungerade, so ist $d^2 + 4$ ebenfalls ungerade, und ist gilt bereits $2 \not| d^2 + 4$. Sei nun $p$ eine ungerade Primzahl. Falls $p \not| d$, ist nichts mehr zu untersuchen. Falls $p|d$, dann gilt aber nicht, dass $p|d^2 + 4$, denn wegen $p|d$ ist $p|d^2$ und somit müsste $4 \equiv 0 \bmod(p)$, was für eine ungerade Primzahl $p$ nicht stimmt. Damit ist auch für ungerade Primzahlen $p$ das Eisensteinkriterium nicht anwendbar. Folglich ist $f$ normiert und das Eisensteinkriterium ist nicht anwendbar. Da $X^2 + 4$ nur zwei konjugiert komplexe Nullstellen, $\pm 2i$, hat, ist $X^2 + 4$ in $\mathbb{Z}[X]$ als Polynom vom Grad 2 überdies irreduzibel. Damit erfüllt unsere Wahl $X^2 + 4$ die Anforderungen der Aufgabenstellung. □

**Aufgabe 203 (F13T3A4(b))** Gegeben ist $f(X) = X^4 + 9X^2 - 2X + 2 \in \mathbb{Q}[X]$. Wir behaupten, dass $f$ irreduzibel ist. Zunächst ist $f$ als normiertes Polynom primitiv, sodass wir uns, infolge der Ganzzahligkeit der Koeffizienten von $f$, nach dem Lemma von Gauss auf den Nachweis der Irreduzibilität in $\mathbb{Z}[X]$ beschränken können. Wir wenden nun das Reduktionskriterium mit der Primzahl $p = 3$ an. Es gilt dann für das Bild $\bar{f}$ von $f$ unter der Reduktion modulo 3, dass $\bar{f} = X^4 + X + 2$. Einsetzen zeigt, dass $\bar{f}(0) = 2 \neq 0$, $\bar{f}(1) = 1 \neq 0$ und $\bar{f}(2) = 2 \neq 0$. Damit hat $\bar{f}$ keine Nullstelle in $\mathbb{F}_3$ und es kommt lediglich einer Zerlegung der Form $\bar{f} = \bar{g}\bar{h}$ in Betracht, wo $\bar{g}$, $\bar{h}$ (normierte) irreduzible Polynome in $\mathbb{F}_3[X]$ vom Grad 2 sind, die in Teil (a)

bestimmt wurden. Diese waren $X^2+1$, $X^2+X+2$ und $X^2+2X+2$. Es gilt aber

$$(X^2+1)(X^2+1) = X^4+2X^2+1 \neq \bar{f} \tag{247}$$
$$(X^2+X+2)(X^2+X+2) = X^4+2X^3+2X^2+X+1 \neq \bar{f} \tag{248}$$
$$(X^2+2X+2)(X^2+2X+2) = X^4+X^3+2X^2+2X+1 \neq \bar{f} \tag{249}$$
$$(X^2+1)(X^2+X+2) = X^4+X^3+X+2 \neq \bar{f} \tag{250}$$
$$(X^2+1)(X^2+2X+2) = X^4+2X^3+2X+2 \neq \bar{f} \tag{251}$$
$$(X^2+X+2)(X^2+2X+2) = X^4+1 \neq \bar{f}. \tag{252}$$

Da dies aller Möglichkeiten sind, die einzigen 3 irreduziblen normierten Polynome vom Grad 2 in $\mathbb{F}_3[X]$ als Produkt zu kombinieren, sehen wir, dass es nicht möglich ist $\bar{f}$ in zwei irreduzible Faktoren vom Grad 2 zu zerlegen. Somit ist $\bar{f}$ irreduzibel in $\mathbb{F}_3[X]$. Das Reduktionskriterium liefert nun die Irreduzibilität von $f$ in $\mathbb{Z}[X]$ und mit dem Lemma von Gauss erhalten wir auch die Irreduzibilität in $\mathbb{Q}[X]$. □

**Aufgabe 204 (H15T1A4)** Sei $P(X) = X^3 - X + 2 \in \mathbb{Z}[X]$.
(a) Wir zeigen, dass $\bar{P} \in \mathbb{F}_3[X]$ irreduzibel ist. Es ist $\bar{P} = X^3 + 2X + 2$ und $\bar{P}(0) = 2 \neq 0$, $\bar{P}(1) = 2 \neq 0$ sowie $\bar{P}(2) = 2 \neq 0$, sodass $\bar{P}$ keine Nullstellen in $\mathbb{F}_3$ hat. Als Polynom vom Grad 3 ist $\bar{P}$ damit bereits in $\mathbb{F}_3[X]$ irreduzibel.
(b) Da $P$ normiert ist, ist es insbesondere primitiv. Da $\bar{P}$ nach (a) irreduzibel in $\mathbb{F}_3[X]$ ist, liefert das Reduktionskriterium, dass $P$ in $\mathbb{Z}[X]$ irreduzibel ist. Da $\mathbb{Q}$ der Quotientenkörper zu $\mathbb{Z}$ ist, liefert das Lemma von Gauss die gewünschte Irreduzibilität von $P$ in $\mathbb{Q}[X]$.
(c) Wir zeigen, dass $P$ genau eine reelle Nullstelle hat. Zunächst ist $P(0) = 2 > 0$ und $P(-2) = -4 < 0$, sodass $P$, aufgefasst als Element von $C^0(\mathbb{R})$ nach dem Zwischenwertsatz mindestens eine Nullstelle in $(-2, 0)$ hat. Wir bilden die Ableitung, $P'(X) = 3X^2 - 1$. Diese hat die beiden Nullstellen $1/\sqrt{3}, -1/\sqrt{3}$. Da zwischen je zwei Nullstellen von $P$ eine Nullstelle der Ableitung liegen muss nach dem Satz von Rolle, sehen wir, dass es genau eine Nullstelle in $(-2, 0)$ gibt. Angenommen, es gäbe noch eine reelle Nullstelle von $P$. Diese müsste dann $\geq 1/\sqrt{3}$ sein. Es gilt aber $P(1/\sqrt{3}) = 2 - 2/(3\sqrt{3}) > 0$ und $P'(X > 1/\sqrt{3}) > 0$, sodass $P$ auf $(1/\sqrt{3}, \infty)$ streng monoton wachsend ist. Zusammen mit $P(1/\sqrt{3}) > 0$ erhalten wir somit einen Widerspruch zur Existenz einer weiteren reellen Nullstelle $\geq 1/\sqrt{3}$. Ebenso gibt es keine weitere reelle Nullstelle $< -2$, denn dann müsste nach dem Satz von Rolle $P'(X)$ eine weitere Nullstelle $< -1/\sqrt{3}$ haben, was nicht der Fall ist. Somit haben wir gezeigt, dass $P$ nur eine Nullstelle hat, die in $(-2, 0)$ liegt.
(d) Sei $L = \mathrm{Zerf}(P)$. Wir zeigen, dass $\mathrm{Gal}(P) \simeq S_3$. Bekanntlich ist die Galoisgruppe von $P$ vermöge eines Gruppenmonomorphismus isomorph zu einer Untergruppe von $S_{\deg(P)} = S_3$. Da $P$ normiert und irreduzibel ist, gilt $[L : \mathbb{Q}] \geq \deg(P) = 3$. Aus Teil (c) wissen wir, dass $P$ zwei Nullstellen in $\mathbb{C} \setminus \mathbb{R}$ hat, die, da die Koeffizienten von $P$ als ganze Zahlen insbesondere reell sind, zueinander konjugiert sind. Somit ist die komplexe Konjugation ein nicht-trivialer $\mathbb{Q}$-Automorphismus von $L$. Da die komplexe Konjugation Ordnung 2 als Element von $\mathrm{Gal}(P)$ hat, gilt $2 || \mathrm{Gal}(P)|$. Da nun $|\mathrm{Gal}(P)| = [L : \mathbb{Q}] \geq 3$, benötigen wir eine Untergruppe der Ordnung $\geq 3$ von $S_3$, deren Gruppenordnung von 2 geteilt wird. Da es in $S_3$ keine Untergruppe der Ordnung 4 gibt, und $2 \not| 3 = |A_3|$, bleibt nur $\mathrm{Gal}(P) \simeq S_3$ übrig. □

**Aufgabe 205 (F12T3A3)** Gesucht ist die Menge aller $(a,b) \in \mathbb{Q} \times \mathbb{Q}$, sodass $(X-1)^2 | f(X) := aX^{30} + bX^{15} + 1 \in \mathbb{Q}[X]$. Da $(X-1)^2 | f$, hat $f$ eine mindestens zweifache Nullstelle bei $X = 1$. Somit gilt $f(1) = 0$ und $f'(1) = 0$. Damit finden wir $a + b + 1 = 0$ und $30a + 15b = 0$, sodass $b = -2a$ und somit $-a = -1$, also $a = 1$ und $b = -2$. Insbesondere gibt es nur ein Paar $(a,b) \in \mathbb{Q} \times \mathbb{Q}$ mit der gewünschten Eigenschaft, die gesuchte Menge ist mithin $\{(1,-2)\}$. □

**Aufgabe 206 (H19T1A1(c))** Zu zeigen ist, dass $1 + \sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Es gilt $1/(\sqrt{2} + \sqrt{3}) = \sqrt{3} - \sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$, wie man anhand der dritten Binomischen Formel sieht. Somit ist $\sqrt{2} = 1/2((\sqrt{2} + \sqrt{3}) - (\sqrt{3} - \sqrt{2})) \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Damit ist auch $1 + \sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. □

**Aufgabe 207 (F12T1A5(a))** Sei $K = \text{Zerf}(f)$, der Zerfällungskörper des Polynoms $f = x^5 + 5 \in \mathbb{Q}[x]$ und $\alpha = \sqrt[5]{5}$ sowie $\zeta = \exp(2\pi i/5)$.
Wir zeigen $K = \mathbb{Q}(\sqrt[5]{5}, \zeta)$. Da $K$ als Zerfällungskörper von $f$ definiert ist, gilt $K = \mathbb{Q}(N)$, wo $N$ die Nullstellenmenge von $f$ ist. Es ist $\zeta$ eine primitive 5-te Einheitswurzel und es gilt, dass $x_k := -\alpha\zeta^k$ ist für alle $0 \leq k \leq 4$ eine Nullstelle von $f$, denn $(-\alpha\zeta^k)^5 = -\alpha^5(\zeta^5)^k = -5$, sodass $x_k^5 + 5 = 0$. Da $\zeta$ die zyklische Gruppe der 5-ten Einheitswurzeln von der Gruppenordnung 5 erzeugt und $\text{ggT}(k,5) = 1$ für $1 \leq k \leq 4$ gilt, ist $\zeta^k \neq 1$ und es gilt für $k \neq l$ mit $0 \leq k, l \leq 4$ $\zeta^k \neq \zeta^l$, da $\zeta \neq 1$. Als Polynom vom Grad 5 kann $f$ nur 5 komplexe Nullstellen haben, die wir mit $-\alpha\zeta^k$ $(0 \leq k \leq 4)$ auch gefunden haben. Somit ist $N = \{-\alpha, -\alpha\zeta, -\alpha\zeta^2, -\alpha\zeta^3, -\alpha\zeta^4\}$. Es ist offenbar $N \subseteq \mathbb{Q}(\alpha, \zeta)$, denn $-\alpha \in \mathbb{Q}(\zeta, \alpha)$ und $x_k = (-1) \cdot \alpha \cdot \zeta^k$ für $1 \leq k \leq 4$. Umgekehrt ist auch $\zeta \in \mathbb{Q}(N)$, denn $x_1/x_0 = (-\alpha\zeta)/(-\alpha) = \zeta$ und mit $-\alpha \in \mathbb{Q}(N)$ ist auch $\alpha \in \mathbb{Q}(N)$. Somit gilt auch $\{\alpha, \zeta\} \subseteq \mathbb{Q}(N)$. Laut Vorlesung ist somit bereits $\mathbb{Q}(N) = \mathbb{Q}(\alpha, \zeta)$ und der rechts stehende Körper mithin der Zerfällungskörper von $f$. □

**Aufgabe 208 (H17T2A4(a))** Sei $L = \text{Zerf}(f)$, wo $f = X^{12} - 729$ und $\zeta = (\sqrt{3} + i)/2$, die primitive 12-te Einheitswurzel.
Wir stellen fest, dass $|\zeta| = 1$, da $\zeta$ primitive 12-te Einheitswurzel, sodass $\zeta^{-1} = \bar{\zeta}$ und, wegen $|\langle\zeta\rangle| = 12$, somit $\bar{\zeta} = (\sqrt{3} - i)/2 = \zeta^{11}$. Also ist $\bar{\zeta} + \zeta = \zeta^{11} + \zeta = \sqrt{3}$ und damit $\sqrt{3} \in \mathbb{Q}(\zeta)$. Wir zeigen nun $L = \mathbb{Q}(\zeta)$. Offenbar ist $729 = 9 \cdot 9 \cdot 9 = \sqrt{3}^{12}$, sodass $X^{12} - 729$ Nullstellen der Form $\sqrt{3}\zeta^k$ mit $0 \leq k \leq 11$ hat. Dies sind in der Tat 12 verschiedene Nullstellen, da $\text{ord}(\zeta) = 12$, und $X^{12} - 729$ hat als Polynom vom Grad 12 genau 12 Nullstellen in $\mathbb{C}$. Somit ist die Menge $N$ der Nullstellen von $X^{12} - 729$ gegeben durch $N = \{\sqrt{3}\zeta^k | 0 \leq k \leq 11\}$. Nach Definition der Zerfällungskörpers ist ferner $L = \mathbb{Q}(N)$. Wir müssen nun zeigen, dass $N \subseteq \mathbb{Q}(\zeta)$ und $\zeta \in \mathbb{Q}(N)$. Da gilt $\sqrt{3} = \zeta^{11} + \zeta$, ist klar, dass $x_k = \sqrt{3}\zeta^k = \zeta^{k+1} + \zeta^{k+11} \in \mathbb{Q}(\zeta)$ für alle $0 \leq k \leq 11$. Umgekehrt folgt aus $0 \neq \sqrt{3}$, dass $\zeta = \sqrt{3}\zeta/\sqrt{3}$, also $\zeta \in \mathbb{Q}(N)$. Damit haben wir beiden Inklusionen nachgerechnet und ein Vorlesungsresultat liefert $\mathbb{Q}(N) = \mathbb{Q}(\zeta)$, wie behauptet. □

**Aufgabe 209 (F19T1A5(a))** Sei $\alpha = \sqrt[3]{2+\sqrt{2}}$. Gesucht ist das Minimalpolynom von $\alpha$ über $\mathbb{Q}$. Zunächst gilt:

$$\begin{aligned} \alpha &= \sqrt[3]{2+\sqrt{2}} \\ \Rightarrow \alpha^3 &= 2+\sqrt{2} \\ \Rightarrow (\alpha^3-2)^2 &= 2 \\ \Rightarrow \alpha^6 - 4\alpha^3 + 2 &= 0. \end{aligned}$$

Wir definieren nun $f = x^6 - 4x^3 + 2 \in \mathbb{Q}[x]$ und zeigen, dass $f$ das Minimalpolynom von $\alpha$ ist. Offenbar ist $\alpha$ eine Nullstelle von $f$, denn $f(\alpha) = (\alpha^3-2)^2 - 2 = \sqrt{2}^2 - 2 = 0$. Zudem ist $f$ normiert und hat ganzzahlige Koeffizienten, sodass es infolge des Eisensteinskriteriums mit $p = 2$ über $\mathbb{Z}$ und somit mittels des Lemmas von Gauss auch über $\mathbb{Q}$ irreduzibel ist. Laut Vorlesung ist damit bereits $f = \mu_{\mathbb{Q},\alpha}$.□

**Aufgabe 210 (H15T2A5(a))** Sei $\xi = \sqrt{2+\sqrt{2}}$. Wir suchen das Minimalpolynom von $\xi$ über $\mathbb{Q}$. Zunächst gilt in $\mathbb{C}$ die Implikation:

$$\begin{aligned} \xi &= \sqrt{2+\sqrt{2}} \\ \Rightarrow \xi^2 &= 2+\sqrt{2} \\ \Rightarrow (\xi^2-2)^2 &= \sqrt{2}^2 = 2 \\ \Rightarrow \xi^4 - 4\xi^2 + 2 &= 0. \end{aligned}$$

Wir definieren nun $f = x^4 - 4x^2 + 2 \in \mathbb{Q}[x]$, und beachten, dass $f$ normiert ist. Zudem erfüllt $\xi$, dass $f(\xi) = 0$. Da $f$ normiert ist und ganzzahlige Koeffizienten hat, liefert uns das Eisensteinsteinkriterium zur Primzahl $p = 2$, dass $f$ in $\mathbb{Z}[x]$ irreduzibel ist. Das Lemma von Gauss liefert dann die Irreduzibilität von $f$ über $\mathbb{Q}$. Da $f$ irreduzibel über $\mathbb{Q}$ ist, normiert und $f(\xi) = 0$ gilt, ist bereits $f = \mu_{\mathbb{Q},\xi}$ laut Vorlesung. □

**Aufgabe 211 (F17T1A2)** Wir setzen $L = \mathbb{Q}(\sqrt{2}, \sqrt{2+\sqrt{3}})$ und betrachten $L|\mathbb{Q}$. Ferner sei $x = \sqrt{2+\sqrt{3}} \in L$.
(a) Wir zeigen, dass $x - \sqrt{2-\sqrt{3}} = \sqrt{2}$. Zunächst haben wir die Implikation, dass

$$\begin{aligned} \left(x - \sqrt{2-\sqrt{3}}\right)^2 &= x^2 - 2\sqrt{2-\sqrt{3}}x + (2-\sqrt{3}) \\ &= 4 - 2\sqrt{2^2 - \sqrt{3}^2} \\ &= 4 - 2 \\ &= 2, \end{aligned}$$

sodass $x - \sqrt{2-\sqrt{3}} \in \{-\sqrt{2}, \sqrt{2}\}$. Da $x > \sqrt{2-\sqrt{3}}$ wegen der strengen Monotonie der Wurzelfunktion auf den positiven reellen Zahlen, ist somit $x - \sqrt{2-\sqrt{3}} = \sqrt{2}$.

(b) Wir bestimmen, das Minimalpolynom von $x$ über $\mathbb{Q}$. Es gilt

$$\begin{aligned} x &= \sqrt{2+\sqrt{3}} \\ \Rightarrow x^2 - 2 &= \sqrt{3} \\ \Rightarrow (x^2-2)^2 &= 3 \\ \Rightarrow x^4 - 4x + 1 &= 0. \end{aligned}$$

Offenbar ist also $x$ eine Nullstelle, des normierten Polynoms $f(X) = X^4 - 4X^2 + 1 \in \mathbb{Q}[X]$. Da ferner $f$ nur ganzzahlige Koeffizienten hat, ist jede rationale Nullstelle von $f$ ein Teiler von $1/1 = 1$ und insbesondere ganzzahlig. Allerdings ist $f(1) = -2 = f(-1)$, sodass $f$ zumindest keine rationale Nullstelle hat. Damit ist es nur möglich, dass $f$ ein Produkt zweier irreduzibler Polynome $g, h \in \mathbb{Q}[X]$ ist. Da $f$ normiert ist, sind auch $g$ und $h$ normiert (ohne Einschränkung). Da das konstante Glied von $f$ gleich 1 ist, ist $g(X) = X^2 + aX + 1$ und $h(X) = X^2 + bX + 1$ oder $g(X) = X^2 + cX - 1$ und $h(X) = X^2 + dX - 1$, wo $a, b, c, d \in \mathbb{Q}$. Im ersten Fall erhalten wir durch Ausmultiplizieren und anschließenden Koeffizientenvergleich, dass $a + b = 0$, $ab + 2 = -4$, was aber wegen $\sqrt{6} \notin \mathbb{Q}$ nicht lösbar ist. Im zweiten Fall erhalten wir auf dieselbe Weise, dass $a - b = 0$ und $ab - 2 = -4$, was aber wegen $\sqrt{2} \notin \mathbb{Q}$ nicht lösbar ist. Damit kann es keine Zerlegung von $f$ in Polynome $g$ und $h$ als quadratische Faktoren, wie beschrieben, geben. Damit ist $f$ als Polynom vom Grad 4 bereits irreduzibel über $\mathbb{Q}$. Da $f$ normiert und irreduzibel in $\mathbb{Q}[X]$ ist, und zudem $f(x) = 0$ nach der eingangs gemachten Rechnung gilt, ist $f$ bereits laut Vorlesung das Minimalpolynom von $x$ über $\mathbb{Q}$.
(c) Die Nullstellenmenge von $f$ in $\mathbb{C}$ ist gegeben durch $N = \{\pm\sqrt{2 \pm \sqrt{3}}\}$. Alle Nullstellen von $f$ sind insbesondere reell. Wir rechnen nun $(X + \sqrt{2-\sqrt{3}})(X - \sqrt{2+\sqrt{3}}) = X^2 - (\sqrt{2+\sqrt{3}} - \sqrt{2-\sqrt{3}})X - \sqrt{2^2 - \sqrt{3}^2} = X^2 - \sqrt{2}X - 1$, wobei wir Teil (a) verwendet haben, $\sqrt{2+\sqrt{3}} - \sqrt{2-\sqrt{3}} = \sqrt{2}$. Wir behaupten nun, dass $F = X^2 - \sqrt{2}X - 1 \in \mathbb{Q}(\sqrt{2})[X]$ das Minimalpolynom von $x$ über $\mathbb{Q}(\sqrt{2})$ ist. Offenbar ist $F$ normiert und es gilt $F(x) = 0$. Da $\sqrt{2}$ Nullstelle von dem nach Eisenstein irreduziblen und normierten $x^2 - 2$ ist, gilt $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Ferner ist $\sqrt{2+\sqrt{3}} = x \notin \mathbb{Q}(\sqrt{2})$, sodass $F$ keine Nullstelle in $\mathbb{Q}(\sqrt{2})$ hat. $F$ ist damit irreduzibel über $\mathbb{Q}(\sqrt{2})$ als Polynom vom Grad 2. Laut Vorlesung ist also $F$ dann das Minimalpolynom von $x$ über $\mathbb{Q}(\sqrt{2})$. Zum Nachweis, dass $\sqrt{2+\sqrt{3}} \notin \mathbb{Q}(\sqrt{2})$ beachtet man, dass falls das Gegenteil stimmt, es $a, b \in \mathbb{Q}$ gibt, sodass $\sqrt{2+\sqrt{3}} = a + b\sqrt{2}$, was aber bedeutet, dass $\deg(\mu_{\mathbb{Q},x}) = 2 < 4$ ist, im Widerspruch dazu, dass das Minimalpolynom von $x$ nach Teil (b) Grad 4 über $\mathbb{Q}$ hat.
(d) Wir zeigen zunächst, dass $L = \mathrm{Zerf}(f|\mathbb{Q})$. Offenbar hat $f$ die Nullstellenmenge $N$, siehe Teil (c). Nach Teil (a) gilt auch $\sqrt{2} \in \mathbb{Q}(N)$, sodass $L \subseteq \mathbb{Q}(N)$. Andererseits gilt $x - \sqrt{2} = -\sqrt{2-\sqrt{3}}$, sodass, weil $\pm 1 \in L$, in der Tat $N \subseteq L$. Somit ist $L = \mathrm{Zerf}(f|\mathbb{Q})$. Es gilt nun $[L : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4$, sodass $[L : \mathbb{Q}] = 4$ nach der Gradformel. Da $\mathbb{Q}$ ein vollkommener Körper ist, ist $L|\mathbb{Q}$ separabel. Infolge der oben nachgewiesenen Eigenschaft, dass $L$ der Zerfällungskörper von $f$ ist, ist $L|\mathbb{Q}$ auch normal. Insgesamt ist $L|\mathbb{Q}$ also galoissch. Nach dem Hauptsatz der Galois-Theorie ist $G := \mathrm{Gal}(L|\mathbb{Q})$ also von Ordnung 4. Da 4 ein Primzahlquadrat ist, ist $G$ abelsch

und nach dem Hauptsatz für endlich erzeugte abelsche Gruppen somit entweder vom Isomorphietyp $\mathbb{Z}/4\mathbb{Z}$ oder $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Im ersten Fall, hätte $G$ als zyklische Gruppe damit genau eine Untergruppe der Ordnung 2, nach dem Hauptsatz der Galois-Theorie hätte also $L|\mathbb{Q}$ genau einen Zwischenkörper vom Erweiterungsgrad $4 : 2 = 2$. Da aber $\mathbb{Q}(\sqrt{2}) \neq \mathbb{Q}(\sqrt{3})$ gilt, und $\sqrt{2} \in L$, sowie $\sqrt{3} = x^2 - 2 \in L$, hat $L$ zwei verschiedene Zwischenkörper $K_1 := \mathbb{Q}(\sqrt{2}), K_1 := \mathbb{Q}(\sqrt{3})$. Da $x^2 - 2$, $x^2 - 3$ jeweils normiert und nach Eisenstein zu $p = 2$ bzw. $p = 3$ irreduzibel sind, und $\sqrt{2}$ bzw. $\sqrt{3}$ als Nullstellen haben, gilt $[K_1 : \mathbb{Q}] = 2 = [K_2 : \mathbb{Q}]$. Damit hat $L|\mathbb{Q}$ mindestens zwei Zwischenkörper vom Erweiterungsgrad 2 über $\mathbb{Q}$. Das ist ein Widerspruch zur Annahme, $G$ wäre zyklisch. Damit ist $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. □

**Aufgabe 212 (F17T2A4)** Sei $f = x^3 + 2x + 2 \in \mathbb{Q}[x]$ und $\alpha \in \mathbb{C}$ eine Nullstelle von $f$.
(a) Zu zeigen ist, dass $\{1, \alpha, \alpha^2\}$ eine Basis von $\mathbb{Q}(\alpha)$ als $\mathbb{Q}$-Vektorraum ist. Wir zeigen hierzu, dass $f$ das Minimalpolynom von $\alpha$ über $\mathbb{Q}$ ist. Aus der Vorlesung ist dann bekannt, dass $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f) = 3$ und ferner die angegebene Menge eine Basis von $\mathbb{Q}(\alpha)$ als $\mathbb{Q}$-Vektorraum ist. Offenbar ist $f$ normiert und laut Voraussetzung ist auch $f(\alpha) = 0$. Für den Nachweis, dass $f$ das Minimalpolynom von $\alpha$ über $\mathbb{Q}$ ist, bleibt nur noch die Irreduzibilität von $f$ in $\mathbb{Q}[x]$ zu zeigen. Da $f$ normiert ist, ist $f$ primitiv. Da $f$ ferner Koeffizienten aus $\mathbb{Z}$ hat, liefert das Eisensteinkriterium zur Primzahl 2 die Irreduzibilität von $f$ über $\mathbb{Z}$. Das Lemma von Gauss liefert dann die Irreduzibilität von $f$ über $\mathbb{Q}$.
(b) Wir sollen das Element $(1 + \alpha)^{-1}$ in der in (a) spezifizierten Basis ausdrücken. Hierzu definieren wir das Polynom $g = 1 + x \in \mathbb{Q}[x]$. Da $f$ irreduzibel laut (a) ist, gilt $\mathrm{ggT}(f, g) = 1$. Nach dem Lemma von Bezout für Hauptidealringe gibt es also $h, j \in \mathbb{Q}[x]$ mit der Eigenschaft, dass $gh + fj = 1$ in $\mathbb{Q}[x]$. Setzen von $x = \alpha$ in dieser Gleichung liefert unter Beachtung von $f(\alpha) = 0$, dass $(1 + \alpha)h(\alpha) = 1$, sodass wir mit $h(\alpha)$ zumindest einen polynomialen Ausdruck für $(1 + \alpha)^{-1}$ finden. Polynomdivision liefert bereits, dass

$$(x^3 + 2x + 2) : (x + 1) = x^2 - x + 3 + (-1) : (x + 1), \tag{253}$$

sodass $(-1)(x^3 + 2x + 2) + (x^2 - x + 3)(x + 1) = 1$. Somit finden wir über das oben beschriebene Vorgehen, dass $(1+\alpha)(\alpha^2 - \alpha + 3) = 1$. Also ist $(1+\alpha)^{-1} = \alpha^2 - \alpha + 3$ die Darstellung des zu untersuchenden Elements von $\mathbb{Q}(\alpha)$ in der gewünschten Form. □

**Aufgabe 213 (F18T2A2)** Sei $a \in \mathbb{Z}$ und $f = x^3 + ax^2 - (3 + a)x + 1 \in \mathbb{Q}[x]$.
(a) Wir zeigen, dass $f$ irreduzibel über $\mathbb{Q}$ ist. Wegen $a \in \mathbb{Z}$, ist $f$ sogar ein normiertes Polynom mit ganzzahligen Koeffizienten. Bei Reduktion modulo 2 stellen wir fest, dass für gerades $a$ gilt $a \equiv 0 \bmod(2)$ aber $-(3 + a) \equiv 1 \bmod(2)$. Für ungerades $a$ gilt $a \equiv 1 \bmod(2)$ und $-(3 + a) \equiv 0 \bmod(2)$. Für das Bild $\bar{f}$ von $f$ unter den Reduktionshomomorphismus mod(2) gilt damit $\bar{f} \in \{x^3 + x + 1, x^3 + x^2 + 1\}$. In jedem der beiden Fälle überprüft man durch Einsetzen, dass $\bar{f}$ keine Nullstelle in $\mathbb{F}_2$ hat. Da $\bar{f}$ als normiertes Polynom mit ganzzahligen Koeffizienten sogar in $\mathbb{Z}[x]$ und primitiv ist, liefert das Reduktionskriterium die Irreduzibilität von $f$ in $\mathbb{Z}[x]$. Mittels des Lemmas von Gauss etablieren wir die Irreduzibilität von $f$ in $\mathbb{Q}[x]$.

(b) Sei nun $\alpha \in \mathbb{C}$ eine Nullstelle von $f$. Wir zeigen, dass auch $f((1-\alpha)^{-1}) = 0$. Da $f$ irreduzibel über $\mathbb{Q}$ ist und den Polynomgrad 3 hat, gilt $\alpha \in \mathbb{C} \setminus \mathbb{Q}$. Somit ist insbesondere $\alpha \neq 1$. Wir führen also die folgenden Äquivalenzumformungen durch:

$$\begin{aligned} f(1/(1-\alpha)) &= 0 \\ \Leftrightarrow \left(\frac{1}{1-\alpha}\right)^3 + a\left(\frac{1}{1-\alpha}\right)^2 - (3+a)\left(\frac{1}{1-\alpha}\right) + 1 &= 0 \\ \Leftrightarrow 1 + a(1-\alpha) - (3+a)(1-\alpha)^2 + (1-\alpha)^3 &= 0 \\ \Leftrightarrow (1+a+1-(3+a)) \cdot 1 + (-a\alpha + (3+a)\cdot 2 - 3)\alpha + (-(3+a)+3)\alpha^2 - \alpha^3 &= 0 \\ \Leftrightarrow -(1-(3+a)\alpha + a\alpha^2 + \alpha^3) &= 0 \\ \Leftrightarrow f(\alpha) &= 0. \end{aligned}$$

Somit ist auch $1/(1-\alpha)$ eine Nullstelle von $f$.
(c) Wir sollen nun zeigen, dass $\mathbb{Q}(\alpha)|\mathbb{Q}$ galoissch ist. Da $\alpha$ Nullstelle von $f$ ist, ist $\alpha$ algebraisch über $\mathbb{Q}$. Damit ist auch $\mathbb{Q}(\alpha)|\mathbb{Q}$ eine algebraische Erweiterung. Da $\mathbb{Q}$ ein vollkommener Körper ist und $\mathbb{Q}(\alpha)|\mathbb{Q}$ wegen $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f) = 3 < \infty$ endlich ist, ist $\mathbb{Q}(\alpha)|\mathbb{Q}$ auch separabel. Zu zeigen ist noch, dass $\mathbb{Q}(\alpha)|\mathbb{Q}$ normal ist. Wir behaupten, dass $\mathbb{Q}(\alpha)$ der Zerfällungskörper von $f$ ist. Zunächst ist $\alpha$ nach Voraussetzung eine Nullstelle von $f$, und mit $\alpha \in \mathbb{Q}(\alpha)$ ist auch $1/(1-\alpha) \in \mathbb{Q}(\alpha)$. Wir zeigen nun, dass $\alpha \neq 1/(1-\alpha)$, denn dann ist $(x-\alpha)(x-(1-\alpha)^{-1})|f$ und es gibt ein Polynom vom Grad 1 über $\mathbb{Q}(\alpha)$, bezeichnet mit $h$, sodass $f = h(x-\alpha)(x-(1-\alpha)^{-1})$. Angenommen, $\alpha = 1/(1-\alpha)$. Dann ist $-\alpha^2 + \alpha - 1 = 0$ und $\alpha$ wäre eine Nullstelle von $p = x^2 - x + 1 \in \mathbb{Q}[x]$. Da $\deg(p) = 2 < \deg(f)$ haben wir damit einen Widerspruch dazu, dass $f$ als Minimalpolynom von $\alpha$ über $\mathbb{Q}$ insbesondere Polynom minimalen Grades ist, das $\alpha$ als Nullstelle hat. Damit ist $\alpha \neq 1/(1-\alpha)$. Da $h \in \mathbb{Q}(\alpha)[x]$ wie eingangs beschrieben vom Grad 1 ist, hat es zumindest eine Nullstelle in $\mathbb{Q}(\alpha)$. Somit zerfällt $f$ über $\mathbb{Q}(\alpha)$ vollständig in Linearfaktoren und alle Nullstellen von $f$ liegen in $\mathbb{Q}(\alpha)$. Da $\alpha$ selbst bereits Nullstelle von $f$ ist, ist $\mathbb{Q}(\alpha)$ der Zerfällungskörper von $f$, also ist $\mathbb{Q}(\alpha)|\mathbb{Q}$ normal wegen $\deg(f) > 0$. Als normale und separable Körpererweiterung ist $\mathbb{Q}(\alpha)|\mathbb{Q}$ galoissch, wie zu zeigen war. □

**Aufgabe 214 (F16T2A4)** Sei $f = x^3 - x - 1 \in \mathbb{Q}[x]$ und $\mathbb{C} \ni a$ sei eine Nullstelle von $f$. Ferner, $b := 2a^2 - a - 2$.
(a) Wir zeigen, dass $f$ irreduzibel über $\mathbb{Q}$ ist. Zunächst stellen wir fest, dass $f$ ein normiertes Polynom ist und darüber hinaus ganzzahlige Koeffizienten besitzt. Daher ist jede rationale Nullstelle von $f$ ganzzahlig und insbesondere ein Teiler des konstanten Glieds, also ein Teiler von $-1$. Allerdings ist $f(1) = -1 \neq 0$ und $f(-1) = -1 \neq 0$, sodass $f$ keine rationalen Nullstellen besitzt. Als Polynom vom Grad 3 ist $f$ damit bereits über $\mathbb{Q}$ irreduzibel.
(b) Wir zeigen, dass $b \neq 0$. Angenommen, $b = 0$. Dann gilt $0 = 2a^2 - a - 2$, also $0 = a^2 - 0.5a - 1$. Somit ist $a$ eine Nullstelle von $g(x) = x^2 - 0.5x - 1 \in \mathbb{Q}[x]$. Da aber $f$ normiert und irreduzibel ist und zudem $f(a) = 0$ gilt, ist $f$ laut Vorlesung bereits das Minimalpolynom von $a$. Damit haben wir einen Widerspruch dazu, dass $a$ Nullstelle von $g$ ist, denn das Minimalpolynom $f = \mu_{\mathbb{Q},a}$ teilt dann $g$, was wegen $2 = \deg(g) < \deg(f) = 3$ ausgeschlossen ist.
(c) Wir bestimmen das Minimalpolynom von $a^2$ über $\mathbb{Q}$. Es gilt $a^2 \in \mathbb{Q}(a)$ und da

$\deg(f) = \deg(\mu_{\mathbb{Q},a}) = 3$ ist $[\mathbb{Q}(a) : \mathbb{Q}] = 3$. Es ist $\mathbb{Q}(a^2)$ ein Zwischenkörper von $\mathbb{Q}(a)|\mathbb{Q}$ und die Gradformel liefert, dass $[\mathbb{Q}(a^2) : \mathbb{Q}]$ ein positiver Teiler von 3 ist, also 1 oder 3. Falls $[\mathbb{Q}(a^2) : \mathbb{Q}] = 1$, dann ist $a^2 \in \mathbb{Q}$, sodass ein $q \in \mathbb{Q}$ mit $a^2 - q = 0$ existiert. Dann ist aber $a$ eine Nullstelle von $h = x^2 - q \in \mathbb{Q}[x]$, was ein Widerspruch zur Gradminimalität von $f = \mu_{\mathbb{Q},a}$ erzeugt, denn $\deg(h) = 2 < \deg(f) = 3$. Somit ist nur $[\mathbb{Q}(a^2) : \mathbb{Q}] = 3$ möglich. Damit setzen wir $h = x^2 + rx^2 + sx + t$ mit $r, s, t \in \mathbb{Q}$ für das Minimalpolynom von $a^2$ an. Es muss gelten $h(a^2) = 0$, sodass

$$\begin{aligned} 0 &= a^6 + ra^4 + sa^2 + t && (254)\\ &= (a+1)^2 + ra(a+1) + sa^2 + t && (255)\\ &= a^2 + 2a + 1 + ra^2 + ra + sa^2 + t && (256)\\ &= (1 + r + s)a^2 + (2 + r)a + (t + 1), && (257) \end{aligned}$$

sodass $0 = 1+r+s$ und $0 = 2+r$ und $t+1 = 0$, da $\{1, a, a^2\}$ laut Vorlesung eine Basis von $\mathbb{Q}(a)$ als $\mathbb{Q}$-Vektorraum bilden und in dieser Eigenschaft linear unabhängig sind. Aus dem linearen Gleichungssystem lesen wir $t = -1$, $r = -2$ und $s = 1$ ab. Damit ist $h = x^3 - 2x^2 + x - 1$ ein Polynom aus $\mathbb{Q}[x]$, das normiert ist und $a^2$ als Nullstelle besitzt. Um zu sehen, dass $h$ auch irreduzibel über $\mathbb{Q}$ ist, bemerken wir, dass $h$ ganzzahlige Koeffizienten hat und infolge der Normiertheit jede rationale Nullstelle von $h$ bereits ganzzahlig und insbesondere ein Teiler von $-1$, dem konstanten Glied, ist. Es ist $h(-1) = -5 \neq 0$ und $h(1) = -1 \neq 0$, sodass $h$ nullstellenfrei in $\mathbb{Q}$ ist. Als Polynom vom Grad 3 ist $h$ damit bereits irreduzibel in $\mathbb{Q}[x]$. Da $h$ insgesamt normiert und irreduzibel ist sowie $a^2$ als Nullstelle besitzt, gilt $h = \mu_{\mathbb{Q},a^2}$. □

**Aufgabe 215 (H19T2A3)** Sei $\alpha \in \mathbb{Q}$ und $\beta \in \mathbb{R}^\times$ sowie $\gamma = \alpha + \beta i$. Ferner sei $\beta$ algebraisch über $\mathbb{Q}$. Wir sollen zeigen, dass $[\mathbb{Q}(\gamma) : \mathbb{Q}]$ endlich und gerade ist. Zunächst gilt, dass $\beta, i \in \mathbb{Q}^{\text{alg}}$, denn $\beta$ ist nach Voraussetzung algebraisch über $\mathbb{Q}$ und $i$ ist als Nullstelle des Polynoms $x^2 + 1 \in \mathbb{Q}[x]$ ebenfalls algebraisch über $\mathbb{Q}$. Zusammen mit $\alpha \in \mathbb{Q} \subseteq \mathbb{Q}^{\text{alg}}$ folgt $\gamma = \alpha + i\beta \in \mathbb{Q}^{\text{alg}}$, sodass $\gamma$ ebenfalls algebraisch über $\mathbb{Q}$ ist. Daher existiert ein $h \in \mathbb{Q}[x]$, sodass $h(\gamma) = 0$. Wegen $[\mathbb{Q}(\gamma) : \mathbb{Q}] \leq \deg(h)$ ist der zu untersuchende Erweiterungsgrad endlich. Um zu sehen, dass $[\mathbb{Q}(\gamma) : \mathbb{Q}]$ gerade ist, definieren wir $K := \mathbb{Q}(\gamma) \cap \mathbb{R}$. $K$ ist ein Zwischenkörper von $\mathbb{Q}(\gamma)|\mathbb{Q}$ und sogar echter Zwischenkörper, denn wegen $\beta \neq 0$ ist $\gamma \notin K$. Andererseits ist $f = (x - \gamma)(x - \bar{\gamma}) = x^2 - 2\alpha x + (\beta^2 + \alpha^2)$ ein Polynom aus $K[x]$. Denn, es ist $i\beta = \gamma - a \in \mathbb{Q}(\gamma)$, also auch $-i\beta \in \mathbb{Q}(\gamma)$. Da $\mathbb{R} \ni \beta^2 = (i\beta)(-i\beta) \in \mathbb{Q}(\gamma)$, gilt $\beta^2 \in K$. Zusammen mit $\alpha, \alpha^2 \in \mathbb{Q} \subseteq K$ folgt, dass $f \in K[x]$ wie behauptet. Nun ist $f$ normiert und als Polynom vom Grad 2 wegen $\gamma \notin K$ irreduzibel über $K$, hat aber $\gamma$ als Nullstelle per Konstruktion. Somit ist $\mu_{K,\gamma} = f$, also $[\mathbb{Q}(\gamma) : K] = \deg(f) = 2$. Die Gradformel liefert $[\mathbb{Q}(\gamma) : \mathbb{Q}] = [\mathbb{Q}(\gamma) : K][K : \mathbb{Q}] = 2[K : \mathbb{Q}]$, sodass $[\mathbb{Q}(\gamma) : \mathbb{Q}]$ gerade ist. □

**Aufgabe 216 (H17T3A5)** Sei $K \subseteq \mathbb{R}$ Teilkörper und $f \in K[x]$. Sei $Z = \text{Zerf}(f|K) \subseteq \mathbb{C}$ und $[Z : K]$ ungerade. Zu zeigen ist, dass dann bereits $Z \subseteq \mathbb{R}$ als Teilkörper. Angenommen, $Z \not\subseteq \mathbb{R}$, dann ist $K \subseteq L := Z \cap \mathbb{R} \subsetneq Z$ und $L$ ist echter Zwischenkörper von $Z|K$. Da $Z \not\subseteq \mathbb{R}$ gibt es eine nicht-reelle Nullstelle $\gamma$ von $f$, $\gamma \in Z$. Da $f$ ferner ein Polynom ist, dessen Koeffizienten in einem Teilkörper von

$\mathbb{R}$ liegen, ist auch $\bar{\gamma}$ eine Nullstelle von $f$. Nun ist $h = (x-\gamma)(x-\bar{\gamma})$ ein Polynom in $L[x]$, denn $\bar{\gamma}, \gamma \in Z$ also $\gamma + \bar{\gamma} \in Z$ und $\gamma\bar{\gamma} \in Z$ aber gleichzeitig $\gamma + \bar{\gamma} \in \mathbb{R}$ und $\gamma\bar{\gamma} \in \mathbb{R}$, also $\gamma + \bar{\gamma}, \gamma\bar{\gamma} \in L$. Da aber $\gamma, \bar{\gamma} \notin \mathbb{R}$ hat $h$ keine Nullstellen in $L$ und ist damit als Polynom von Grad 2 über $L$ irreduzibel. Wegen $h(\gamma) = 0$ und der Normiertheit von $h$ gilt $h = \mu_{L,\gamma}$. Somit ist $[L(\gamma) : L] = \deg(h) = 2$. Die Gradformel liefert nun $[Z : K] = [Z : L(\gamma)][L(\gamma) : L][L : K] = 2[Z : L(\gamma)][L : K]$, sodass $[Z : K]$ gerade ist. Das widerspricht aber der Voraussetzung, dass $[Z : K]$ ungerade ist. Somit war die Annahme, $Z \not\subseteq \mathbb{R}$ falsch und es gilt $Z \subseteq \mathbb{R}$. □

**Aufgabe 217 (F16T2A3)** Gegeben sei $f = x^4 - 6x^2 - 14 \in \mathbb{Q}[x]$.
(a) Wir zeigen, dass $K = \mathbb{Q}(\sqrt{3+\sqrt{23}}, \sqrt{-14})$ der Zerfällungskörper von $f$ ist. Die Nullstellen von $f$ finden wir aus

$$\begin{aligned} 0 &= x^4 - 6x^2 - 14 \\ \Leftrightarrow 23 &= x^4 - 6x^2 + 9 \\ \Leftrightarrow 23 &= (x^2-3)^2 \\ \Leftrightarrow \{\pm\sqrt{23}\} &\ni x^2 - 3 \\ \Leftrightarrow \{\pm\sqrt{3 \pm \sqrt{23}}\} &\ni x \end{aligned} \tag{258}$$

Wir setzen $N = \{\pm\sqrt{3 \pm \sqrt{23}}\}$. Der Zerfällungskörper $L$ von $f$ über $\mathbb{Q}$ ist dann definitionsgemäß $L = \mathbb{Q}(N)$. Wir zeigen nun $L = K$. Es reicht zu zeigen, dass $\{\sqrt{3+\sqrt{23}}, \sqrt{-14}\} \subseteq \mathbb{Q}(N)$ und $N \subseteq K$. Für die erste zu prüfende Aussage beachten wir, dass

$$\sqrt{3+\sqrt{23}}\sqrt{3-\sqrt{23}} = \sqrt{3^2 - \sqrt{23}^2} = \sqrt{9-23} = \sqrt{-14}. \tag{259}$$

Aus dieser Identität sehen wir unmittelbar, dass $\sqrt{-14} \in \mathbb{Q}(N)$. Da $N \ni \sqrt{3+\sqrt{23}}$, haben wir $\{\sqrt{3+\sqrt{23}}, \sqrt{-14}\} \subseteq \mathbb{Q}(N)$, also $K \subseteq L$. Um auch die umgekehrte Inklusion zu zeigen, beachten wir, dass die obenstehende Identität unmittelbar

$$\sqrt{3-\sqrt{23}} = \sqrt{-14} : \sqrt{3+\sqrt{23}} \in K \tag{260}$$

liefert. Zusammen mit $-1 \in K$ haben wir also $\sqrt{3+\sqrt{23}}, -\sqrt{3+\sqrt{23}}, \sqrt{3-\sqrt{23}} = \sqrt{-14} : \sqrt{3+\sqrt{23}}, -\sqrt{3-\sqrt{23}} = -\sqrt{-14} : \sqrt{3+\sqrt{23}} \in K$, also $N \subseteq K$. Somit ist $L = \mathbb{Q}(N) \subseteq K$ und insgesamt haben wir Gleichheit $K = L$.
(b) Wir zeigen nun, dass $[K : \mathbb{Q}] = 8$. Wir haben in Teil (a) festgestellt, dass $\alpha = \sqrt{3+\sqrt{23}}$ Nullstelle von $f$ ist, was normiert und mit ganzzahligen Koeffizienten ist und wegen des Eisensteinkriteriums zur Primzahl $p = 2$ über $\mathbb{Z}$ irreduzibel ist, wegen des Lemmas von Gauss dann auch über $\mathbb{Q}$. Somit ist $f = \mu_{\mathbb{Q},\alpha}$ und wegen $\deg(f) = 4$ ist $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Da $\alpha \in \mathbb{R}$, ist auch $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$ als Teilkörper. Für $\beta = \sqrt{-14}$ hingegen gilt, dass $\beta \notin \mathbb{R}$ und, dass $\beta$ Nullstelle von $h = x^2 + 14 \in \mathbb{Q}[x]$ ist. $h$ ist normiert, mit ganzzahligen Koeffizienten und nach Eisenstein zur Primzahl 2 und dem Lemma von Gauss über $\mathbb{Q}$ irreduzibel. Da $h$ eine (und wegen $h \in \mathbb{Q}[x]$ damit bereits zwei) echt komplexe Nullstellen besitzt,

hat $h$ keine Nullstellen in $\mathbb{Q}(\alpha)$. Als Polynom vom Grad 2 ist $h$ somit auch in $\mathbb{Q}(\alpha)[x]$ irreduzibel. $h$ ist damit insgesamt das Minimalpolynom von $\sqrt{-14}$ über $\mathbb{Q}(\alpha)$ und es gilt $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}(\alpha)] = \deg(h) = 2$. Die Gradformel liefert uns nun $[K:\mathbb{Q}] = [\mathbb{Q}(\alpha,\beta):\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha):\mathbb{Q}] = 2\cdot 4 = 8$, was zu zeigen war. □

**Aufgabe 218 (F12T3A2)** Sei $2 \neq p$ eine Primzahl, $\zeta = \exp(2\pi i/p) \in \mathbb{C}$ und $\sqrt[n]{p} \in \mathbb{R}^+$ für alle $n \in \mathbb{N}$. Sei $L \subseteq \mathbb{C}$ der Zerfällungskörper von $f = x^p - p \in \mathbb{Q}[x]$ und $M \subseteq \mathbb{C}$ der Zerfällungskörper von $g = x^{p^2} - 1 \in \mathbb{Q}[x]$.
(a) Wir behaupten $L = \mathbb{Q}(\zeta, \sqrt[p]{p})$. Nach Definition eines Zerfällungskörpers ist $L = \mathbb{Q}(N)$, wobei $N$ die Menge der Nullstellen von $f$ in $\mathbb{C}$ ist. Da $\mathbb{C}$ algebraisch abgeschlossen ist, hat $f$ genau $p$ Nullstellen in $\mathbb{C}$. Sei $\zeta$ die primitive $p$-te Einheitswurzel, wie angegeben. Dann gilt $x_k = \sqrt[p]{p}\zeta^k$ für $0 \leq k < p$ ist eine Nullstelle von $f$. Denn $x_k^p = \sqrt[p]{p}^p(\zeta^k)^p = p(\zeta^p)^k = p\cdot 1 = p$. Da $\zeta$ primitive $p$-te Einheitswurzel ist, sind zudem $\{\zeta^k | 0 \leq k < p\}$ paarweise verschieden. Damit haben wir insbesondere $p$ verschiedene Nullstellen gefunden und wir müssen $\mathbb{Q}(\sqrt[p]{p}, \zeta) = \mathbb{Q}(N)$ noch nachrechnen. Es gilt $\sqrt[p]{p} = \sqrt[p]{p}\zeta^0 \in N$ und zudem $\mathbb{Q}(N) \ni \sqrt[p]{p}\zeta / \sqrt[p]{p} = \zeta$. Also gilt laut Vorlesung bereits $\mathbb{Q}(N) \supseteq \mathbb{Q}(\sqrt[p]{p}, \zeta)$. Umgekehrt ist für jedes $0 \leq k \leq p-1$ auch $\sqrt[p]{p}\zeta^k \in \mathbb{Q}(\zeta, \sqrt[p]{p})$. Damit ist $N \subseteq \mathbb{Q}(\zeta, \sqrt[p]{p})$ und wir erhalten $\mathbb{Q}(N) \subseteq \mathbb{Q}(\zeta, \sqrt[p]{p})$ unter Rückgriff auf ein Vorlesungsresultat.
(b) Wir sollen nun zeigen, dass $[L:\mathbb{Q}] = [M:\mathbb{Q}]$. Zunächst ist $M$ der Zerfällungskörper des Polynoms $g = x^{p^2}-1$. Die Nullstellen dieses Polynoms in $\mathbb{C}$ sind gerade die $p^2$-ten Einheitswurzeln, sodass $[M:\mathbb{Q}] = \deg(\Phi_{p^2}) = \Phi(p^2) = p^2 - p$ resultiert, wo $\Phi(...)$ die Eulersche $\Phi$-Funktion und $\Phi_{p^2}$ das $p^2$-te Kreisteilungspolynom ist. Wir zeigen nun auch, dass $[L:\mathbb{Q}] = p^2 - p$. Dazu beachten wir, dass $f = x^p - p$ wegen Eisenstein zur Primzahl $p$ über $\mathbb{Q}$ irreduzibel ist. Zudem ist es normiert und es gilt $f(\sqrt[p]{p}) = 0$. Damit ist $f$ das Minimalpolynom von $\sqrt[p]{p}$ über $\mathbb{Q}$. Für $\mathbb{Q}(\sqrt[p]{p})$ gilt wegen $\sqrt[p]{p} \in \mathbb{R}^+$, dass $\mathbb{Q}(\sqrt[p]{p}) \subseteq \mathbb{R}$ und wegen $\deg(f) = p$, dass $[\mathbb{Q}(\sqrt[p]{p}):\mathbb{Q}]$. Da $L$ aus $\mathbb{Q}(\sqrt[p]{p})$ durch Adjunktion der primitiven $p$-ten Einheitswurzel $\zeta$ entsteht, die Nullstelle des über $\mathbb{Q}$ irreduziblen normierten $p$-ten Kreisteilungspolynoms $\Phi_p(x) = x^{p-1} + ... + x + 1$ ist, $[L:\mathbb{Q}] = [\mathbb{Q}(\zeta, \sqrt[p]{p}):\mathbb{Q}(\sqrt[p]{p})][\mathbb{Q}(\sqrt[p]{p}):\mathbb{Q}] \leq [\mathbb{Q}(\zeta):\mathbb{Q}][\mathbb{Q}(\sqrt[p]{p}):\mathbb{Q}] = p^2 - p$. Andererseits ist $\mathbb{Q}(\sqrt[p]{p})$ bzw. $\mathbb{Q}(\zeta)$ jeweils ein Zwischenkörper der Erweiterung $L|\mathbb{Q}$ vom respektiven Erweiterungsgrad $p$ bzw. $p-1$. Da $p$ Primzahl ist, gilt $\mathrm{kgV}(p, p-1) = p^2 - p | [L:\mathbb{Q}]$, sodass auch $[L:\mathbb{Q}] = p^2 - p$. Zusammen mit dem ersten Teilresultat der Aufgabe haben wir also $[L:\mathbb{Q}] = [M:\mathbb{Q}]$.
(c) Wir zeigen nun, dass die Galoisgruppe $G_1 := \mathrm{Gal}(L|\mathbb{Q})$ nicht abelsch ist. Aus der Vorlesung ist bekannt, dass $|G_1| = [L:\mathbb{Q}] = p^2 - p$. Angenommen, $G_1$ ist abelsch. Dann gibt es eine Untergruppe der Ordnung $p-1$ von $G_1$, bezeichnet mit $U$. Da $G_1$ abelsch ist, gilt $U \trianglelefteq G$. Es ist $\mathbb{Q}(\sqrt[p]{p})$ ein Zwischenkörper von $L|\mathbb{Q}$ und es gilt $[\mathbb{Q}(\sqrt[p]{p}):\mathbb{Q}] = p$. Indem wir $U$ nach dem Hauptsatz der Galoistheorie so wählen, dass $\mathbb{Q}(\sqrt[p]{p}) = L^U$, haben wir $(G:U) = p = [L^U:\mathbb{Q}]$. Da $U$ ein Normalteiler von $G_1$ ist, ist $L^U|\mathbb{Q}$ normal. Aber $L^U|\mathbb{Q}$ ist nicht normal, denn $\sqrt[p]{p}$ hat $f$ als Minimalpolynom, aber dieses Polynom zerfällt über $\mathbb{Q}(\sqrt[p]{p}) \subseteq \mathbb{R}$ nicht in Linearfaktoren, denn die übrigen, in (a) gegebenen Nullstellen von $f$ haben nicht-verschwindenden Imaginärteil. Damit haben wir einen Widerspruch zur Annahme, $\mathrm{Gal}(L|\mathbb{Q}) = G_1$ wäre abelsch. Somit ist $\mathrm{Gal}(L|\mathbb{Q})$ nicht-abelsch.
(d) Wir zeigen nun, dass $\mathrm{Gal}(L|\mathbb{Q})$ und $\mathrm{Gal}(M|\mathbb{Q})$ nicht isomorph sind. Da $M$ nach

(b) der Zerfällungskörper von $x^{p^2}-1$ über $\mathbb{Q}$ ist, gilt $G_2 := \mathrm{Gal}(M|\mathbb{Q}) \simeq (\mathbb{Z}/p^2\mathbb{Z}) \simeq \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Insbesondere ist $G_2$ abelsch. Somit kann $G_2$ nicht isomorph zum nach Teil (d) nicht-abelschen $G_1 = \mathrm{Gal}(L|\mathbb{Q})$ sein. □

**Aufgabe 219 (F18T3A5)** Sei $K = \mathbb{Q}(i)$, $\alpha = \sqrt[4]{7}$ und $L$ der Zerfällungskörper von $f = x^4 - 7 \in \mathbb{Q}[x]$.
(a) Wir zeigen, dass $L = K(\alpha)$. Dazu bestimmen wir die komplexen Nullstellen von $f$. Es gilt $0 = x^4 - 7 \Leftrightarrow x \in \{\pm\alpha, \pm i\alpha\}$. Somit müssen wir zeigen, dass $K(N) = \mathbb{Q}(\{i\} \cup N) = \mathbb{Q}(i, \alpha) = K(\alpha)$. Offenbar gilt $i, \alpha \in \mathbb{Q}(i, \alpha)$ und somit auch $\pm\alpha, \pm i\alpha \in \mathbb{Q}(i, \alpha)$. Damit ist bereits $K(N) \subseteq K(\alpha)$. Andersherum ist $i, \alpha \in K(N)$ und daher ist auch $K(\alpha) \subseteq K(N)$. Insgesamt haben wir also Gleichheit.
(b) Wir sollen die Grade der Erweiterung $L|\mathbb{Q}$ und $L|K$ bestimmen. Zunächst ist nach (a) $L = \mathbb{Q}(i, \alpha)$. Es ist sogar $f = x^4 - 7 \in \mathbb{Q}[x]$ und es gilt $f(\alpha) = 0$. Da $f$ normiert und wegen Eisenstein zur Primzahl $p = 7$ irreduzibel über $\mathbb{Q}$ ist, handelt es sich bei $f$ um das Minimalpolynom $\mu_{\mathbb{Q},\alpha}$. Damit ist $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f) = 4$. Nun ist $i$ Nullstelle des über $\mathbb{Q}$ irreduziblen Polynoms $x^2 + 1$. Als Polynom vom Grad 2 und weil $x^2 + 1$ auch über $\mathbb{R} \supseteq \mathbb{Q}(\alpha)$ keine Nullstellen besitzt, ist es irreduzibel auch über $\mathbb{Q}(\alpha)$. Damit ist $x^2 + 1 = \mu_{\mathbb{Q}(\alpha),i}$ unter zusätzlicher Beachtung der Normiertheit von $x^2 + 1$. Also ist $[L = \mathbb{Q}(\alpha, i) : \mathbb{Q}(\alpha)] = \deg(x^2 + 1) = 2$. Mithilfe der Gradformel erhalten wir $[L : \mathbb{Q}] = [L : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot 4 = 8$. Nach den obigen Ausführungen ist auch $x^2 + 1 = \mu_{\mathbb{Q},i}$, sodass $[K : \mathbb{Q}] = \deg(x^2 + 1) = 2$. Nochmaliges Anwenden der Gradformel liefert dann

$$[L : \mathbb{Q}] = [L : K][K : \mathbb{Q}] \Leftrightarrow [L : K] = \frac{[L : \mathbb{Q}]}{[K : \mathbb{Q}]} = \frac{8}{2} = 4. \tag{261}$$

Damit ist $[L : \mathbb{Q}] = 8$ und $[L : K] = 4$.
(c) Wir zeigen, dass $L|K$ galoissch ist. Zunächst ist $L|\mathbb{Q}$ als endliche, und da von endlich vielen, nämlich 2, über $\mathbb{Q}$ algebraischen Elementen erzeugte Erweiterung über einem perfekten Körper separabel. Dasselbe gilt für $K|\mathbb{Q}$. Somit ist auch $L|K$ separabel. Nach Definition ist $L$ der Zerfällungskörper von $f$ über $K$, und weil $f \in \mathbb{Q}[x]$, ist $L$ auch der Zerfällungskörper von $f$ über $\mathbb{Q}$. Damit ist sowohl $L|K$ als auch $L|\mathbb{Q}$ normal. Somit ist $L|\mathbb{Q}$ galoissch. Damit ist laut Vorlesung bereits $L|K$ ebenfalls galoissch.
(d) Sei nun $\sigma \in \mathrm{Gal}(L|K)$ sodass $\sigma(\alpha) = i\alpha$. Wegen $i \in K$ gilt $\sigma^2(\alpha) = \sigma(i\alpha) = i\sigma(\alpha) = i^2\alpha = -\alpha$. Zudem ist $\sigma^3(\alpha) = \sigma(\sigma^2(\alpha)) = \sigma(-\alpha) = -\sigma(\alpha) = -i\alpha$ und $\sigma^4(\alpha) = -i\sigma(\alpha) = i(-i)\alpha = \alpha$. Damit hat $\sigma$ die Ordnung 4 in $\mathrm{Gal}(L|K)$. Weil zudem $\mathrm{Gal}(L|K) = [L : K] = 4$, ist $\mathrm{Gal}(L|K)$ von der Ordnung 4, und weil $\langle\sigma\rangle \leq \mathrm{Gal}(L|K)$ eine Untergruppe der Ordnung 4 ist, gilt bereits $\mathrm{Gal}(L|K) = \langle\sigma\rangle$. □

**Aufgabe 220** Gesucht ist der Erweiterungsgrad $[\mathbb{Q}(\sqrt[3]{2}, \sqrt{5}, \sqrt{-7}) : \mathbb{Q}]$. Zunächst ist $f_1 = x^3 - 2 \in \mathbb{Q}[x]$ und $f_2 = x^2 - 3 \in \mathbb{Q}[x]$ jeweils normiert und nach dem Eisensteinkriterium jeweils zur Primzahl 2 bzw. 3 irreduzibel über $\mathbb{Q}$. Da $f_1(\sqrt[3]{2}) = 0 = f_2(\sqrt{3})$ handelt es sich also um Minimalpolynome, genauer $f_1 = \mu_{\mathbb{Q},\sqrt[3]{2}}$ und $f_2 = \mu_{\mathbb{Q},\sqrt{3}}$. Wir schätzen mithilfe der Gradformel ab, dass $[\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] \leq [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = \deg(f_1)\deg(f_2) = 6$. Da zudem $\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt{3})$ Zwischenkörper von $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3})|\mathbb{Q}$ mit Erweiterungsgrad 3

respektive 2 über $\mathbb{Q}$ sind, gilt nach Gradformel $2|[\mathbb{Q}(\sqrt[3]{2},\sqrt{3}):\mathbb{Q}]$ und $3|[\mathbb{Q}(\sqrt[3]{2},\sqrt{3}):\mathbb{Q}]$ und damit auch $6=\mathrm{kgV}(2,3)|[\mathbb{Q}(\sqrt[3]{2},\sqrt{3}):\mathbb{Q}]$. Somit ist $6=[\mathbb{Q}(\sqrt[3]{2},\sqrt{3}):\mathbb{Q}]$. Da $\mathbb{Q}(\sqrt[3]{2},\sqrt{3})\subseteq\mathbb{R}$ und $f_3=x^2+7\in\mathbb{Q}[x]$ mit $\sqrt{-7},-\sqrt{-7}$ keine reellen Nullstellen hat, ist $f_3$ als Polynom vom Grad 2 bereits irreduzibel über $\mathbb{Q}(\sqrt[3]{2},\sqrt{3})$. Als irreduzibles, normiertes Polynom, das $\sqrt{-7}$ als Nullstelle ha, handelt es sich bei $f_3$ unter Beachtung der vorangegangenen Bemerkungen um das Minimalpolynom von $\sqrt{-7}$ über $\mathbb{Q}(\sqrt[3]{2},\sqrt{3})$. Damit ist $[\mathbb{Q}(\sqrt[3]{2},\sqrt{3},\sqrt{-7}):\mathbb{Q}(\sqrt[3]{2},\sqrt{3})]=\deg(f_3)=2$. Zusammen mit der Gradformel erhalten wir also $[\mathbb{Q}(\sqrt[3]{2},\sqrt{3},\sqrt{-7}):\mathbb{Q}]=[\mathbb{Q}(\sqrt[3]{2},\sqrt{3},\sqrt{-7}):\mathbb{Q}(\sqrt[3]{2},\sqrt{3})][\mathbb{Q}(\sqrt[3]{2},\sqrt{3}):\mathbb{Q}]=2\cdot 3=6$. □

**Aufgabe 221 (H15T3A4)** Sei $p>3$ eine Primzahl und $a\in\mathbb{Q}$ dergestalt, dass $f=x^p-a\in\mathbb{Q}[x]$ irreduzibel ist. Ferner ist $\zeta\in\mathbb{C}$ eine primitive $p$-te Einheitswurzel, $\alpha\in\mathbb{C}$ eine Nullstelle von $f$ und $Z=\mathbb{Q}(\alpha,\zeta)$.
(a) Wir zeigen, dass $Z$ Zerfällungskörper von $f$ ist und $[Z:\mathbb{Q}]=p(p-1)$ gilt. Die Nullstellenmenge von $f$ in $\mathbb{C}$ ist gerade $N=\{\alpha\zeta^k|0\leq k\leq p-1\}$, denn $f$ hat über dem algebraisch abgeschlossenen Körper $\mathbb{C}$ als Polynom vom Grad $p$ genau $p$ Nullstellen nach dem Fundamentalsatz der Algebra. Diese sind alle ungleich 0, wegen $|x|^p=|a|$ und $a\neq 0$, da $f$ sonst reduzibel die $p$-fache Nullstelle 0 besäße, also reduzibel wäre. Wir müssen also $\mathbb{Q}(\alpha,\zeta)=\mathbb{Q}(N)$ zeigen. Dazu reicht es laut Vorlesung, $\{\zeta,\alpha\}\subseteq\mathbb{Q}(N)$ und $N\subseteq\mathbb{Q}(\alpha,\zeta)$ zu zeigen. Für die erste Inklusion bemerken wir, dass bereits unmittelbar $\alpha\in N$ gilt und wegen $\alpha,\alpha\zeta\in N\subseteq\mathbb{Q}(N)$ direkt $\zeta=\alpha\zeta/\alpha\in\mathbb{Q}(N)$ folgt. Damit haben wir $\{\alpha,\zeta\}\subseteq\mathbb{Q}(N)$. Für die zweite Inklusion beachten wir, dass aus $\alpha,\zeta\in\mathbb{Q}(\alpha,\zeta)$ auch $\alpha\zeta^k\in\mathbb{Q}(\alpha,\zeta)$ für $0\leq k\leq p-1$ folgt. Somit ist $N\subseteq\mathbb{Q}(\alpha,\zeta)$. Insgesamt haben wir also $\mathbb{Q}(N)=\mathbb{Q}(\alpha,\zeta)$. Offenbar ist $f$ das Minimalpolynom von $\alpha$, denn $\alpha$ ist Nullstelle von $f$ und $f$ ist normiert und irreduzibel. Damit ist $\mathbb{Q}(\alpha)$ ein Zwischenkörper von $Z|\mathbb{Q}$, der den Erweiterungsgrad $p$ hat. Andererseits ist $\zeta$ eine primitive $p$-te Einheitswurzel und hat als solche das $p$-te Kreisteilungspolynom $\Phi_p=x^{p-1}+...+x+1\in\mathbb{Q}[x]$ als Minimalpolynom, über $\mathbb{Q}$ ($p\geq 3$). Damit ist $[\mathbb{Q}(\zeta):\mathbb{Q}]=p-1$ und $\mathbb{Q}(\zeta)$ ein weiterer Zwischenkörper von $Z|\mathbb{Q}$. Aus der Gradformel erhalten wir, dass $(p-1)|[Z:\mathbb{Q}]$ und $p|[Z:\mathbb{Q}]$, also $p(p-1)|[Z:\mathbb{Q}]$, da $p$ prim. Andererseits sind $\Phi_p$ und $f$ beide über $\mathbb{Q}$ irreduzibel und wir können abschätzen $[Z:\mathbb{Q}]=[Z:\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha):\mathbb{Q}]\leq[\mathbb{Q}(\zeta):\mathbb{Q}][\mathbb{Q}(\alpha):\mathbb{Q}]=(p-1)p$. Zusammen mit der vorher hergeleiteten Teilbarkeitsaussage folgt $[Z:\mathbb{Q}]=p^2-p$.
(b) Wir zeigen nun, dass $G=\mathrm{Gal}(Z|\mathbb{Q})$ genau eine $p$-Sylowgruppe besitzt. Diese ist dann ein Normalteiler von $G$ nach einer Folgerung aus dem zweiten Sylow-Satz. Da $|G|=[Z:\mathbb{Q}]=p(p-1)$, wissen wir aus dem dritten Sylowsatz, dass für die Anzahl $\nu_p$ der $p$-Sylowgruppen von $G$ gilt, dass $\nu_p|(p-1)$, also insbesondere $\nu_p<p$ und zudem $\nu_p\equiv 1\,\mathrm{mod}(p)$. Wegen $\nu_p<p$ ist nur $\nu_p=1$ möglich. Die einzige $p$-Sylowgruppe $H$ von $G$ ist damit ein Normalteiler von $G$. Da $[\mathbb{Q}(\zeta):\mathbb{Q}]=p-1=(G:H)$ nach dem Satz von Lagrange, ist $H=\mathrm{Gal}(Z|\mathbb{Q}(\zeta))$. Eine Folgerung aus dem Hauptsatz der Galois-Theorie besagt, dass für eine endliche Galois-Erweiterung $L|K$ mit Zwischenkörper $M$, sodass $M|K$ ebenfalls galoissch ist, $\Pi:\mathrm{Gal}(L|K)\to\mathrm{Gal}(M|K),\sigma\mapsto\sigma|_M$ vermöge eines Gruppenepimorphismus. Der Kern erfüllt $\ker\Pi=\mathrm{Gal}(L|M)$, sodass nach dem Homomorphiesatz für Gruppen $\mathrm{Gal}(L|K)/\mathrm{Gal}(L|M)\simeq\mathrm{Gal}(M|K)$. In unserem Beispiel ist $L=Z$, $M=\mathbb{Q}(\zeta)$ und $K=\mathbb{Q}$. Damit finden wir in der Notation unserer Bearbeitung

$G/H \simeq \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$, wobei die zuletzt aufgeführte Isomorphie aus der Vorlesung zur Galoistheorie der Kreisteilungskörper bekannt ist.
(c) Wir sollen einen Gruppenisomorphismus angeben, sodass $\mathrm{Gal}(Z|\mathbb{Q}(\alpha)) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$. Die Gruppe rechts ist isomorph zu $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$. Wir definieren $\mathrm{Gal}(Z|\mathbb{Q}(\alpha)) \to \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$ durch $\sigma \mapsto \sigma|_{\mathbb{Q}(\zeta)}$. Da $\mathbb{Q}(\zeta)|\mathbb{Q}$ normal ist, beschränkt sich jeder $\mathbb{Q}$-Homomorphismus $\mathbb{Q}(\zeta) \to Z$ zu einem $\mathbb{Q}$-Automorphismus $\mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta)$, also ein Element von $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$. Damit ist $\phi$ wohldefiniert. Da die Restriktion kompatibel mit der Komposition von Abbildungen ist, handelt es sich um einen Gruppenhomomorphismus. Die Surjektivität von $\phi$ ergibt sich direkt aus dem Fortsetzungssatz. Zum Nachweis der Injektivität sei $\sigma \in \mathrm{Gal}(Z|\mathbb{Q}(\alpha))$ mit $\phi(\sigma) = \mathrm{id}_{\mathbb{Q}(\zeta)}$ vorgegeben. Es ist $\sigma(\alpha) = \alpha$, da $\sigma$ ein $\mathbb{Q}(\alpha)$-Automorphismus von $Z$ ist und $\sigma(\zeta) = \zeta$. Damit ist $\sigma = \mathrm{id}_Z$ in $\mathrm{Gal}(Z|\mathbb{Q})$ laut Fortsetzungssatz, also $\ker\phi = \{\mathrm{id}_Z\}$. Damit haben wir zunächst die Isomorphie $\mathrm{Gal}(Z|\mathbb{Q}(\alpha)) \simeq \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$ und Komposition mit dem Isomorphismus aus (b) liefert uns den gewünschten Isomorphismus für $\mathrm{Gal}(Z|\mathbb{Q}(\alpha)) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$.
(d) Wir zeigen nun, dass $G = \mathrm{Gal}(Z|\mathbb{Q})$ mehr als eine 2-Sylowgruppe besitzt. Angenommen, $P$ ist die einzige 2-Sylowgruppe von $G$. Da $p \geq 3$, gilt $|P||(p-1)$ und somit ist $P$ auch eine und wegen der Annahme die einzige 2-Sylowgruppe von $\mathrm{Gal}(Z|\mathbb{Q}(\alpha))$. Nach dem Hauptsatz der Galoistheorie korrespondiert $P$ vermöge $P \mapsto Z^P =: M$ zu einem Zwischenkörper von $\mathbb{Q}(\alpha)|Z$. Da $p-1 \geq 2$ ist $\mathbb{Q}(\alpha) \subsetneq M$. Ebenso ist $\mathbb{Q}(\zeta\alpha) \subseteq M$ mit derselben Argumentation wie oben, denn $f(\zeta\alpha) = 0$ ebenfalls und $[\mathbb{Q}(\zeta\alpha) : \mathbb{Q}] = p$. Da nun $\alpha, \alpha\zeta \in M$ ist $\{\alpha, \zeta\} \subseteq M$ und mit $M \subseteq Z$ folgt bereits die Gleichheit $M = Z$. Das ist aber ein Widerspruch dazu, dass $P$ eine (nicht-triviale wegen $p-1 \geq 2$) 2-Sylowgruppe ist. □

**Aufgabe 222 (F14T3A4)** Sei $L \subseteq \mathbb{C}$ der Zerfällungskörper von $f = x^3 - \pi \in K[x]$, wo $K = \mathbb{Q}(\pi)$. Als bekannt wird vorausgesetzt, dass $\pi$ transzendent über $\mathbb{Q}$ ist.
(a) Wir behaupten, dass $[L : K] = 6$. Es ist zunächst $L = K(N)$, wo $N$ die Nullstellenmenge von $f$ in $\mathbb{C}$ ist. Es ist $N = \{\sqrt[3]{\pi}, \sqrt[3]{\pi}\zeta, \sqrt[3]{\pi}\zeta^2\}$, wo $\zeta$ eine primitive 3-te Einheitswurzel ist. Man rechnet leicht nach, dass für $X$ in der rechts stehenden Menge $f(X) = 0$. Da $f$ als Polynom vom Grad 3 genau 3 Nullstellen in $\mathbb{C}$ hat, haben wir damit bereits alle Nullstellen gefunden. Offenbar ist $L = K(\sqrt[3]{\pi}, \zeta)$, denn $\sqrt[3]{\pi}\zeta^k$ ist für $k \in \{0, 1, 2\}$ in $K(\sqrt[3]{\pi}, \zeta)$. Umgekehrt ist $\sqrt[3]{\pi} \in N$ und aus $\sqrt[3]{\pi}, \sqrt[3]{\pi} \in K(N)$ folgt $\zeta = \sqrt[3]{\pi}\zeta/\sqrt[3]{\pi} \in K(N)$. Laut Vorlesung reichte dies bereits aus, um die Gleichheit nachzuweisen. Wir behaupten nun, dass $f$ das Minimalpolynom von $\sqrt[3]{\pi}$ über $K$ ist. $f$ ist normiert und es gilt $f(\sqrt[3]{\pi}) = \sqrt[3]{\pi}^3 - \pi = \pi - \pi = 0$. Zum Nachweis der Irreduzibilität beachten wir, dass es wegen $\deg(f) = 3$ ausreicht, zu zeigen, dass $f$ keine Nullstellen in $K$ hat. Angenommen $\Pi \in K$ ist eine Nullstelle. Dann gilt $\Pi^3 = \pi$. Da $\Pi \in K$ gibt es Polynome $g, h \in \mathbb{Q}[x]$ mit $h(\pi) \neq 0$, sodass $\Pi = g(\pi)/h(\pi)$. Einsetzen liefert dann $g(\pi)^3/h(\pi)^3 = \pi$, was wir zu $g(\pi)^3 - \pi h(\pi)^3 = 0$ umformen können. Da $\mathbb{Q}[x]$ ein Ring ist, ist $H(x) := g(x)^3 - xh(x)^3 \in \mathbb{Q}[x]$ ein Polynom, das $\pi$ als Nullstelle hat (s. vorherige Rechnung). Das geht aber nicht, weil $\pi$ transzendent über $\mathbb{Q}$ ist. Somit ist $f$ nullstellenfrei in $K$ und als Polynom vom Grad 3 damit irreduzibel über $K$. Insgesamt ist also $f$ das Minimalpolynom von $\sqrt[3]{\pi}$ über $K$. Es ist $K(\sqrt[3]{\pi}) \subseteq \mathbb{R}$ und die primitive dritte Einheitswurzel $\zeta$ hat

nicht-verschwindenden Imaginärteil. Da sie über $\mathbb{Q}$ das dritte Kreisteilungspolynom $\Phi_3 = x^2 + x + 1$, welches Grad 2 hat, als Minimalpolynom hat, ist $\Phi_3$ auch das Minimalpolynom von $\zeta$ über $K$. Andernfalls wäre $\Phi_3$ reduzibel über $K$, hätte also eine rein reelle Nullstelle, was aber nicht der Fall ist. Damit ist nach der Gradformel $[K(\sqrt[3]{\pi}, \zeta) : K] = [K(\sqrt[3]{\pi})(\zeta) : K(\sqrt[3]{\pi})][K(\sqrt[3]{\pi}) : K] = 2 \cdot 3 = 6$, denn $[K(\sqrt[3]{\pi}) : K] = \deg(x^3 - \pi) = 3$ und $[K(\sqrt[3]{\pi})(\zeta) : K(\sqrt[3]{\pi})] = \deg(x^2 + x + 1) = 2$.
(b) Da $L$ der Zerfällungskörper von $f$ über $K$ ist, gibt es laut Vorlesung einen injektiven Gruppenhomomorphismus $\mathrm{Gal}(L|K) \to S_{\deg(f)=3}$. Da $|\mathrm{Gal}(L|K)| = [L : K] = 6$, ist $\mathrm{Gal}(L|K) = S_3$. Nach dem Hauptsatz der Galoistheorie entsprechen die Zwischenkörper $F$ von $L|K$ vermöge einer antitonischen Bijektion gerade den Untergruppen von $\mathrm{Gal}(L|K)$. Die $S_3$ hat die beiden trivialen Untergruppen $\{\mathrm{id}\}, S_3$, die zu $L$ respektive $K$ vermöge des Hauptsatzes der Galoistheorie korrespondieren und für die Angabe der gesuchten echten Zwischenkörper unbeachtlich sind. Ferner hat die $S_3$ drei Untergruppen der Ordnung 2 und eine Untergruppe der Ordnung 2. Die drei Untergruppen der Ordnung 2 korrespondieren dann zu Zwischenkörpern $M_1, M_2, M_3$ die Erweiterungsgrad 3 über $K$ haben. Die Untergruppe der Ordnung 2 korrespondiert zu einem Zwischenkörper $M_4$ des Erweiterungsgrads 2 über $K$. Es ist $M_4 = K(\zeta)$, denn $[K(\zeta) : K] = \deg(x^2 + x + 1) = 2$. Ebenso ist $x^3 - \pi$ Minimalpolynom jedes $X \in N$, sodass wir mit $M_1 = K(\sqrt[3]{\pi})$, $M_2 = K(\sqrt[3]{\pi}\zeta)$ und $M_3 = K(\sqrt[3]{\pi}\zeta^2)$ drei weitere Zwischenkörper von $L|K$ vom Erweiterungsgrad 3 diesmal gefunden haben. Da $M_1 \subseteq \mathbb{R}$ ist $M_1 \neq M_2$ und $M_1 \neq M_3$. Um $M_2 \neq M_3$ zu sehen, beachten wir, dass falls $M_2 = M_3$ wäre aus $\sqrt[3]{\pi}\zeta, \sqrt[3]{\pi}\zeta^2 \in M_2$ direkt $\sqrt[3]{\pi} = (\sqrt[3]{\pi})^2/(\sqrt[3]{\pi}\zeta^2), \zeta = \sqrt[3]{\pi}\zeta^2/\sqrt[3]{\pi} \in M_2$ folgt. Damit wäre aber bereits $M_2 = L$, was $[M_2 : K] = 3 \neq [L : K] = 6$ widerspricht. Also sind $M_1, M_2, M_3$ paarweise verschiedene Zwischenkörper von $L$.
(c) Die trivialen Erweiterungen $K|K$ und $L|K$ sind normal, im ersten Fall weil der Erweiterungsgrad gleich 1 ist und im zweiten Fall, weil $L$ gerade Zerfällungskörper von $f$ über $K$ ist. Da $[M_4 : K] = 2$, ist $M_4|K$ normal. $M_l|K$ ist für $l\{1, 2, 3\}$ nicht normal, denn dann das bedeutet gerade, dass die Galois-Gruppen $\mathrm{Gal}(L|M_l) \trianglelefteq \mathrm{Gal}(L|K) \simeq S_3$. Da diese Galois-Gruppen jeweils die Ordnung 2 haben, sind sie 2-Sylowgruppen von $S_3$. Damit eine 2-Sylowgruppe aber Normalteiler sein kann, muss sie die einzige 2-Sylowgruppe sein, was bei der $S_3$ aber nicht der Fall ist. Somit ist $M_l|K$ für kein $k \in \{1, 2, 3\}$ normal. □

**Aufgabe 223** Gesucht ist der Erweiterungsgrad $[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt[5]{2}) : \mathbb{Q}]$. Die ganzen Zahlen 2 und 3 sind als Primzahlen insbesondere quadratfrei in der Primfaktorzerlegung, sodass $\sqrt{2} \notin \mathbb{Q}(\sqrt{3})$ und $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Da $f_1 = x^2 - 2$ und $f_2 = x^2 - 3$ als normierte Polynome aus $\mathbb{Q}[x]$ nach dem Eisensteinkriterium zur Primzahl $p = 2$ respektive $p = 3$ jeweils über $\mathbb{Q}$ irreduzibel sind, haben wir direkt $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})]$. Es gilt somit $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ nach der Gradformel. Wegen $f_3 = x^5 - 2 \in \mathbb{Q}[x]$ normiert und, wegen Eisenstein mit $p = 2$ ist $f_3$ über $\mathbb{Q}$ irreduzibel, ist $[\mathbb{Q}(\sqrt[5]{2}) : \mathbb{Q}] = \deg(f_3) = 5$, denn es ist zusätzlich $f_3(\sqrt[5]{2}) = 0$, sodass $f_3 = \mu_{\mathbb{Q}, \sqrt[5]{2}}$. Da $\mathbb{Q}(\sqrt[5]{2}), \mathbb{Q}(\sqrt{2}, \sqrt{3})$ jeweils Zwischenkörper von $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt[5]{2})|\mathbb{Q}$ von teilerfremden Erweiterungsgrad, $\mathrm{ggT}(4, 5) = 1$, sind, ist $20|[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt[5]{2}) : \mathbb{Q}]$. Mittels Gradformel sehen wir aber, dass $[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt[5]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt[5]{2}) : \mathbb{Q}(\sqrt{2}, \sqrt{3})][\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] \leq [\mathbb{Q}(\sqrt[5]{2}) : \mathbb{Q}][\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 5 \cdot 4 = 20$. Zu-

sammen mit der Teilbarkeitsaussage, die wir vorher hergeleitet haben, folgt nun $[\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt[5]{2}):\mathbb{Q}]=20$. □

**Aufgabe 224 (H19T1A5)** Gegeben sei die Gleichung $x^2+ux+v=0$ in $\mathbb{F}_q$.
(a) Sei $q$ ungerade. Die Gleichung von oben ist lösbar genau dann wenn es ein $a\in\mathbb{F}_q$ gibt, sodass $a^2+ua+v=0$. Da für $q$ ungerade 2 und damit 4 in der Einheitengruppe $\mathbb{F}_q^\times$ ist, haben wir $4a^2+4ua+4v=0$. Letzteres ist äquivalent zu $4a^2+4ua+u^2=(2a+u)2=u^2-4v$. Indem wir $b=2a+u$ setzen, sehen wir, dass die angegebene quadratische Gleichung genau dann lösbar in $\mathbb{F}_q$ ist, wenn ein $b\in\mathbb{F}_q$ existiert, sodass $b^2=u^2-4v$, mit anderen Worten, wenn $u^2-4v$ ein Quadrat in $\mathbb{F}_q$ ist.
(b) Sei $q$ nun gerade und $u\neq 0$. Die Gleichung ist genau dann lösbar über $\mathbb{F}_q$ wenn ein $a\in\mathbb{F}_q$ existiert, sodass $a^2+ua+v=0$, d.h., wegen $u\neq 0$, $(a/u)^2+(a/u)=-v/u^2$. Wegen $a/u\in\mathbb{F}_q$ bedeutet das gerade, dass $-v/u^2$ von der Form $-v/u^2=z^2+z$ mit $z=a/u$ ist. Da $\mathrm{char}(\mathbb{F}_q)=2$, wegen $q$ gerade, ist das somit gleichbedeutend mit $v/u^2=z^2+z$ mit dem oben definierten $z$. □

**Aufgabe 225 (H19T3A4)** Sei $p$ eine Primzahl.
(a) Ist $g\in\mathbb{F}_p[X]$ vom Grad $m$ und irreduzibel über $\mathbb{F}_p$, so ist die Teilbarkeitsrelation $g|X^{p^m}-X$ erfüllt. Bis auf eine Einheit ist dann $g$ das Minimalpolynom eines $\alpha\in\bar{\mathbb{F}}_p$, einem algebraischen Abschluss von $\mathbb{F}_p$. Dann ist $[\mathbb{F}_p(\alpha):\mathbb{F}_p]=m$. Damit ist $\mathbb{F}_p(\alpha)=\mathbb{F}_{p^m}$ wegen der Eindeutigkeit endlicher Körper. Andererseits besteht $\mathbb{F}_{p^m}$ gerade aus den Nullstellen von $X^{p^m}-X$ in $\bar{\mathbb{F}}_p$. Da $\mathbb{F}_p[X]$ euklidisch ist, finden wir, dass $X^{p^m}-X=q(X)g(X)+r(X)$ mit einem Polynom $q,r\in\mathbb{F}_p[X]$ und $\deg(r)<m$. Einsetzen von $\alpha$ liefert dann $r(\alpha)=0$. Sei nun $r\neq 0$. Da $\deg(r)<\deg(g)=m$, haben wir einen Widerspruch dazu, dass $g$ Minimalpolynom von $\alpha$ ist, also dasjenige normierten Polynom minimalen Grades ist, das $\alpha$ als Nullstelle besitzt. Damit haben wir einen Widerspruch zu $r\neq 0$. Da somit $r=0$ haben wir $X^{p^m}-X=q(X)g(X)$ und damit die Teilbarkeitsrelation $g|X^{p^m}-X$.
(b) Wir zeigen, dass $f\in\mathbb{F}_p[X]$ irreduzibel über $\mathbb{F}_p$ ist genau dann, wenn für alle $m\in\mathbb{N}$ gilt mit $1\leq m\leq\deg(f)/2$, dass $\mathrm{ggT}(f(X),X^{p^m}-X)$. Sei $f$ ist reduzibel über $\mathbb{F}_p$. Dann gibt es ein irreduzibles $h\in\mathbb{F}_p[X]$ mit der Eigenschaft, dass $\deg(h)\leq\deg(f)/2$ und $h|f$. Da $h$ irreduzibel über $\mathbb{F}_p[X]$ ist, gilt laut Teil (a), dass $h|X^{p^{\deg(h)}}-X$ und somit gibt es mindestens ein $m$, $1\leq m\leq\deg(f)/2$, sodass $\mathrm{ggT}(X^{p^m}-X,f)\neq 1$. Sei $f$ nun irreduzibel über $\mathbb{F}_p$ und $m$, $1\leq m\leq\deg(f)/2$, dann ist $\mathrm{ggT}(f,X^{p^m}-X)\in\{1,f\}$. Falls $\mathrm{ggT}(f,X^{p^m}-X)=f$, dann ist jede Nullstelle von $f$ in einem algebraischen Abschluss von $\mathbb{F}_p$ auch eine Nullstelle von $X^{p^m}-X$. Da $f$ irreduzibel ist, ist $f$ bis auf eine Einheit Minimalpolynom eines $\alpha\in\bar{\mathbb{F}}_p$. Somit ist $[\mathbb{F}_p(\alpha):\mathbb{F}_p]=\deg(f)$ und $\mathbb{F}_p(\alpha)\subseteq\mathbb{F}_{p^m}$ wegen der obigen Ausführungen. Damit ist aber bereits wegen $[\mathbb{F}_{p^m}:\mathbb{F}_p]=m<\deg(f)$ ein Widerspruch gefunden. Also ist nur $\mathrm{ggT}(f,X^{p^m}-X)=1$ möglich für $1\leq m\leq\deg(f)/2$ □

**Aufgabe 225** Gegeben sei $f=x^{16}-x\in\mathbb{F}_2[x]$.
(a) Es ist $\mathbb{F}_{16=2^4}$ der Zerfällungskörper von $f$. Die Körpererweiterung $\mathbb{F}_{16}|\mathbb{F}_2$ hat den Zwischenkörper $\mathbb{F}_{4=2^2}$. Es ist $|\mathbb{F}_2|=2$, $|\mathbb{F}_4\setminus\mathbb{F}_2|=2$ und $[\mathbb{F}_4:\mathbb{F}_2]=2$ sowie $|\mathbb{F}_{16}\setminus\mathbb{F}_4|=12$ und $[\mathbb{F}_{16}:\mathbb{F}_2]=4$. Damit hat $f$ genau zwei irreduzible Faktoren

vom Grad 1, genau $2/2 = 1$ irreduziblen Faktor vom Grad 2 und genau $12/4 = 3$ irreduzible Faktoren vom Grad 4.
(b) Es ist $\mathbb{F}_{16=4^2}$ der Zerfällungskörper von $f$ und $[\mathbb{F}_{16} : \mathbb{F}_4] = 2$ sowie $|\mathbb{F}_{16} \setminus \mathbb{F}_4| = 12$. Somit erlaubt $f$ einer Zerlegung in 4 irreduzible Faktoren vom Grad 1 und in $6 = 12/2$ irreduzible Faktoren vom Grad 2 über $\mathbb{F}_4$. □

**Aufgabe 226 (H17T2A3)** Sei $p$ eine Primzahl und $k \in \mathbb{N}$ sowie $q = p^k$ und $f = x^7 + x + 1 \in \mathbb{F}_2[x]$ sowie $g = x^7 - x - 1 \in \mathbb{Q}[x]$.
(a) Da $f(0) = 1 \neq 0$ und $f(1) = 1^7 + 1 + 1 = 1 \neq 0$ jeweils in $\mathbb{F}_2$ gilt, hat $f$ keine Nullstellen in $\mathbb{F}_2$. In $\mathbb{F}_4$ sind nur potentiell Einheiten aus $\mathbb{F}_4^\times$ Nullstellen von $f$, denn wir haben bereits vorher ausgeschlossen, dass 0 eine Nullstelle von $f$ ist. Andererseits hat die Einheitengruppe $\mathbb{F}_4^\times$ gerade Ordnung 3, sodass für $\alpha \in \mathbb{F}_4^\times$ gilt $\alpha^3 = 1$. Somit $f(\alpha) = \alpha^7 + \alpha + 1 = \alpha + \alpha + 1 = 1 \neq 0$, denn $\mathrm{char}(\mathbb{F}_4) = 2$. Somit ist $f(\alpha) = 1 \neq 0$ für alle $\alpha \in \mathbb{F}_4^\times$ und wegen $f(0) = 1 \neq 0$ hat $f$ somit insgesamt keine Nullstellen in $\mathbb{F}_4$. Analog hat die Einheitengruppe $\mathbb{F}_8^\times$ die Ordnung 7, also ist $\alpha^7 = 1$ für alle $\alpha \in \mathbb{F}_8^\times$. So wie oben stellen wir fest, dass $f(0) = 1 \neq 0$ in $\mathbb{F}_8$ und zudem gilt $f(\alpha) = \alpha^7 + \alpha + 1 = 1 + \alpha + 1 = \alpha \neq 0$, denn $\alpha \in \mathbb{F}_8^\times = \mathbb{F}_8 \setminus \{0\}$. Also hat $f$ auch keine Nullstellen in $\mathbb{F}_8$.
(b) Angenommen, $f$ wäre reduzibel in $\mathbb{F}_2[x]$. Als Polynom vom Grad 7 hat $f$ somit mindestens einen normierten und irreduziblen Faktor $g$ vom Grad $\leq 3$. Da $g$ normiert und irreduzibel ist, ist $g$ das Minimalpolynom eines $\alpha \in \mathbb{F}_2^{\mathrm{alg}}$. Somit ist $[\mathbb{F}_2(\alpha) : \mathbb{F}_2] = \deg(g) \leq 3$ und wegen der Eindeutigkeit endlicher Körper $\mathbb{F}_2(\alpha) = \mathbb{F}_{2^{\deg(g)}} \in \{\mathbb{F}_2, \mathbb{F}_4, \mathbb{F}_8\}$. In jedem Fall hat dann $f$ eine Nullstelle in einer der Körper $\mathbb{F}_2, \mathbb{F}_4, \mathbb{F}_8$. Das ist aber ausgeschlossen, nach Teil (a). Somit war die Annahme, $f$ wäre reduzibel über $\mathbb{F}_2$ falsch und $f$ ist irreduzibel in $\mathbb{F}_2[x]$ als Nicht-Einheit.
(c) Da $\mathbb{Q}$ der Quotientenkörper von $\mathbb{Z}$ ist, und $g \in \mathbb{Z}[x]$ als normiertes Polynom primitiv ist, reicht es nach dem Lemma von Gauss aus, zu zeigen, dass $g$ in $\mathbb{Z}[x]$ irreduzibel ist. Da $f$ gerade das Bild von $g$ unter der Reduktionsabbildung modulo 2 ist, liefert uns das Reduktionskriterium wegen der Irreduzibilität von $f$ über $\mathbb{F}_2$ die Irreduzibilität von $g$ über $\mathbb{Z}$. Mit dem Lemma von Gauss schließt man wie beschrieben auf die Irreduzibilität von $g$ in $\mathbb{Q}[x]$. □

**Aufgabe 227** Gegeben sei $f = x^{64} - x \in \mathbb{F}_2[x]$.
(a) Es ist $64 = 2^6$ und $\mathbb{F}_{64}$ ist demnach der Zerfällungskörper von $f$. Die Körpererweiterung $\mathbb{F}_{64}|\mathbb{F}_2$ hat die beiden echten Zwischenkörper $\mathbb{F}_4$ und $\mathbb{F}_8$, die jeweils Erweiterungsgrad 2 bzw. 3 über $\mathbb{F}_2$ haben. Da zudem $\mathbb{F}_4 \cap \mathbb{F}_8 = \mathbb{F}_2$ hat $x^{64} - x$ in einem algebraischen Abschluss von $\mathbb{F}_2$ genau 64 Nullstellen, von denen 2 in $\mathbb{F}_2$ liegen, $4 - 2 = 2$ in $\mathbb{F}_4$, $8 - 2 = 6$ in $\mathbb{F}_8$ und $64 - 6 - 2 - 2 = 54$ in $\mathbb{F}_{64}$. Zusammen mit den vorher gefundenen Erweiterungsgraden und $[\mathbb{F}_{64} : \mathbb{F}_2] = 6$ finden wir, dass $f$ zwei irreduzible Faktoren vom Grad 1 hat, 1 irreduziblen Faktoren vom Grad 2, 2 irreduzible Faktoren vom Grad 3 und 9 irreduzible Faktoren vom Grad 6, wobei irreduzibel als irreduzibel über $\mathbb{F}_2$ zu verstehen ist.
(b) Es ist $64 = 4^3$ und $x^{64} - x = x^{4^3} - x$ zerfällt demnach in $\mathbb{F}_{64}$ in Linearfaktoren. Zudem hat $f$ vier Nullstellen bereits in $\mathbb{F}_4$ und wegen $[\mathbb{F}_{64} : \mathbb{F}_4] = 3$ gibt es $(64 - 4)/3 = 20$ verschiedene, über $\mathbb{F}_4$ irreduzible Faktoren vom Grad 3 in der

Faktorzerlegung von $f$ über $\mathbb{F}_4$. Insgesamt lässt sich als $f$ also in $\mathbb{F}_4[x]$ als Produkt von 4 irreduziblen Faktoren vom Grad 1 und 20 irreduziblen Faktoren vom Grad 3 darstellen.
(c) Es ist $64 = 8^2$ und $x^{64} - x = x^{8^2} - x = f$ kann als Polynom in $\mathbb{F}_8[x]$ aufgefasst werden. Zudem ist $f$ der Zerfällungskörper von $f$ wiederum $\mathbb{F}_{64=8^2}$. Alle 8 Elemente von $\mathbb{F}_8$ sind Nullstellen von $f$, sodass $f$ bereits 8 irreduzible Faktoren vom Grad 1 in $\mathbb{F}_8[x]$ hat. Da $[\mathbb{F}_{64} : \mathbb{F}_8] = 2$ und $|\mathbb{F}_{64} \setminus \mathbb{F}_8| = 56$ liegen die übrigen 56 Nullstellen von $f$ in $\mathbb{F}_{64} \setminus \mathbb{F}_8$. Jeweils zwei dieser Nullstellen haben dasselbe Minimalpolynom über $\mathbb{F}_8$, und wegen $[\mathbb{F}_{64} : \mathbb{F}_8] = 2$ hat dieses jeweils den Grad 2. Somit lässt sich $f$ als Produkt von 8 irreduziblen Faktoren vom Grad 1 und 28 irreduziblen Faktoren vom Grad 2 darstellen, wobei irreduzibel hier als irreduzibel in $\mathbb{F}_8[x]$ zu verstehen ist.
(d) Zunächst ist $\mathbb{F}_{32}|\mathbb{F}_2$ einer Körpererweiterung vom Grad 5 also von Primzahlordnung. Somit hat $\mathbb{F}_{32}|\mathbb{F}_2$ keine echten Zwischenkörper. Da $f$ gerade den Zerfällungskörper $\mathbb{F}_{64}$ hat, der über $\mathbb{F}_2$ den Erweiterungsgrad 6 hat, kann keine Nullstelle von $f$ in $\mathbb{F}_{32} \setminus \mathbb{F}_2$ liegen. Andernfalls wäre für eine solche Nullstelle $\mathbb{F}_2(\alpha) = \mathbb{F}_{32}$ und $\mathbb{F}_{32}$ ein Zwischenkörper von $\mathbb{F}_{64}|\mathbb{F}_2$, da alle Nullstellen von $f$ auf jeden Fall in $\mathbb{F}_{64}$ liegen. Aber wegen $5 \not| 6$ ist ausgeschlossen, dass $\mathbb{F}_{32}$ ein Zwischenkörper von $\mathbb{F}_{64}|\mathbb{F}_2$ ist. Nullstellen von $f$, die in $\mathbb{F}_4, \mathbb{F}_8$, aber nicht in $\mathbb{F}_2$ liegen können ebenfalls nicht in $\mathbb{F}_{32}$ liegen, denn $\mathbb{F}_{32}|\mathbb{F}_2$ hat als Körpererweiterung eines endlichen Körpers mit Erweiterungsgrad von Primzahlordnung keine echten Zwischenkörper. Da die restlichen Nullstellen von $f$ bereits in $\mathbb{F}_{64} \setminus (\mathbb{F}_8 \cup \mathbb{F}_4)$ liegen und $\mathbb{F}_{32}$ kein Zwischenkörper von $\mathbb{F}_{64}|\mathbb{F}_2$ ist, haben wir insgesamt gezeigt, dass die Zerlegungen von $f$ in irreduzible Faktoren in $\mathbb{F}_2[x]$ und $\mathbb{F}_{32}[x]$ übereinstimmen. Damit hat $f$, aufgefasst als Polynom aus $\mathbb{F}_{32}[x]$, eine Zerlegung in, in $\mathbb{F}_{32}[x]$ irreduzible, Faktoren, von denen 2 vom Grad 1, 1 vom Grad 2, 2 vom Grad 3 und 9 vom Grad 6 sind.
(e) Da $\mathbb{F}_{64}$ der Zerfällungskörper von $f$ ist, zerfällt $f$ über $\mathbb{F}_{64}$ in 64 irreduzible Faktoren vom Grad 1. □

**Aufgabe 228 (H13T2A1)** Gegeben ist das Polynom $f = x^4 + x + 1 \in \mathbb{F}_2[x]$.
(a) Wir zeigen, dass $f$ über $\mathbb{F}_2$ irreduzibel ist. Dazu bemerken wir, dass $f(0) = 1 \neq 0$ und $f(1) = 1 \neq 0$, also $f$ keine Nullstellen in $\mathbb{F}_2$ hat. Als Polynom vom Grad 4 ist $f$ demzufolge nur noch dann reduzibel, wenn es sich als Produkt zweier in $\mathbb{F}_2[x]$ irreduzibler Faktoren vom Grad 2 schreiben lässt. Das einzige, über $\mathbb{F}_2$ irreduzible Polynom vom Grad 2 ist $g = x^2 + x + 1$. Aber es gilt $(x^2 + x + 1)^2 = x^4 + x^2 + 1 \neq x^4 + x + 1 = f$. Damit ist $f$ bereits in $\mathbb{F}_2[x]$ irreduzibel.
(b) Es ist $\alpha \in \mathbb{F}_2^{\text{alg}}$ eine Nullstelle von $f$. Da $\alpha$ normiert und irreduzibel ist, ist $f$ das Minimalpolynom von $\alpha$. Wegen $\deg(f) = 4$ ist $[\mathbb{F}_2(\alpha) : \mathbb{F}_2] = 4$ und somit $\mathbb{F}_2(\alpha) = \mathbb{F}_{16}$ wegen der Eindeutigkeit endlicher Körper. Da $f$ als über $\mathbb{F}_2$ irreduzibles Polynom insbesondere nicht die Nullstelle 0 hat und $\mathbb{F}_{16}^\times = \mathbb{F}_{16} \setminus \{0\}$ wegen der Körperaxiome, ist $\alpha \in \mathbb{F}_{16}^\times$. Es gilt somit $\alpha^{15} = 1$. Bekanntlich ist die Einheitengruppe endlicher Körper zyklisch, und in diesem Fall ist die Einheitengruppe $\mathbb{F}_{16}^\times$ sogar zyklisch von Ordnung 15. Da $\alpha^{15} = 1$, ist $\text{ord}(\alpha)$ ein Teiler von 15. Der Fall, dass $\text{ord}(\alpha) = 1$, scheidet dabei aus, denn sonst wäre $\alpha = 1$, also hätte $f$ eine Nullstelle in $\mathbb{F}_2$. Das widerspricht aber der Irreduzibilität von $f$ in $\mathbb{F}_2[x]$. Wenn $\alpha$ die Ordnung 3 hätte, wäre $\alpha$ Nullstelle des Polynoms $g_1 = x^3 - 1$, was aber der Minimalität des Grads

von $f$ als Minimalpolynom von $\alpha$ widerspricht. Wäre $\alpha$ von Ordnung 5, so $g_2 = x^5 - 1 = (x-1)(x^4+x^3+x^2+x+1)$ ein Polynom, das $\alpha$ als Nullstelle hat. Da aber $\alpha \neq 1$, ist $\alpha$ dann Nullstelle von $g_3 = x^4+x^3+x^2+x+1$. Da nun $\alpha$ Nullstelle von $g_3$ und $f$ ist, ist auch $g_3 - f = x^3 + x^2$ ein Polynom aus $\mathbb{F}_2[x]$, das $\alpha$ als Nullstelle hat. Insbesondere müsste dann der Grad des Minimalpolynoms von $\alpha$ über $\mathbb{F}_2 \leq 3$ sein, was aber $\deg(f) = 4$ und der Eigenschaft von $f$, Minimalpolynom von $\alpha$ zu sein, widerspricht. Damit ist nur noch $\mathrm{ord}(\alpha) = 15$ möglich, sodass $\mathbb{F}_{16}^\times = \langle\alpha\rangle$. □

**Aufgabe 229 (H13T2A4)** Sei $K$ ein endlicher Körper und $a \in K$. Wir zeigen, dass es Elemente $x, y \in K$ gibt, sodass $a = x^2 + y^2$. Sei $Q$ die Menge der Quadrate in $K$. Da $0^2 = 0$ ist $Q = (K^\times)^2 \cup \{0\}$. Die Abbildung $\phi : K^\times \to (K^\times)^2, x \mapsto x^2$ ist ein surjektiver Homomorphismus von Gruppen laut Vorlesung. Falls $\mathrm{char}(K) = 2$, dann ist $\ker(\phi) = \{1\}$, denn $X^2 - 1 = (X-1)^2$ in $K$. In diesem Fall ist also $|Q| \geq |K^\times|/2 + 1 = (q+1)/2$. Falls $\mathrm{char}(K) > 2$, dann ist $\ker\phi = \{\pm 1\}$ und $X^2 - 1$ hat als Polynom vom Grad 2 auch keine weiteren Nullstellen. In diesem Fall ist also $|Q| \geq (|K^\times| - 1)/|\ker\phi| + 1 = (q+1)/2$. In jedem Fall ist $|Q| \geq (q+1)/2$. Wir definieren nun $N = \{a - x^2 | x^2 \in Q\}$. Offenbar ist durch $\phi : Q \to N, x^2 \mapsto a - x^2$ eine Bijektion gegeben, denn $\psi : N \to Q, z \mapsto a - z$ ist die Umkehrabbildung: Für alle $z \in Q$ gilt $\psi(\phi(z)) = a - (a - z) = z$ und für alle $z \in N$ gilt $\phi(\psi(z)) = a - (a - z) = z$. Da $\phi$ eine Bijektion zwischen $Q$ und $N$ definiert, sind $|Q| = |N|$. Angenommen, $Q \cap N = \emptyset$. Dann ist $K \supseteq Q \cup N$ und $|K| = q \geq |Q| + |N| = 2|Q| \geq q + 1$. Das ist ein Widerspruch! Somit gibt es ein $c \in N \cap Q$, d.h., es existiert ein $y \in K$, sodass $y^2 = a - x^2$ bzw. $a = x^2 + y^2$, wie behauptet. □

**Aufgabe 230 (F17T3A5)** Sei $K$ ein endlicher Körper mit $q$ Elementen. Wir zeigen, dass $f = x^2 + x + 1 \in K[x]$ genau dann irreduzibel ist, wenn $q \equiv -1 \bmod(3)$. Wir wenden Kontraposition an. Ist $q \not\equiv -1 \bmod(3)$, dann ist entweder $q \equiv 0 \bmod(3)$ oder $q \equiv 1 \bmod(3)$. Im ersten Fall ist $\mathbb{F}_3 \subseteq K$ als Primkörper und es gilt $f(1) = 1^2 + 1 + 1 = 0$, sodass $f$ als Polynom vom Grad 2 mit einer Nullstelle in $K$ bereits reduzibel ist. Im zweiten Fall ist $q = 3k + 1$ mit $k \in \mathbb{N}$. Insbesondere ist dann $K^\times$ eine zyklische Gruppe mit einer durch 3 teilbaren, endlichen Ordnung $3k$ und Erzeuger $\alpha \in K^\times$. Es ist dann $(\alpha^k)^3 - 1 = 0$, also $\alpha^k$ ein Element der Ordnung 3 in $K^\times$. Nun ist $g(x) = x^3 - 1 = (x-1)f(x)$ ein Polynom in $K[x]$ und es gilt $f(\alpha^k) = 0$, denn sonst wäre $\alpha^k - 1 = 0$, d.h., es hätte $\alpha$ die Ordnung $k$ statt $3k$. Somit hat $f$ auch im zweiten Fall eine Nullstelle in $K$ und ist als Polynom vom Grad 2 damit reduzibel. Ist umgekehrt $f \in K[x]$ reduzibel, dann hat $f$ als Polynom vom Grad 2 eine Nullstelle. Es ist also $f(x) = (x - \alpha)(x - \beta)$ mit $\alpha, \beta \in K$. Falls $\alpha = 1$, dann gilt $f(1) = 3 \cdot 1 = 0$ und es ist $\mathrm{char}(K) = 3$, sodass $q \equiv 0 \bmod(3)$. Falls $\alpha \neq 1$, dann hat $\alpha$ als Element von $K^\times$ die Ordnung 3, denn es ist $(\alpha - 1)f(\alpha) = 0$ und $(\alpha - 1)f(\alpha) = \alpha^3 - 1$ also $\alpha^3 = 1$. Da $|K^\times| = q - 1$ und $K^\times$ zyklisch ist, gilt auf jeden Fall $3|(q-1)$, da es sonst kein Element der Ordnung 3 in $K^\times$ gäbe. Die Teilbarkeitsrelation von gerade eben lautet als Kongruenz dann $q \equiv 1 \bmod(3)$. Zusammen genommen impliziert die Reduzibilität von $f$ also $q \not\equiv -1 \bmod(3)$. Mit der am Anfang des Beweises angesprochenen Kontraposition haben wir also die Gültigkeit der zu beweisenden Aussage nachgewiesen. □

**Aufgabe 231 (H15T1A1(a,b,c))** Sei $\zeta_5$ eine primitive fünfte und $\zeta_7$ eine primitive siebte Einheitswurzel. Ferner, $u := \zeta_7 + \zeta_7^{-1}$.
(a) Wir zeigen, dass $[\mathbb{Q}(\zeta_7) : \mathbb{Q}(u)] = 2$. Zunächst stellen wir fest, dass $|\zeta_7| = 1$, sodass $\zeta_7^{-1} = \bar{\zeta_7}$, wobei der Überstrich die Komplexe Konjugation, $\bar{\cdot} : \mathbb{C} \to \mathbb{C}, z \mapsto \bar{z}$ anzeigt. Offenbar ist $u \in \mathbb{Q}(\zeta_7)$, sodass $\mathbb{Q}(\zeta_7)|\mathbb{Q}(u)$ eine Körpererweiterung ist. Ferner ist $u = \zeta_7 + \bar{\zeta_7} = 2\Re[\zeta_7] \in \mathbb{R}$. Zudem stellen wir fest, dass $f = x^2 - ux + 1 = x^2 - (\zeta_7 + \bar{\zeta_7})x + \zeta_7\bar{\zeta_7} = (x - \zeta_7)(x - \bar{\zeta_7}) \in \mathbb{Q}(u)[x]$ ein normiertes Polynom ist, das $\zeta_7$ als Nullstelle hat. Folglich hat das Minimalpolynom $\mu_{\mathbb{Q}(u),\zeta_7}$ einen Grad $\leq 2$ und es gilt $\mu_{\mathbb{Q}(u),\zeta_7}|f$. Bekanntlich ist $[\mathbb{Q}(\zeta_7) : \mathbb{Q}] = \deg(\Phi_7) = \phi(7) = 6$, sodass $\langle\zeta_7\rangle \leq \mathbb{C}^\times$ zyklisch von Ordnung 6 ist. Da $\{\pm 1\}$ die einzigen (siebten) Einheitswurzeln sind, deren Imaginärteil verschwindet, deren Ordnung aber $\leq 2$ ist, ist $\Im[\zeta_7] \neq 0$. Damit ist $\zeta_7 \notin \mathbb{R} \supseteq \mathbb{Q}(u)$. Als Polynom vom Grad 2 ist $f$ damit wegen Nullstellenfreiheit in $\mathbb{Q}(u)$ bereits über $\mathbb{Q}(u)$ irreduzibel. Da $f$ normiert und irreduzibel ist sowie $\zeta_7$ als Nullstelle hat, gilt $\mu_{\mathbb{Q}(u),\zeta_7} = f$. Damit ist $[\mathbb{Q}(\zeta_7) : \mathbb{Q}(u)] = \deg(\mu_{\mathbb{Q}(u),\zeta_7}) = 2$, wie behauptet.
(b) Wir zeigen $[\mathbb{Q}(u) : \mathbb{Q}] = 3$. Zunächst gilt $[\mathbb{Q}(\zeta_7) : \mathbb{Q}] = \phi(7) = 6$, da $\zeta_7$ als primitive siebte Einheitswurzel vorausgesetzt war und als solche das siebte Kreisteilungspolynom $\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ als Minimalpolynom über $\mathbb{Q}$ hat. In Teil (a) wurde bereits $u \in \mathbb{Q}(\zeta_7)$ festgestellt. Zudem ist $\mathbb{Q}(u)$ ein Zwischenkörper der (endlichen) Körpererweiterung $\mathbb{Q}(\zeta_7)|\mathbb{Q}$. Die Gradformel liefert nun $6 = [\mathbb{Q}(\zeta_7) : \mathbb{Q}] = [\mathbb{Q}(\zeta_7) : \mathbb{Q}(u)][\mathbb{Q}(u) : \mathbb{Q}] = 2 \cdot [\mathbb{Q}(u) : \mathbb{Q}]$, wobei das in Teil (a) bewiesene Resultat bemüht wurde. Die Gleichung liefert nach Auflösen $[\mathbb{Q}(u) : \mathbb{Q}] = 3$, wie behauptet.
(c) Wir zeigen $[\mathbb{Q}(u, \zeta_5) : \mathbb{Q}] = 12$. Bekanntlich ist $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$ das fünfte Kreisteilungspolynom und irreduzibel in $\mathbb{Q}[x]$. Insbesondere ist $\Phi_5(\zeta_5) = 0$ und wegen zusätzlicher Normiertheit insgesamt das Minimalpolynom von $\zeta_5$ über $\mathbb{Q}$. Also gilt $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = \deg(\Phi_5) = 4$. Aus Aufgabenteil (b) ist ferner $[\mathbb{Q}(u) : \mathbb{Q}] = 3$ bekannt. Da $\mathbb{Q}(\zeta_5), \mathbb{Q}(u)$ jeweils Zwischenkörper der endlichen Erweiterung $\mathbb{Q}(u, \zeta_5)|\mathbb{Q}$ (da von endlich vielen algebraischen Elementen erzeugt) sind, folgt $[\mathbb{Q}(u) : \mathbb{Q}] = 3|[\mathbb{Q}(u, \zeta_5)]$ und $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 4|[\mathbb{Q}(u, \zeta_5) : \mathbb{Q}]$. Zusammen ergibt sich also $12 = \mathrm{kgV}(3, 4)|[\mathbb{Q}(u, \zeta_5) : \mathbb{Q}]$. Andererseits gilt für das Minimalpolynom von $\zeta_5$ über $\mathbb{Q}(u)$, dass $\deg(\mu_{\mathbb{Q}(u),\zeta_5}) \leq \deg(\Phi_5) = 4$, da auch $\Phi_5 \in \mathbb{Q}(u)[x]$ gilt und zumindest $\Phi_5(\zeta_5) = 0$. Mittels Gradformel erhalten wir also $[\mathbb{Q}(u, \zeta_5) : \mathbb{Q}] = [\mathbb{Q}(u)(\zeta_5) : \mathbb{Q}(u)][\mathbb{Q}(u) : \mathbb{Q}] \geq 4 \cdot 3 = 12$, wobei wiederum das Ergebnis aus Teil (b) bemüht wurde. Zusammen mit $12|[\mathbb{Q}(u, \zeta_5) : \mathbb{Q}]$, also insbesondere $[\mathbb{Q}(u, \zeta_5) : \mathbb{Q}] \geq 12$, ergibt sich die gewünschte Gleichheit $[\mathbb{Q}(u, \zeta_5) : \mathbb{Q}] = 12$. □

**Aufgabe 232 (F16T1A5)** (a) Gesucht ist das Minimalpolynom von $\alpha = \sqrt{(\sqrt{5}+5)/8}$ über $\mathbb{Q}$. Zunächst gilt

$$\begin{aligned} \alpha &= \sqrt{\frac{\sqrt{5}+5}{8}} \\ \Rightarrow \alpha^2 &= \frac{\sqrt{5}+5}{8} \\ \Rightarrow \left(\alpha^2 - \frac{5}{8}\right)^2 &= \frac{5}{64} \\ \Rightarrow \alpha^4 - \frac{10}{64}\alpha^2 + \frac{20}{64} &= 0. \end{aligned}$$

Damit ist $\alpha$ Nullstelle des normierten Polynoms $f = x^4 - 10/64x^2 + 20/64 \in \mathbb{Q}[x]$. Es verbleibt der Nachweis der Irreduzibilität über $\mathbb{Q}$. Da 32 eine Einheit in $\mathbb{Q}$ ist, reicht es, nachzuweisen, dass $g = 32f = 32x^4 - 5x^2 + 10 \in \mathbb{Z}[x]$ irreduzibel ist. Wegen $1 = \mathrm{ggT}(32, -5, 10)$, handelt es sich bei $g$ um ein primitives Polynom. Ferner ist $5|-5$ und $5|10$ sowie $5 \not| 32$ und $5^2 \not| 10$. Mithin liefert das Eisensteinkriterium zur Primzahl $p = 5$ die Irreduzibilität von $g$ über $\mathbb{Z}$. Da $g$ primitiv ist, liefert das Lemma von Gauss die Irreduzibilität von $g$ über $\mathbb{Q} = \mathrm{Quot}(\mathbb{Z})$. Zusammen mit dem eingangs Gesagten folgt, dass $f$ irreduzibel über $\mathbb{Q}$ ist. Da $f$ normiert und irreduzibel ist und ferner $\alpha$ als Nullstelle besitzt, handelt es sich bei $f$ um das Minimalpolynom von $\alpha$ über $\mathbb{Q}$.
(b) Wir zeigen, dass $i \notin \mathbb{Q}(\zeta_5)$. Da $\zeta_5$ eine primitive 5-te Einheitswurzel ist, gilt $|\zeta_5|^2 = 1$. Zudem ist $\bar{\zeta_5} = \zeta_5^{-1} \in \mathbb{Q}(\zeta_5)$. Damit ist auch $-i/2(\zeta_5 - \bar{\zeta_5}) = \alpha \in \mathbb{Q}(\zeta_5)$, wenn wir annehmen, dass $i \in \mathbb{Q}(\zeta_5)$. Somit ist $\mathbb{Q}(\alpha)$ ein Zwischenkörper der Erweiterung $\mathbb{Q}(\zeta_5)|\mathbb{Q}$. Es gilt $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = \phi(5) = 4$ für den fünften Kreisteilungskörper. Da $\mu_{\mathbb{Q},\alpha}$ vom Grad 4 nach Teil (a) ist, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Wegen $\alpha \in \mathbb{R}$ gilt aber $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$, wohingegen $\zeta_5 \notin \mathbb{R}$, da $\Im[\zeta_5] = \alpha \neq 0$ laut Angabe. Also ist einerseits aus Gradgründen und wegen $\alpha \in \mathbb{Q}(\zeta_5)$ $\mathbb{Q}(\alpha) = \mathbb{Q}(\zeta_5)$, andererseits $\zeta_5 \notin \mathbb{Q}(\alpha)$. Der Widerspruch zeigt, dass $i \in \mathbb{Q}(\zeta_5)$ falsch war, also $i \notin \mathbb{Q}(\zeta_5)$. □

**Aufgabe 233 (F13T3A5)** Es sei $\zeta_n = \exp(2\pi i/n)$ für $n \in \mathbb{N}$ eine primitive $n$-te Einheitswurzel und $k_n := \mathrm{kgV}(1, 2, \cdots, n)$.
(a) Wir zeigen $[\mathbb{Q}(\zeta_1, ..., \zeta_n) : \mathbb{Q}] = \phi(k_n)$. Um dies zu sehen, beweisen wir, dass $\mathbb{Q}(\zeta_1, ..., \zeta_n) = \mathbb{Q}(\zeta_{k_n})$. Da $k_n$ das kleinste gemeinsame Vielfache der Zahlen $1, ..., n$ ist, gibt es zu einem beliebigen $m \in \{1, ..., n\}$ ein $d_m \in \mathbb{N}$, sodass $m \cdot d_m = k_n$. Somit können wir $1/m = d_m/k_n$ schreiben und erhalten $\zeta_{k_n}^{d_m} = \exp(2\pi i d_m/k_n) = \exp(2\pi i/m) = \zeta_m$. Diese Rechnung zeigt, dass $\zeta_m \in \mathbb{Q}(k_n)$ für beliebiges $m \in \{1, ..., n\}$. Laut Vorlesung gilt also bereits $\mathbb{Q}(\zeta_1, ..., \zeta_n) \subseteq \mathbb{Q}(\zeta_{k_n})$. Um zu sehen, dass auch $\zeta_{k_n} \in \mathbb{Q}(\zeta_1, ..., \zeta_n)$ versuchen wir, $c_1, ..., c_n \in \mathbb{N}_0$ dergestalt zu finden, dass $\zeta_{k_n} = \prod_{l=1}^n \zeta_l^{c_l}$. Somit benötigen wir Zahlen $c_1, ..., c_n \in \mathbb{Z}$ dergestalt, dass $1/k_n = \sum_{l=1}^n c_l/l$. Indem wir $d_l := k_n/l \in \mathbb{Z}$ für $l \in \{1, 2, ..., n\}$ definieren, haben wir $1 = \sum_{l=1}^n c_l d_l$. Zu zeigen ist also, dass $\mathrm{ggT}(d_1, d_2, ..., d_n) = 1$. Mit dem Lemma von Bezout folgt dann die Existenz der $c_l$'s. Angenommen, $\mathrm{ggT}(d_1, ..., d_n) = k > 1$. Dann gibt es ein $q_l \in \mathbb{Z}$, sodass $q_l k = d_l$ für $1 \leq l \leq n$. Somit ist $q_l l k = k_n$

und $k_n' := k_n/k < k_n$ wegen $k > 1$ unabhängig von $l \in \{1, 2, ..., n\}$. Damit haben wir einen Widerspruch dazu, dass $k_n$ das kleinste gemeinsame Vielfache von $1, 2, ..., n$ ist. Somit ist $\mathrm{ggT}(d_1, d_2, ..., d_n) = 1$ wie behauptet und die Existenz der $c_l$ wie beschrieben folgt aus dem Lemma von Bezout. Mit diesen $c_l$ finden wir also $\prod_{l=1}^n \zeta_l^{c_l} = \prod_{l=1}^n \exp(2\pi i c_l/l) = \exp(2\pi i \sum_{l=1}^n c_l/l) = \exp(2\pi i/k_n) = \zeta_{k_n}$ wie behauptet. Somit ist $\zeta_{k_n} \in \mathbb{Q}(\zeta_1, ..., \zeta_n)$ und mit dem oben referenzierten Vorlesungsresultat folgt $\mathbb{Q}(\zeta_{k_n}) \subseteq \mathbb{Q}(\zeta_1, ..., \zeta_n)$. Insgesamt haben wir also die behauptete Gleichheit nachgewiesen. Als $k_n$-ter Kreisteilungskörper hat $\mathbb{Q}(\zeta_{k_n})$ den Erweiterungsgrad $[\mathbb{Q}(\zeta_{k_n}) : \mathbb{Q}] = \phi(k_n)$. Mithin ist auch $[\mathbb{Q}(\zeta_1, ...\zeta_n) : \mathbb{Q}] = k_n$.
(b) Wir zeigen $[\mathbb{Q}(\sqrt[1]{2}, ..., \sqrt[n]{2}) : \mathbb{Q}] = k_n$. Zu diesem Zwecke zeigen wir, dass $\mathbb{Q}(\sqrt[1]{2}, ..., \sqrt[n]{2}) = \mathbb{Q}(\sqrt[k_n]{2})$. Sei $m \in \{1, ..., n\}$ beliebig. Dann gibt es ein $d_m \in \mathbb{N}$, sodass $d_m m = k_n$, da $k_n$ das kleinste gemeinsame Vielfache der Zahlen $1, 2, 3, ..., n$ ist. Dann gilt $\sqrt[m]{2} = \sqrt[k_n]{2}^{d_m}$, sodass $\sqrt[m]{2} \in \mathbb{Q}(\sqrt[k_n]{2})$. Beliebigkeit von $m \in \{1, 2, ..., n\}$ impliziert $\{\sqrt[1]{2}, \sqrt[2]{2}, ..., \sqrt[m]{2}\} \subseteq \mathbb{Q}(\sqrt[k_n]{2})$. Umgekehrt haben wir bereits in Teil (a) gesehen, dass es $c_1, c_2, ..., c_n \in \mathbb{Z}$ gibt, sodass $1/k_n = \sum_{l=1}^n c_l/l$. Damit gilt auch

$$\sqrt[k_n]{2} = 2^{\frac{1}{k_n}} = 2^{\sum_{l=1}^n \frac{c_l}{l}} = \prod_{l=1}^n 2^{\frac{c_l}{l}} = \prod_{l=1}^n \sqrt[l]{2}^{c_l}. \tag{262}$$

Damit ist dann insbesondere $\sqrt[k_n]{2} \in \mathbb{Q}(\sqrt[1]{2}, ..., \sqrt[n]{2})$. Mit der bereits vorher etablierten Inklusion folgt $\mathbb{Q}(\sqrt[k_n]{2}) = \mathbb{Q}(\sqrt[1]{2}, ...., \sqrt[n]{2})$. Wir zeigen nun, dass $[\mathbb{Q}(\sqrt[k_n]{2}) : \mathbb{Q}] = k_n$ und damit folgt dann $[\mathbb{Q}(\sqrt[1]{2}, ..., \sqrt[n]{2})] = k_n$. Es ist $f = x^{k_n} - 2 \in \mathbb{Q}[x]$ ein normiertes und ganzzahliges, damit primitives, Polynom aus $\mathbb{Q}[x]$, das $\sqrt[k_n]{2}$ offensichtlich als Nullstelle besitzt. Wegen des Eisensteinkriteriums zur Primzahl $p = 2$ in Verbindung mit dem Lemma von Gauss ist $f$ überdies irreduzibel in $\mathbb{Q}[x]$. Damit handelt es sich bei $f$ bereits um das Minimalpolynom von $\sqrt[k_n]{2}$ über $\mathbb{Q}$. Somit ist $[\mathbb{Q}(\sqrt[k_n]{2}) : \mathbb{Q}] = \deg(\mu_{\mathbb{Q}, \sqrt[k_n]{2}}) = \deg(f) = k_n$ und, wie vorher erläutert, folgt die Behauptung, dass $[\mathbb{Q}(\sqrt[1]{2}, ..., \sqrt[n]{2}) : \mathbb{Q}] = k_n$. □

**Aufgabe 234 (H18T3A3(a,b))** Gegeben sei ein irreduzibles Polynom $f \in \mathbb{Q}[x]$ vom Grad 5 mit Galoisgruppe $\mathrm{Gal}(f) \simeq S_5$ und es sei $L$ ein Zerfällungskörper von $f$.
(a) Wir zeigen, dass $[L : \mathbb{Q}] = 120$. Sei $L$ ein Zerfällungskörper von $f$. Da $f$ ein Polynom ist, ist $L|K$ endlich, insbesondere also algebraisch. Da $\mathrm{char}(\mathbb{Q}) = 0$ ist $L|\mathbb{Q}$ separabel. Da $L$ zudem Zerfällungskörper von $f$ ist, handelt es sich bei $L|\mathbb{Q}$ um eine normale Erweiterung. Als normale und separable Erweiterung ist $L|\mathbb{Q}$ galoissch. Es ist $[L : \mathbb{Q}] = |\mathrm{Gal}(L|\mathbb{Q})| = |\mathrm{Gal}(f)| = |S_5| = 120$, denn $\mathrm{Gal}(f) = \mathrm{Gal}(L|\mathbb{Q})$ definitionsgemäß.
(b) Da $f$ irreduzibel ist und normiert ist, ist $f$ Minimalpolynom einer seiner Nullstellen, ohne Einschränkung $x_1 \in L \setminus \mathbb{Q}$ und letzteres wegen $\deg(f) = 5 > 1$. Da $L|\mathbb{Q}$ galoissch, also insbesondere separabel, ist, ist $x_1$ separabel. Da $f = \mu_{\mathbb{Q}, x_1}$, ist $f$ separabel. Damit hat $f$ nur einfache Nullstellen in $L$. Der Fall, dass zwei Nullstellen von $f$ übereinstimmen, kann also nicht auftreten. □

**Aufgabe 235 (H19T2A5(a,b,c))** Sei $K$ ein Körper der Charakteristik $p$, $a \in K$ und $f = x^p - x - a \in \mathbb{K}[x]$.

(a) Sei $L$ Erweiterungskörper von $K$ und $b \in L$ eine Nullstelle von $f$. Wir zeigen, dass auch $f(b+1) = 0$, d.h., dass auch $b+1$ eine Nullstelle von $f$ ist. Es gilt nämlich $f(b+1) = (b+1)^p - (b+1) - a = b^p + 1 - b - 1 - a = b^p - b - a = f(b) = 0$. Mit $b \in L$ ist also auch $b+1$ Nullstelle von $f$ und in $L$.
(b) Wir zeigen, dass $f$ entweder eine Nullstelle in $K$ hat oder irreduzibel ist. Falls $f$ eine Nullstelle in $K$ hat, ist $f$ offenbar nicht irreduzibel. Mit Teil (a) sehen wir, dass alle $p$ Nullstellen von $f$ die Form $b+k$ mit $0 \leq k \leq p-1$ haben und somit in $K$ liegen. Wir zeigen nun, dass im Falle, dass $f$ keine Nullstellen in $K$ hat, $f$ auch irreduzibel ist. Angenommen, $f$ hat keine Nullstelle in $K$ und ist reduzibel. Dann gibt es zwei Polynome $g, h$, beide vom Grad $\geq 2$, sodass $f = gh$. Sei $L = \mathrm{Zerf}(f)$ und $b \in L$ eine Nullstelle von $f$. Mit der obenstehenden Bemerkung wissen wir, dass bereits alle Nullstellen von $f$ in $L$ liegen und die Form $b+k$ mit $0 \leq k \leq p-1$ haben. Da $\deg(g) \geq 2$ hat $g$ in $L$ mindestens zwei Nullstellen. Genauer gibt es $l, k \in \{0, 1, .., p-1\}$ mit $l > k$, sodass $b+k$ und $b+l$ zwei verschiedene Nullstellen von $g$ sind. Nun existiert laut Fortsetzungssatz ein $K$-Homomorphismus $\sigma : K(b+k) \to L$ mit $\sigma(b+k) = b+l$. Laut Vorlesung ist dann $b+l$ ebenfalls eine Nullstelle von $g$ und wegen $(b+l) - (b+k) = l - k \in K$ ist auch $b + l \in K(b+k)$. Induktiv sehen wir damit, dass auch $b + k + q(l-k)$ für $q \in \mathbb{N}_0$ Nullstellen von $g$ sind. Da $l - k \geq 1$ ist $l - k \in \mathbb{F}_p^\times$ und wir finden ein $q$, sodass $q(l-k) = 1$. Damit ist auch $(b+k) + q(l-k) = (b+k) + 1 \in K(b+k)$ und Nullstelle von $g$, und zudem $b + k + 1 \neq b + k$. Induktiv sieht man nun, dass $g$ $p$ verschiedene Nullstellen hat, also aus Gradgründen $h \in K^\times$ gelten muss. Das ist aber ein Widerspruch dazu, dass $f$ als reduzibel angenommen wurde. Also ist $f$ irreduzibel, da es wegen $\deg(f) > 0$ eine Nicht-Einheit in $K[x]$ ist.
(c) Sei nun $f$ als irreduzibel vorausgesetzt. Wir zeigen, dass $\mathrm{Gal}(f|K)$ dann zyklisch und von Ordnung $p$ ist. Bezeichne $L = \mathrm{Zerf}(f)$ den Zerfällungskörper von $f$ über $K$. Dann gilt $\mathrm{Gal}(f|K) = \mathrm{Gal}(L|K)$. Wir müssen noch zeigen, dass $L|K$ galoissch ist. Da $L$ Zerfällungskörper von $f$ ist und $f$ nach Voraussetzung irreduzibel ist, ist $L|K$ normal. Sei $b \in L$ eine Nullstelle von $f$. Nach Teil (b) ist dann $N = \{b+l | 0 \leq l < p\}$ die Nullstellenmenge von $f$ in $L$ und es gilt $L = K(N) \supsetneq K$. Da $N$ eine endliche Menge von über $K$ algebraischen Elementen ist, ist $L|K$ algebraisch und wegen $\mathrm{char}(K) = p \in \mathbb{P}$, eine Primzahl also, ist $L|K$ separabel. Insgesamt ist $L|K$ also galoissch. Es gilt nun $K(N) = K(b)$, denn $b \in N$ liefert die Inklusion $\supseteq$ und andererseits ist mit $1, b \in K(b)$ auch $b + l = b + l \cdot 1 \in K(b)$ für alle $l \in \{0, 1, 2, ..., p-1\}$. Nun ist nach Voraussetzung $f$ irreduzibel über $K$ und $f(b) = 0$ nach Definition von $b$. Da $f$ zudem normiert ist, ist $f = \mu_{K,b}$ und es gilt für den Grad der Erweiterung $L|K$ $[L : K] = \deg(f) = p$. Damit ist $|\mathrm{Gal}(f|K)| = [L : K] = p$. Die Galoisgruppe von $f$ über $K$ hat also die Ordnung $p$. Als Gruppe von Primzahlordnung ist $\mathrm{Gal}(f|K)$ damit bereits zyklisch. □

**Aufgabe 236 (H16T2A4)** Sei $p > 2$ eine Primzahl und $\zeta_p := \exp(2\pi i/p)$ eine primitive $p$-te Einheitswurzel sowie $\alpha_p := \sqrt[p]{p}$. Wir betrachten $K := \mathbb{Q}(\alpha_p, \zeta_p)|\mathbb{Q}$.
(a) Wir zeigen, dass $K|\mathbb{Q}$ galoissch ist. Zunächst sind $\zeta_p$ und $\alpha_p$ Nullstellen des $p$-ten Kreisteilungspolynoms $\Phi_p(x) = x^{p-1} + x^{p-2} + ... + x + 1 \in \mathbb{Q}[x]$ und $f(x) = x^p - p \in \mathbb{Q}[x]$ respektive. Damit sind $\zeta_p$ und $\alpha_p$ jeweils algebraisch über $\mathbb{Q}$. Als von zwei, also insbesondere endlich vielen, algebraischen Elementen erzeugte Körpererweiterung

ist $K|\mathbb{Q}$ endlich und damit laut Vorlesung algebraisch. Als endliche Erweiterung über dem Körper $\mathbb{Q}$, der die Charakteristik 0 hat, ist $K|\mathbb{Q}$ somit separabel. Die Nullstellen von $f$ sind ferner gegeben durch $x_k = \alpha_p \zeta_p^k$, wo $k \in \{0, 1, 2, ..., p-1\}$. Wir behaupten, dass $K = \text{Zerf}(f)$, d.h., der Zerfällungskörper von $f$ ist. Sei $N = \{\alpha_p, \alpha_p\zeta_p, ...\alpha_p\zeta_p^{p-1}\}$ die Nullstellenmenge von $f$. Zu zeigen ist, dass $\mathbb{Q}(N) = K$. Es ist $x_k = \alpha_p \cdot (\zeta_p)^k \in K$ für alle $k \in \{0, 1, 2, ..., p-1\}$, womit bereits $\mathbb{Q}(N) \subseteq K$ gezeigt ist. Für die umgekehrte Inklusion beachten wir, dass $\alpha_p \in N$, sodass $\alpha_p \in \mathbb{Q}(N)$. Weiterhin ist $\zeta_p = x_1/x_0 = \alpha_p\zeta_p/\alpha_p$, denn $\alpha_p \neq 0$. Somit ist $\zeta_p \in \mathbb{Q}(N)$. Insgesamt gilt also auch $K \subseteq \mathbb{Q}(N)$ und zusammen mit der vorher bewiesenen Inklusion $\mathbb{Q}(N) = K$. Als Zerfällungskörper des Polynoms $f \in \mathbb{Q}[x]$ ist $K|\mathbb{Q}$ somit auch eine normale Körpererweiterung. Da $K|\mathbb{Q}$ normal und separabel ist, ist $K|\mathbb{Q}$ wie behauptet galoissch.
(c) Wir zeigen, dass $[K : \mathbb{Q}] = p(p-1)$. Zunächst ist das in Aufgabenteil (a) definierte Polynom $f$ als ganzzahliges und normiertes Polynom sogar als Element aus $\mathbb{Z}[x]$ interpretierbar und dort primitiv. Das Eisensteinkriterium für die Primzahl $p$ liefert dann die Irreduzibilität von $f$ in $\mathbb{Z}[x]$. Wegen des Lemmas von Gauss ist das primitive Polynom $f$ auch in $\mathbb{Q}[x]$ irreduzibel. Da $f$ normiert und irreduzibel ist und zudem $f(\alpha_p = \sqrt[p]{p}^p - p = p - p = 0$, also $\alpha_p$ eine Nullstelle von $f$ ist, handelt es sich bei $f$ um das Minimalpolynom $\mu_{\mathbb{Q},\alpha_p}$ von $\alpha_p$ über $\mathbb{Q}$. Aus der Vorlesung ist bekannt, dass das $p$-te Kreisteilungspolynom $\Phi_p$, wie in (a) angegeben, das Minimalpolynom von $\zeta_p$ über $\mathbb{Q}$ ist. Da $\zeta_p, \alpha_p \in K$ aber $\zeta_p, \alpha_p \notin \mathbb{Q}$ besitzt $K|\mathbb{Q}$ zwei echte Zwischenkörper $M_1 := \mathbb{Q}(\alpha_p)$ und $M_2 := \mathbb{Q}(\zeta_p)$. Für den Erweiterungsgrad von $M_1|\mathbb{Q}$ und $M_2|\mathbb{Q}$ gilt jeweils $[M_1 : \mathbb{Q}] = \deg(\mu_{\mathbb{Q},\alpha_p}) = \deg(f) = p$ und $[M_2 : \mathbb{Q}] = \deg(\mu_{\mathbb{Q},\zeta_p}) = \deg(\Phi_p) = p - 1$. Damit ist wiederum wegen der Gradformel $(p-1)|[K : \mathbb{Q}]$ und $p|[K : \mathbb{Q}]$. Da $p$ prim ist, $\text{kgV}(p-1, p) = p(p-1)|[K : \mathbb{Q}]$. Mit der Gradformel folgt aber weiter die Abschätzung, dass

$$\begin{aligned}[K : \mathbb{Q}] &= [\mathbb{Q}(\alpha_p)(\zeta_p) : \mathbb{Q}(\alpha_p)][\mathbb{Q}(\alpha_p) : \mathbb{Q}] \\ &\leq [\mathbb{Q}(\zeta_p) : \mathbb{Q}][\mathbb{Q}(\alpha_p) : \mathbb{Q}] \\ &= p(p-1).\end{aligned}$$

Infolge der beiden Ungleichungen gilt insgesamt $[K : \mathbb{Q}]$, wie behauptet.
(c) Wir zeigen zunächst, dass $M_1|\mathbb{Q}$ nicht normal ist. Angenommen, $M_1|\mathbb{Q}$ wäre normal. Dann würde jeder $\mathbb{Q}$-Homomorphismus von $M_1$ in einen algebraischen Abschluss $\bar{\mathbb{Q}}$ sich zu einem $\mathbb{Q}$-Automorphismus von $M_1$ beschränken. Andererseits lässt sich $\text{id} : \mathbb{Q} \to \mathbb{Q}$ durch $\sigma(\alpha_p) = \alpha_p\zeta_p$ zu einem $\mathbb{Q}$-Homomorphismus $\sigma : M_1 \to \bar{\mathbb{Q}}$ fortsetzen. Wegen $\alpha_p \in \mathbb{R}$ gilt aber $M_1 \subseteq \mathbb{R}$, sodass $\alpha_p\zeta_p \notin M_1$, da $\zeta_p \notin \mathbb{R}$ für $p > 2$. Somit beschränkt sich $\sigma$ nicht zu einem $\mathbb{Q}$-Automorphismus von $M_1$. Das ist ein Widerspruch zur Annahme, dass die Erweiterung $M_1|\mathbb{Q}$ normal ist. Damit ist $M_1|\mathbb{Q}$ nicht normal. Wir zeigen nun, dass $\text{Gal}(K|\mathbb{Q})$ nicht abelsch ist. Angenommen, $\text{Gal}(K|\mathbb{Q})$ ist abelsch. Dann ist insbesondere jede Untergruppe $U$ von $\text{Gal}(K|\mathbb{Q})$ ein Normalteiler und es gilt nach einem Korollar zum Hauptsatz der Galoistheorie, dass der nach dem Hauptsatz der Galoistheorie zu $U$ korrespondierende Fixkörper $K^U$ vermöge $K^U|\mathbb{Q}$ eine normale Erweiterung definiert. Andererseits ist $\text{Gal}(K|M_1)$ die nach dem Hauptsatz der Galoistheorie zu $M_1$ korrespondierende Galoisgruppe, die wegen der obigen Ausführungen ein Normalteiler von $\text{Gal}(K|\mathbb{Q})$ ist. Die obigen Ausführungen liefern weiter, dass $M_1 = K^{\text{Gal}(K|M_1)}|\mathbb{Q}$ eine normale Körpererweiterung ist. Das

hatten wir aber bereits im ersten Teil der Teilaufgabe (c) ausgeschlossen. Wegen des so entstandenen Widerspruchs war die Annahme, $\mathrm{Gal}(K|\mathbb{Q})$ wäre eine abelsche Gruppe, falsch. Damit ist $\mathrm{Gal}(K|\mathbb{Q})$ eine nicht-abelsche Gruppe.
(d) Wir zeigen, dass $\mathrm{Gal}(K|\mathbb{Q})$ einen Normalteiler der Ordnung $p$ hat. Sei für jede Primzahl $q$ mit $\nu_q$ die Anzahl der $q$-Sylowgruppen von $G := \mathrm{Gal}(K|\mathbb{Q})$ bezeichnet. Aus der Vorlesung ist zudem $|\mathrm{Gal}(K|\mathbb{Q})| = [K : \mathbb{Q}] = (p-1)p$ bekannt. Dann gilt nach dem dritten Sylowschen Satz für die Anzahl $\nu_p$ der $p$-Sylowgruppen von $G$, dass $\nu_p|(p-1)$ und $\nu_p \equiv 1 \bmod(p)$. Die zweite Bedingung impliziert $\nu_p = 1$ oder $\nu_p > p$. Der zweite Fall kann aber nicht auftreten, denn die erste Bedingung erfordert $\nu_p \leq (p-1) < p$. Somit ist $\nu_p = 1$. Da die höchste $p$-Potenz, die $|G|$ teilt, gerade $p^1$ ist, ist die einzige $p$-Sylowgruppe $P$ von $G$ von der Ordnung $p$. Da $\nu_p = 1$, liefert der zweite Sylowsche Satz, dass $P \trianglelefteq G$, d.h., $\mathrm{Gal}(K|\mathbb{Q})$ besitzt mit $P$ einen Normalteiler der Ordnung $p$. □

**Aufgabe 237 (F16T3A5)** Gegeben sei $f = x^4 - 2x^2 - 2 \in \mathbb{Q}[x]$ und $\alpha_1 = \sqrt{1+\sqrt{3}}$ sowie $\alpha_2 = \sqrt{1-\sqrt{3}}$.
(a) Wir zeigen, dass $N = \{\alpha_1, \alpha_2, -\alpha_1, -\alpha_2\}$ die Nullstellenmenge von $f$ ist. Zunächst gilt $\alpha_1 \neq 0$ und $\alpha_2 \neq 0$. Ferner ist $\alpha_1^2 = 1 + \sqrt{3} > 0$ aber $\alpha_2^2 = 1 - \sqrt{3} < 0$, sodass $\pm\alpha_1 \in \mathbb{R}$ aber $\pm\alpha_2 \in \mathbb{C} \setminus \mathbb{R}$. Somit ist $|N| = 4$. Es gilt ferner mit quadratischer Ergänzung

$$\begin{aligned} 0 &= f(x) \\ \Leftrightarrow 0 &= (x^2-1)^2 - 3 \\ \Leftrightarrow x^2 &= 1 \pm \sqrt{3} \\ \Leftrightarrow x &= \pm\sqrt{1 \pm \sqrt{3}} \\ \Leftrightarrow x &\in N, \end{aligned}$$

sodass $N$ tatsächlich die Nullstellenmenge von $f$ ist.
(b) Wir zeigen, dass $\mathbb{Q}(\alpha_1) \neq \mathbb{Q}(\alpha_2)$. Wegen $\alpha_1 \in \mathbb{R}$ wie in Teil (a) festgestellt wurde, aber $\alpha_2 \notin \mathbb{R}$ folgt $\alpha_2 \notin \mathbb{Q}(\alpha_1)$, sodass $\mathbb{Q}(\alpha_1) \neq \mathbb{Q}(\alpha_2)$.
(c) Wir zeigen, dass $\mathbb{Q}(\alpha_1) \cap \mathbb{Q}(\alpha_2) = \mathbb{Q}(\sqrt{3})$. Wegen $\sqrt{3} = \alpha_1^2 - 1 \in \mathbb{Q}(\alpha_1)$ und $\sqrt{3} = -\alpha_2^2 + 1 \in \mathbb{Q}(\alpha_2)$ ist $\sqrt{3} \in \mathbb{Q}(\alpha_1) \cap \mathbb{Q}(\alpha_2)$, sodass laut Vorlesung bereits $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\alpha_1) \cap \mathbb{Q}(\alpha_2)$. Es ist $f$ normiert, also primitiv, und nach Eisenstein zur Primzahl $p = 2$ irreduzibel über $\mathbb{Q}$. Zusammen mit Teil (a) sehen wir, dass $f = \mu_{\mathbb{Q},\alpha_1}$ und $f = \mu_{\mathbb{Q},\alpha_2}$. Da $\alpha_2 \notin \mathbb{Q}(\alpha_1)$ handelt es sich bei $M := \mathbb{Q}(\alpha_1) \cap \mathbb{Q}(\alpha_2)$ um einen echten Zwischenkörper von $\mathbb{Q}(\alpha_2)$. Wegen $[\mathbb{Q}(\alpha_2) : \mathbb{Q}] = \deg(f) = 4$, muss also $[M : \mathbb{Q}]$ ein Teiler von 4, aber ungleich 4 sein. Da zudem $\sqrt{3} \in M$ nach der oben bewiesenen Inklusion muss zudem $[M : \mathbb{Q}] > 1$, denn $\sqrt{3} \notin \mathbb{Q}$ aber $\mathbb{Q} \subseteq M$ als Teilkörper. Somit ist $[M : \mathbb{Q}] = 2$ als einzig verbleibende Möglichkeit für den Erweiterungsgrad. Da aber $g = x^2 - 3 \in \mathbb{Q}[x]$ normiert, damit primitiv, und nach Eisenstein zu $p = 2$ irreduzibel über $\mathbb{Q}[x]$ ist und ferner $\sqrt{3}$ als Nullstelle besitzt, gilt $g = \mu_{\mathbb{Q},\sqrt{3}}$ und damit $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$. Da $\mathbb{Q}(\sqrt{3}) \subseteq M$ und beide $\mathbb{Q}$-Vektorräume dieselbe $\mathbb{Q}$-Dimension haben, gilt bereits Gleichheit $\mathbb{Q}(\sqrt{3}) = M$.
(d) Da $\mathrm{char}(\mathbb{Q}(\sqrt{3})) = \mathrm{char}(\mathbb{Q}) = 0$, ist $\mathbb{Q}(\alpha_i)|\mathbb{Q}$ als endliche und algebraische Körpererweiterung für $i \in \{1, 2\}$ separabel. Genauer gilt mit der Gradformel und

den Ergebnissen aus Teil (b) für den Erweiterungsgrad $[\mathbb{Q}(\alpha_i) : \mathbb{Q}] = [\mathbb{Q}(\alpha_i) : \mathbb{Q}]/[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = \deg(\mu_{\mathbb{Q},\alpha_i})/\deg(\mu_{\mathbb{Q},\sqrt{3}}) = \deg(f)/\deg(g) = 4/2 = 2$ unabhängig von $i \in \{1, 2\}$. Damit sind $\mathbb{Q}(\alpha_i)|\mathbb{Q}$ als algebraische Körpererweiterungen vom Erweiterungsgrad 2 laut Vorlesung bereits normal. Die Algebraizität der Erweiterungen ist eine Konsequenz davon, dass $\mu_{\mathbb{Q}(\sqrt{3}),\alpha_i}|f$ für $i \in \{1, 2\}$ und $f$ das Minimalpolynom von $\alpha_i$ für $i \in \{1, 2\}$ über $\mathbb{Q}$ nach Teil (b) ist. Als normale und separable Körpererweiterungen (von endlichem Grad) sind $\mathbb{Q}(\alpha_i)|\mathbb{Q}(\sqrt{3})$ für $i \in \{1, 2\}$ jeweils (endliche) galoissche Körpererweiterungen.
(e) Sei $K = \mathrm{Zerf}(f|\mathbb{Q})$. Wir zeigen zunächst, dass $K|\mathbb{Q}(\sqrt{3})$ galoissch ist. Zunächst gilt, dass $K = \mathbb{Q}(N) = \mathbb{Q}(\alpha_1, \alpha_2, -\alpha_1, -\alpha_2) = \mathbb{Q}(\alpha_1, \alpha_2)$. Da $\mathbb{Q}(\sqrt{3})$ Zwischenkörper von $\mathbb{Q}(\alpha_1, \alpha_2)|\mathbb{Q}$ ist, ist $K$ auch Zerfällungskörper von $f$ über $\mathbb{Q}(\sqrt{3})$. Zudem ist $\mathbb{Q}(\alpha_1, \alpha_2)|\mathbb{Q}$ endlich und algebraisch und damit $\mathbb{Q}(\alpha_1, \alpha_2)|\mathbb{Q}(\sqrt{3})$ endlich und algebraisch. Damit ist $\mathbb{Q}(\alpha_1, \alpha_2)|\mathbb{Q}(\sqrt{3})$ eine normale Körpererweiterung. Wegen $\mathrm{char}(\mathbb{Q}(\sqrt{3})) = \mathrm{char}(\mathbb{Q}) = 0$, ist $\mathbb{Q}(\alpha_1, \alpha_2)|\mathbb{Q}(\sqrt{3})$ laut Vorlesung separabel. Im Ergebnis ist $\mathbb{Q}(\alpha_1, \alpha_2)|\mathbb{Q}(\sqrt{3})$ also eine endliche Galois-Erweiterung. Sei nun $P_1$ das Minimalpolynom von $\alpha_2$ über $\mathbb{Q}(\sqrt{3})$ und $P_2$ das Minimalpolynom von $\alpha_2$ über $\mathbb{Q}(\alpha_1)$. Wegen $2 = [\mathbb{Q}(\alpha_2) : \mathbb{Q}(\sqrt{3})] = \deg(P_1)$ nach Teil (c) ist $0 < \deg(P_2) \leq 2$. Falls $\deg(P_2) = 1$, dann ist $\alpha_2 \in \mathbb{Q}(\alpha_1)$, was aber wegen $\mathbb{Q}(\alpha_1) \subseteq \mathbb{R}$ und $\alpha_2 \notin \mathbb{R}$ unmöglich ist. Also ist $\deg(P_1) = \deg(P_2)$ und zusammen mit den Eigenschaften von $P_1$ bzw. $P_2$ Minimalpolynome von $\alpha_2$ über $\mathbb{Q}(\sqrt{3})$ bzw. $\mathbb{Q}(\alpha_1)$ zu sein, folgt bereits Gleichheit $P_1 = P_2$. Damit finden wir $[K : \mathbb{Q}] = [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}(\alpha_1)][\mathbb{Q}(\alpha_1) : \mathbb{Q}] = \deg(P_2)\deg(f) = 2 \cdot 4 = 8$ und wegen $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$ liefert de Gradformel, dass $[\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}(\sqrt{3})] = [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}]/[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 8/2 = 4$. Aus der Vorlesung ist bekannt, dass für die Galoisgruppe $\mathrm{Gal}(\mathbb{Q}(\alpha_1, \alpha_2)|\mathbb{Q}(\sqrt{3})) =: G$ dann gilt $|G| = [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}(\sqrt{3})] = 4$. Als Gruppe von Primzahlquadratordnung ist $G$ abelsch. Genauer ist entweder $G \simeq \mathbb{Z}/4\mathbb{Z}$ oder $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/23\mathbb{Z}$. Im ersten Fall ist $G$ sogar zyklisch und hat somit genau einer Untergruppe $U$ von Ordnung und, nach Lagrange somit auch vom Index, 2. Nach dem Hauptsatz der Galoistheorie hat dann $\mathbb{Q}(\alpha_1, \alpha_2)|\mathbb{Q}(\sqrt{3})$ genau einen Zwischenkörper $M$ vom Erweiterungsgrad 2 über $\mathbb{Q}(\sqrt{3})$. Das ist aber ein Widerspruch dazu, dass $[\mathbb{Q}(\alpha_1) : \mathbb{Q}(\sqrt{3})] = 2 = [\mathbb{Q}(\alpha_2) : \mathbb{Q}(\sqrt{3})]$ nach Teil (c) und $\mathbb{Q}(\alpha_1) \neq \mathbb{Q}(\alpha_2)$ nach Teil (b). Somit war die Annahme, $G \simeq \mathbb{Z}/4\mathbb{Z}$ falsch, und es gilt $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. □

**Aufgabe 238 (H10T2A5)** Sei für ein $n \in \mathbb{N}$ $A \in \mathrm{Mat}(n \times n, \mathbb{Z})$ mit der Eigenschaft, dass $A^p = E_n$ für eine Primzahl $p$. Zu zeigen ist, dass $\det(A - E) \in \mathbb{Z}$ und durch $p$ teilbar. Dass $\det(A - E) \in \mathbb{Z}$ ist klar, denn mit $A, E \in \mathrm{Mat}(n \times n, \mathbb{Z})$ ist auch $A - E \in \mathrm{Mat}(n \times n, \mathbb{Z})$ und mit der Leibniz'schen Darstellung der Determinantenfunktionen, sehen wir, dass sich diese auf $\mathrm{Mat}(n \times n; \mathbb{Z})$ zu einer Abbildung nach $\mathbb{Z}$ beschränkt. Zudem ist $\pi : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}, x \mapsto x \bmod(p)$ verträglich mit der Determinantenabbildung im Sinne, dass $\det' \circ \pi' = \pi \circ \det$, wo $\pi' : \mathrm{Mat}(n \times n, \mathbb{Z}) \to \mathrm{Mat}(n \times n, \mathbb{Z}/p\mathbb{Z})$ die komponentenweise Reduktion einer Matrix modulo $p$ und $\det : \mathrm{Mat}(n \times n, \mathbb{Z}/p\mathbb{Z}) \to \mathbb{Z}/p\mathbb{Z}$ die Determinantenfunktion für $n \times n$-Matrizen mit Koeffizienten in $\mathbb{Z}/p\mathbb{Z}$ bezeichnet. Nach diesen Vorbereitungen finden wir, dass $\pi(\det(A - E_n)) = \det'(\pi'(A - E_n))$. Zudem gilt, wegen $AE_n = E_nA$, $0 = \pi'(0) = \pi'(A^p - E_n^p) = \pi'(A - E_n)^p$, und somit $\det'(\pi'(A - E_n))^p = \det(0) = 0$, also $0 = \pi(\det(A - E_n))$, d.h., $p|\det(A - E_n)$. □

**Aufgabe 239 (H12T2A4)** Sei $p$ eine Primzahl und $K$ ein Körper der Charakteristik 0.
(a) Sei $E|K$ eine endliche galoissche Erweiterung. Zu zeigen ist, dass $E|K$ einen Zwischenkörper $F$ besitzt, sodass $[E : F]$ eine $p$-Potenz ist und $[F : K]$ nicht von $p$ geteilt wird. Da $E|K$ endlich und galoissch ist, gilt für die Ordnung der Galoisgruppe $G$ von $E|K$, dass $\infty > |G| = [E : K]$. Da $p \nmid [F : K] =: m$ und $[E : F] = p^r$ für ein $r \in \mathbb{N}_0$ für den noch zu bestimmenden, gilt mittels Gradformel $[E : K] = [E : F][F : K] = p^r m$. Wir schreiben also $|G| = p^r m$ mit $p \nmid m$ für eine beliebige, aber feste Primzahl $p$. Damit ist $p^r$ die maximale $p$-Potenz, die $|G|$ teilt. Aus der Sylow-Theorie ist bekannt, dass die Gruppe $G$ der Ordnung $p^r m$ mindestens eine $p$-Sylowgruppe $P$ besitzt, die Ordnung $p^r$ hat. Zu einem solchen, nun fixierten $P$, existiert wegen des Hauptsatzes der Galoistheorie (genau) ein Zwischenkörper $M = E^P$, nämlich der Fixkörper von $P$. Laut Vorlesung gilt ferner $[E : M] = |\mathrm{Gal}(E|M)| = |P| = p^r$. Zudem gilt mittels Gradformel und $[E : K] = p^r m$, dass $[M : K] = [E : K]/[M : K] = m$, also $p \nmid [M : K]$. Damit haben wir mit $M$ einen Zwischenkörper von $E|K$ gefunden, der die geforderten Eigenschaften besitzt.
(b) Besitze $K$ nun die zusätzliche Eigenschaft, dass der Grad ein jeder endlichen, nicht-trivialen Körpererweiterung $L|K$ von $p$ geteilt wird. Zu zeigen ist, dass der Grad von $L|K$ dann eine $p$-Potenz ist. Sei $L|K$ eine endliche, nicht-triviale Körpererweiterung. Da $\mathrm{char}(K) = 0$ und $L|K$ endlich ist, ist $L|K$ separabel und mit dem Satz vom primitiven Element finden wir zusätzlich ein $\alpha \in L \setminus K$ (wegen Nicht-Trivialität von $L|K$), sodass $L = K(\alpha)$. Bezeichne nun mit $f = \mu_{K,\alpha}$. Sei nun $E = \mathrm{Zerf}(f|K)$. Dann ist $E|K$ eine endliche Körpererweiterung und zudem ist $E|K$ endliche und separable Körpererweiterung. Da $E|K$ als endliche Körpererweiterung insbesondere endlich erzeugt und algebraisch ist sowie $E$ definitionsgemäß der Zerfällungskörper des Polynoms $f \in K[x]$ ist, ist $E|K$ zudem normal. Als endliche, separable und normale Körpererweiterung ist $E|K$ eine endliche galoissche Erweiterung und $L$ ist ein Zwischenkörper dieser. Für die beliebig aber fest gewählte Primzahl $p$ gilt laut Voraussetzung an $K$ nun, dass $p|[L : K]$. Sei $P$ eine der $p$-Sylowgruppen von $\mathrm{Gal}(E|K)$, sodass $P \geq U$, wo $U$ die nach dem Hauptsatz zu $L|K$ korrespondierende Untergruppe von $\mathrm{Gal}(E|K)$ ist. Nach der Gradformel ist dann $E^P$ echter Teilkörper von $L|K$ und es gilt $[L : K] = [L : E^P][E^p : K]$. Zudem ist $|G|/|P| = [E^P : K]$ der größte, von $L$ verschiedene Teilkörper von $L|K$ mit nicht durch $p$ teilbaren Erweiterungsgrad. Es gilt dann mit $|G| = p^r m$ und $p \nmid m$ ($m \in \mathbb{N}$, $r \in \mathbb{N}_0$), dass $|P| = p^r$ und $|U| = p^k, (0 \leq k < r)$, also $[E : E^P] = p^r$ und $[E : L] = p^k$. Mit der Gradformel folgt $[L : K] = p^{r-k} m$ und $[E^P : K] = m$. Angenommen, $E^P|K$ ist nicht-trivial. Dann ist nach Teil (a) zunächst $[E^P : K] = m > 1$ und $p \nmid m$. Das widerspricht aber der Eigenschaft von $K$, dass jede endliche nicht-triviale Erweiterung von $K$ einen durch $p$ teilbaren Erweiterungsgrad hat. Also ist $[E^P : K] = 1$ im Widerspruch dazu, dass $E^P|K$ nicht-triviale Erweiterung ist. Damit gilt bereits $E^P = K$ und somit $[E^P : K] = 1$, also $[L : K] = p^{r-k}$ und der Erweiterungsgrad von $L|K$ ist schließlich in der Tat eine $p$-Potenz. □

**Aufgabe 240** (a) Gesucht ist die Anzahl der Körperhomomorphismen $\mathbb{Q}(\sqrt[4]{3}) \to \mathbb{C}$. Jeder Körperhomomorphismus, der wie gewünscht abbildet beschränkt sich auf

$\mathbb{Q}$ zur Identität. Es ist $f = x^4 - 3 \in \mathbb{Q}[x]$ normiert und nach dem Eisensteinkriterium zur Primzahl 3 irreduzibel über $\mathbb{Q}$. Zudem ist $f(\sqrt[4]{3}) = 0$. In $\mathbb{C}$ gilt unter einem Körperhomomorphismus $\sigma : \mathbb{Q}(\sqrt[4]{3}) \to \mathbb{C}$, dass $\sigma(f) = x^4 - 3$. Dieses Polynom hat die vier Nullstellen $\pm\sqrt[4]{3}, \pm\sqrt[4]{3}$ in $\mathbb{C}$. Nach dem Fortsetzungssatz der Körpertheorie ist $\sigma$ dann bereits als Fortsetzung von $\mathrm{id}_{\mathbb{Q}}$ auf $\mathbb{Q}(\sqrt[4]{3})$ durch Angabe von $\sigma(\sqrt[4]{3}) \in \{\pm\sqrt[4]{3}, \pm i\sqrt[4]{3}\}$ festgelegt. Da die letzte Menge vier Elemente enthält, gibt es genau vier verschiedene Möglichkeiten, $\sigma(\sqrt[4]{3})$ und damit $\sigma$ festzulegen. Die gesuchte Anzahl ist also 4.
(b) Gesucht ist die Anzahl der Körperhomomorphismen $\mathbb{Q}(\sqrt[4]{3}) \to \mathbb{R}$. Da unter Beibehaltung der Bezeichnungen aus Teil (a) genau zwei der komplexen Nullstellen von $f$ in $\mathbb{R}$ liegen, nämlich $\pm\sqrt[4]{2} \in \mathbb{R}$, haben wir lediglich zwei Möglichkeiten, $\mathrm{id}_{\mathbb{Q}}$ zu einem Körperhomomorphismus $\sigma \in \mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[4]{2}) \to \mathbb{R})$ fortzusetzen. Die gesuchte Anzahl ist also in diesem Fall 2.
(c) Gesucht ist die Anzahl der Körperhomomorphismen $\mathbb{Q}(\sqrt[4]{3}, \sqrt{-3}) \to \mathbb{C}$. Wir suchen Fortsetzungen der Körperhomorphismen aus Teil (a). Das Polynom $g = x^2 + 3 \in \mathbb{Q}[x]$ ist nach Eisenstein zur Primzahl $p = 3$ irreduzibel über $\mathbb{Q}$ und hat nur die beiden rein imaginären Nullstellen $\pm\sqrt{-3}$. Damit ist $g$ auch über dem Teilkörper $\mathbb{Q}(\sqrt{-3})$ von $\mathbb{R}$ irreduzibel als Polynom vom Grad 2. Damit haben wir laut dem Fortsetungssatz genau zwei Möglichkeiten, den Körperhomomorphismus $\sigma \in \mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[4]{2}, \sqrt{-3}))$ durch Angabe des Bildes von $\sqrt{-3}$ in $\mathbb{C}$ fortzusetzen. Denn es stehen hierfür nur die Möglichkeiten $\pm\sqrt{-3}$ zur Disposition. Da es laut Fortsetzungssatz ferner keine weiteren Körperhomomorphismen mit dem gewünschten Abbildungsverhalten gibt, existiere genau $4 \cdot 2 = 8$ Körperhomomorphismen.
(d) Gesucht ist die Anzahl der Körperhomomorphismen $\mathbb{Q}(\sqrt[4]{3}, \sqrt{-3}) \to \mathbb{R}$. Einen solchen Homomorphismus kann es nicht geben, denn wäre $\sigma$ ein solcher, so wäre $\sigma(\sqrt{-3}) \in \mathbb{R}$ eine Nullstelle von $f = x^2 + 3 \in \mathbb{Q}[x]$. Da aber $f$ laut (c) nur rein imaginäre Nullstellen besitzt, in $\mathbb{R}$ also nullstellenfrei ist, haben wir einen Widerspruch. Einen Körperhomomorphismus mit dem gewünschten Abbildungsverhalten kann es also nicht geben.
(e) Gesucht ist die Anzahl der Körperhomomorphismen $\mathbb{Q}(\sqrt[3]{2}, \zeta\sqrt[3]{2}) \to \mathbb{C}$, wobei $\zeta = \exp(2\pi i/3)$ eine dritte primitive Einheitswurzel ist.
□

**Aufgabe 241 (F18T3A5)** Sei $K = \mathbb{Q}(i)$ und $\alpha = \sqrt[4]{7}$. Ferner sei $L$ der Zerfällungskörper von $f = x^4 - 7 \in K[x]$ über $K$.
(a) Wir zeigen, dass $L = K(\alpha)$. Sei $N$ die Nullstellenmenge von $f$ in $\mathbb{C}$. Es ist $|N| \leq 4$, da $\deg(f) = 4$ und $\mathbb{C}$ algebraisch abgeschlossen ist. Es ist $f(\alpha) = 0$, $f(-\alpha) = 0$ und $f(i\alpha) = 0 = f(-i\alpha)$ und zudem sind $\alpha, -\alpha, i\alpha, -i\alpha$ paarweise verschieden, denn $\alpha \neq 0$ und die ersten beiden komplexen Zahlen sind sogar reell, wohingegen die beiden letzten Zahlen rein imaginär sind. Damit gilt $N = \{\alpha, -\alpha, i\alpha, -i\alpha\}$. Nach Definition von $L$ in der Angabe, $L = K(N)$. Wegen $\alpha \in N$ ist $K(\alpha) \subseteq K(N)$ klar. Umgekehrt ist mit $i \in K \subseteq K(\alpha)$ und $\alpha \in K(\alpha)$ auch $i\alpha, -i\alpha \in K(\alpha)$. Aus $\alpha \in K(\alpha)$ folgt bereits $-\alpha \in K(\alpha)$. Damit ist $N \subseteq K(\alpha)$ und wir haben auch $K(N) \subseteq K(\alpha)$. Insgesamt ist also $K(\alpha) = K(N)$ und damit $K(\alpha) = L$.
(b) Wir sollen $L|K$ und $L|\mathbb{Q}$ bestimmen. Zunächst gilt $L = \mathbb{Q}(i, \alpha)$. Wir stellen fest, dass $f = \mu_{\mathbb{Q},\alpha}$, denn $f$ ist über $\mathbb{Q}$ nach dem Eisensteinkriterium zur Primzahl

7 irreduzibel, ferner normiert und es gilt $f(\alpha) = 0$. Somit ist $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Das Polynom $g = x^2 + 1 \in \mathbb{Q}[x]$ hat keine reellen Nullstellen, und ist somit als Polynom vom Grad 2 bereits über jedem Teilkörper von $\mathbb{R} \supseteq \mathbb{Q}(\alpha)$ irreduzibel. Insbesondere ist $g$ über $\mathbb{Q}(\alpha)$ irreduzibel. Da $g(i) = 0 = g(-i)$, $g$ normiert und über $\mathbb{Q}(\alpha)$ irreduzibel ist, folgt $[\mathbb{Q}(\alpha)(i) : \mathbb{Q}(\alpha)] = \deg(g) = 2$. Mit der Gradformel erhalten wir also $[L : \mathbb{Q}] = [\mathbb{Q}(\alpha, i) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot 4 = 8$. Indem wir $g = \mu_{\mathbb{Q},i}$ verwenden, da $g$ insbesondere keine Nullstellen in $\mathbb{Q}$ besitzt und als Polynom vom Grad 2 somit über $\mathbb{Q}$ irreduzibel ist, finden wir $[\mathbb{Q}(i) : \mathbb{Q}] = \deg(g) = 2$. Die Gradformel liefert dann $8 = [L : \mathbb{Q}] = [L : K][K : \mathbb{Q}] = [L : K][\mathbb{Q}(i) : \mathbb{Q}] = [L : K] \cdot 2$ unter Verwendung unseres vorherigen Ergebnisses und schließlich $[L : K] = 8/2 = 4$.
(c) Wir zeigen, dass $L|K$ galoissch ist. Da $\mathbb{Q}$ ein Teilkörper von $K$ ist, gilt $\mathrm{char}(K) = \mathrm{char}(\mathbb{Q}) = 0$. Da $L = K(\alpha)$, also insbesondere algebraisch und endlich nach (b), ist $L|K$ laut Vorlesung separabel. Da $[K(\alpha) : K] = 4$ und $\deg(f) = 4$, ist $f = \mu_{K,\alpha}$ aus Gradgründen. Somit ist $f$ irreduzibel über $K$ und als Zerfällungskörper eines über $K$ irreduziblen Polynoms liefert $L$ die normale Erweiterung $L|K$. Als normale und separable Erweiterung vom endlichen Erweiterungsgrad 4 handelt es sich bei $L|K$ um eine endliche galoissche Erweiterung.
(d) Zunächst gilt $|\mathrm{Gal}(L|K)| = [L : K] = 4$ und die erste Gleichheit gilt laut Vorlesung. Laut Voraussetzung ist $\sigma \in \mathrm{Gal}(L|K)$ und definiert durch $\sigma(\alpha) = i\alpha$. Somit ist $\mathrm{ord}(\sigma) > 1$, denn $\alpha \in \mathbb{R}$ aber $i\alpha \notin \mathbb{R}$. Ferner gilt $\sigma^2(\alpha) = \sigma(\sigma(\alpha)) = \sigma(i\alpha) = i\sigma(\alpha) = i \cdot i\alpha = -\alpha \neq \alpha$, wobei wir verwendet haben, dass $i \in K$ und für alle $x \in K$ $\sigma(x) = x$ gilt. Somit ist auch $\mathrm{ord}(\alpha) > 2$. Da $\langle\sigma\rangle \leq \mathrm{Gal}(L|K)$ und $\mathrm{ord}(\sigma) = |\langle\sigma\rangle||\mathrm{Gal}(L|K)$ nach dem Satz von Lagrange, ist bereits $\mathrm{ord}(\sigma) = 4$. Somit ist $\mathrm{Gal}(L|K) = \langle\sigma\rangle$, die betrachtete Galoisgruppe also zyklisch und von der Ordnung 4. □

**Aufgabe 242** Sei $L|K$ eine galoissche Erweiterung mit $G := \mathrm{Gal}(L|K) \simeq \mathbb{Z}/10\mathbb{Z}$. Gesucht ist die Anzahl der Zwischenkörper von $L|K$. Da $G$ isomorph zu einer zyklischen Gruppe der Ordnung 10 ist, ist $G$ selbst zyklisch und von Ordnung 10. Laut Vorlesung hat eine zyklische Gruppe der Ordnung $n \in \mathbb{N}$ für jeden (positiven) Teiler $k|n$ genau eine Untergruppe der Ordnung $n/k$ und es gibt darüber hinaus keine weiteren Untergruppen der betrachteten zyklischen Gruppe. Die Menge $M$ der Teiler von 10 ist $M = \{1, 2, 5, 10\}$. Also hat $G$ genau 4 Untergruppen. Nach dem Hauptsatz der Galoistheorie korrespondieren die Untergruppen von $G$ vermöge $U \mapsto L^U$ bijektiv zu den Zwischenkörpern von $L|K$, wo $U$ eine solche Untergruppe und $L^U$ den Fixkörper unter $U$ bezeichnet. Insbesondere ist die Anzahl der Zwischenkörper von $L|K$ gleich der Anzahl der Untergruppen von $G$ im Falle einer endlichen Galoiserweiterung. Somit hat $L|K$ genau 4 Zwischenkörper. □

**Aufgabe 243 (F10T2A5)** Sei $E|K$ eine endliche Galoiserweiterung und $\alpha \in E$ sei dergestalt, dass $\sigma(\alpha) \neq \alpha$ für alle $\sigma \in \mathrm{Gal}(E|K) \setminus \{\mathrm{id}\}$. Wir zeigen, dass $E = K(\alpha)$. Da $\alpha \in E$ ist $Z := K(\alpha) \subseteq E$. Angenommen, $Z \neq E$. Dann ist $Z$ ein von $E$ verschiedener Zwischenkörper der galoisschen Erweiterung $E|K$. Nach dem Hauptsatz der Galoistheorie gibt es somit eine eindeutige Untergruppe $U \leq \mathrm{Gal}(E|K)$, sodass $E^U = Z$, nämlich gerade $U = \mathrm{Gal}(E|Z)$. Da $\mathrm{Gal}(E|E) = \{\mathrm{id}\}$, gibt es ein $\sigma \in \mathrm{Gal}(E|Z)$, das von der Identität $\mathrm{id} : E \to E$ verschieden ist. Dann

gilt $\sigma(\alpha) = \alpha$, denn $K = E^U$ und $\sigma \in U$. Das ist aber ein Widerspruch dazu, dass $\sigma(\alpha) \neq \alpha$ für alle von der Identität auf $E$ verschiedenen $K$-Automorphismen von $L$, insbesondere also das $\sigma$ von gerade eben, gilt. Damit ist $E = K(\alpha)$. □

**Aufgabe 244** Sei $L \subseteq \mathbb{C}$ der Zerfällungskörper des Polynoms $f = x^5 - 2 \in \mathbb{Q}[x]$ und seien $\alpha = \sqrt[5]{2}$ sowie $\zeta = \exp(2\pi i/5)$.
(a) Wir zeigen, dass $L = \mathbb{Q}(\alpha, \zeta)$. Nach Definition ist $L$ der Zerfällungskörper von $f$ über $\mathbb{Q}$. Bezeichne $N \subseteq \mathbb{C}$ die Nullstellenmenge von $f$ in $\mathbb{C}$. Da $\mathbb{C}$ algebraisch abgeschlossen und $f$ ein Polynom in $\mathbb{Q}[x] \subseteq \mathbb{C}[x]$ vom Grad 5 ist, ist $|N| \leq 5$. Es gilt die Äquivalenz $f(x) = 0 \Leftrightarrow x^5 = 2 \Leftrightarrow x \in \{\alpha\zeta^k | 0 \leq k < 5\}$, wobei $\alpha := \sqrt[5]{2} \neq 0$ und $\zeta = \exp(2\pi i/5)$ eine primitive fünfte Einheitswurzel, wie in der Angabe angegeben, sind. Für $L$ gilt definitionsgemäß $L = \mathbb{Q}(N)$. Dann ist $\{\alpha, \zeta\} \subseteq \mathbb{Q}(N)$ und $N \subseteq \mathbb{Q}(\alpha, \zeta)$ zu zeigen, um $\mathbb{Q}(\alpha, \zeta) = L$ zu beweisen. Da $\alpha \in N \subseteq \mathbb{Q}(N)$ und mit $\alpha, \alpha\zeta \in \mathbb{Q}(N)$ auch $\zeta = (\alpha\zeta)/\alpha \in \mathbb{Q}(N)$, ist die Inklusion $\{\alpha, \zeta\} \subseteq \mathbb{Q}(N)$ klar. Für die umgekehrte Inklusion beachten wir, dass für $z \in N$ ein $k \in \{0, 1, 2, 3, 4\}$ existiert, sodass $z = \alpha\zeta^k$. Da $\alpha, \zeta \in \mathbb{Q}(\alpha, \zeta)$ ist auch $\alpha \cdot \zeta^k \in \mathbb{Q}(\alpha, \zeta)$, d.h., $z \in \mathbb{Q}(\alpha, \zeta)$. Beliebigkeit von $z \in N$ liefert nun die Gültigkeit der in Rede stehenden Inklusion. Mithin ist $L = \mathbb{Q}(\alpha, \zeta)$.
(b) Wir zeigen, dass $L|\mathbb{Q}$ galoissch ist. Dazu beachten wir, dass $f$ irreduzibel über $\mathbb{Q}[x]$ ist. Denn $f$ ist normiert und hat nur ganzzahlige Koeffizienten, ist also primitiv. Das Eisenstein-Kriterium zur Primzahl $p = 2$, angewendet auf $f$, das als Element von $\mathbb{Z}[x]$ aufgefasst wird, liefert die Irreduzibilität von $f$ in $\mathbb{Z}[x]$. Das Lemma von Gauss liefert nun die Irreduzibilität von $f$ über $\mathbb{Q}$. Als Zerfällungskörper eines irreduziblen Polynoms über $\mathbb{Q}$ ist $L|\mathbb{Q}$ normal und zudem algebraisch. Als algebraische und, da von endlich vielen algebraischen Elementen erzeugte, endliche Erweiterung über einer Körper der Charakteristik 0, ist $L|\mathbb{Q}$ separabel. Als normale und separable endliche Erweiterung ist $L|\mathbb{Q}$ galoissch und von endlichem Erweiterungsgrad.
(c) Wir zeigen, dass $G = \mathrm{Gal}(L|\mathbb{Q})$ eine nichtabelsche Gruppe der Ordnung 20 ist. Um zu sehen, dass $|G| = 20$, verwenden wir, dass $|G| = [L : \mathbb{Q}]$, da $L|\mathbb{Q}$ endlich und galoissch ist. Es ist $M_1 := \mathbb{Q}(\alpha)$ und $M_2 := \mathbb{Q}(\zeta)$, der fünfte Kreisteilungskörper, jeweils ein Zwischenkörper von $L|\mathbb{Q}$. In Teil (b) wurde bereits die Irreduzibilität und Normiertheit von $f$ festgestellt und in Teil (a) wurde $f(\alpha) = 0$ erhalten. Damit ist $f = \mu_{\mathbb{Q},\alpha}$, d.h., das Minimalpolynom von $\alpha$ über $\mathbb{Q}$. Es ist $[M_1 : \mathbb{Q}] = \deg(\mu_{\mathbb{Q},\alpha}) = \deg(f) = 5$, sodass laut Gradformel $5 = [M_1 : \mathbb{Q}]|[L : \mathbb{Q}]$. Für den fünften Kreisteilungskörper gilt $[M_2 : \mathbb{Q}] = \deg(\Phi_5(x) = x^4 + x^3 + x^2 + x + 1) = 4$ getreu bekannter Vorlesungsresultate. Mithilfe der Gradformel folgt die Teilbarkeitsaussage $4 = [M_2 : \mathbb{Q}]|[L : \mathbb{Q}]$ analog der vorherigen Betrachtung des Zwischenkörpers $M_2$. Somit muss $\mathrm{kgV}(4, 5) = 20|[L : \mathbb{Q}]$. Andererseits ist $[L : \mathbb{Q}] = [\mathbb{Q}(\alpha)(\zeta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] \leq [\mathbb{Q}(\zeta) : \mathbb{Q}][\mathbb{Q}(\alpha) : \mathbb{Q}] = 4 \cdot 5 = 20$ unter Verwendung der Gradformel, sodass insgesamt $[L : \mathbb{Q}] = 20$. Wie eingangs beschrieben gilt nun $|G| = [L : \mathbb{Q}] = 20$, sodass die Galoisgruppe von $L|\mathbb{Q}$ zumindest die Ordnung 20 hat. Um zu sehen, dass $G$ auch nicht-abelsch ist, führen wir einen Widerspruchsbeweis. Angenommen, $G$ wäre abelsch. Dann ist $U \trianglelefteq G$ für jede Untergruppe $U$ von $G$. Laut dem Hauptsatz der Galoistheorie ist dann der dazugehörige Fixkörper $L^U$ dergestalt, dass $L^U|\mathbb{Q}$ eine normale Erweiterung ist. Also ist für jede nicht-normale Erweiterung $M|\mathbb{Q}$, sodass $M$ Zwischenkörper von $L|\mathbb{Q}$ ist, $\mathrm{Gal}(L|M) \leq \mathrm{Gal}(L|\mathbb{Q})$ kein Normalteiler.

Für den oben definierten Zwischenkörper $M_1 := \mathbb{Q}(\alpha)$ von $L|\mathbb{Q}$ gilt $M_1 \subseteq \mathbb{R}$. Da $f(\alpha) = 0$ hat $f$ in $M_1$ bereits eine Nullstelle, und zerfällt über $M_1$, wenn $M_1|\mathbb{Q}$ normal wäre. Da aber $N \not\subseteq \mathbb{R}$, da $\zeta \notin \mathbb{R}$, kann $M_1$ nicht der Zerfällungskörper von $f$ sein. Alternativ führt man einen Widerspruchsbeweis zur Minimalitätseigenschaft des Zerfällungskörpers $L$ hinsichtlich der durch den Erweiterungsgrad definierten partiellen Ordnung. Damit besitzt $L|\mathbb{Q}$ einen Zwischenkörper $M$, nämlich $M_1$, sodass $M|\mathbb{Q}$ nicht normal ist. Der Zusatz zum Hauptsatz der Galoistheorie liefert nun, dass $\mathrm{Gal}(L|M) \leq \mathrm{Gal}(L|\mathbb{Q})$ kein Normalteiler ist. Das ist aber ein Widerspruchs zur eingangs zitierten Eigenschaft abelscher Gruppen, dass jede Untergruppe einer solchen bereits ein Normalteiler ist. Somit ist $\mathrm{Gal}(L|\mathbb{Q})$ nicht-abelsch.
(d) Wir zeigen, dass $\mathrm{Gal}(L|\mathbb{Q}) =: G$ keinen Normalteiler der Ordnung 4 hat. Angenommen, $N$ wäre ein Normalteiler der Ordnung 4 von $G$. Da $|G| = 20 = 5 \cdot 2^2$, ist $4 = 2^2$ die größte 2-Potenz, die die Gruppenordnung $|G| = 20$ teilt. Da 2 prim ist, ist $N$ dann eine 2-Sylowgruppe von $G$. Da $N$ zudem ein Normalteiler von $G$ ist, liefert ein bekanntes Korollar zum zweiten Sylowschen Satz, dass $N$ zudem die einzige 2-Sylowgruppe von $G$ ist. Damit ist $N$ zugleich die einzige Untergruppe von $G$, die Ordnung 4 hat. Damit ist $L^N = \mathbb{Q}(\alpha)$, da $(G : N) = |G|/|N| = 5 = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ nach dem Satz von Lagrange. Nach den Ergänzungssätzen zum Hauptsatz der Galoistheorie ist zudem $\mathbb{Q}(\alpha)|\mathbb{Q}$ in dieser Situation normal. Andererseits haben wir in Teil (c) gesehen, dass $\mathbb{Q}(\alpha)|\mathbb{Q}$ nicht normal ist. Das ist ein Widerspruch zur Annahme, dass $G$ einen Normalteiler der Ordnung 4 hat. Somit hat $G$ keinen Normalteiler der Ordnung 4. □

**Aufgabe 245 (F12T1A5)** Sei $L$ der Zerfällungskörper des Polynoms $f = x^5+5 \in \mathbb{Q}[x]$ über $\mathbb{Q}$. Ferner seien $\alpha = \sqrt[5]{-5}$ und $\zeta = \exp(2\pi i/5)$.
(a) Wir zeigen, dass $L = \mathbb{Q}(\alpha, \zeta)$. Nach Definition ist $L = \mathbb{Q}(N)$, wo $N$ die Nullstellenmenge von $f$ in $\mathbb{C}$ bezeichnet. Es gilt die Äquivalenz $f(x) = 0 \Leftrightarrow x^5 = -5 \Leftrightarrow x \in \{\alpha\zeta^k | 0 \leq k < 5\}$, wobei $k \in \mathbb{N}_0$. Somit ist $\mathbb{Q}(N) = \mathbb{Q}(\alpha, \zeta)$ zu zeigen. Laut Vorlesung reicht es aus, $\{\alpha, \zeta\} \subseteq \mathbb{Q}(N)$ und $N \subseteq \mathbb{Q}(\alpha, \zeta)$ zu zeigen. Für die erste Inklusion beachten wir, dass bereits $\alpha \in N$ und wegen $\alpha^5 = -5$ gilt $(\alpha^2)^5 = 25 \neq 0$, also $\alpha^2 = \sqrt[5]{25} \neq 0$ und somit auch $|\alpha| \neq 0$ wegen der Definitheit des komplexen Absolutbetrags. Also ist $\zeta = \alpha\zeta/\alpha \in \mathbb{Q}(N)$. Damit haben wir $\{\alpha, \zeta\} \subseteq \mathbb{Q}(N)$ nachgewiesen. Sei für die umgekehrte Inklusion $z \in N$ beliebig. Dann gibt es ein $k \in \{0, 1, 2, 3, 4\}$, sodass $z = \alpha\zeta^k$. Wegen $\alpha, \zeta \in \mathbb{Q}(\alpha, \zeta)$ ist somit auch $z \in \mathbb{Q}(\alpha, \zeta)$. Die Beliebigkeit von $z \in N$ liefert die angegebenen Inklusion. Mithin ist $\mathbb{Q}(\alpha, \zeta) = \mathbb{Q}(N) = L$.
(b) Wir zeigen nun, dass $L|\mathbb{Q}$ galoissch ist. Nach Definition ist $L$ der Zerfällungskörper des Polynoms $f = x^5 + 5 \in \mathbb{Q}[x]$ und somit nach Vorlesung bereits normal. Damit ist $L|\mathbb{Q}$ insbesondere algebraisch. Da $L = \mathbb{Q}(\alpha, \zeta)$, handelt es sich bei $L|\mathbb{Q}$ um eine von endlich vielen über $\mathbb{Q}$ algebraischen Elementen erzeugte Körpererweiterung, die somit laut Vorlesung endlich ist. Als endliche algebraische Erweiterung des Körpers $\mathbb{Q}$, der $\mathrm{char}(\mathbb{Q}) = 0$ genügt, ist $L|\mathbb{Q}$ separabel. Da $L|\mathbb{Q}$ normal und separabel ist, ist $L|\mathbb{Q}$ galoissch. Wir zeigen nun, dass $[L : \mathbb{Q}] = 20$. Es ist $f(\alpha) = 0$, $f$ normiert und nach Eisenstein zur Primzahl $p = 5$ irreduzibel, wenn wir $f$ infolge der Ganzzahligkeit seiner Koeffizienten als Element von $\mathbb{Z}[x]$ auffassen. Das Lemma von Gauss liefert dann die Irreduzibilität von $f$ über $\mathbb{Q}$, da $f$ als normiertes Polynom insbesondere primitives Polynom ist. Somit ist $f$ das Minimalpolynom von $\alpha$ über $\mathbb{Q}$ und

für den Zwischenkörper $\mathbb{Q}(\alpha)$ von $L|\mathbb{Q}$ gilt $[\mathbb{Q}(\alpha):\mathbb{Q}] = \deg(f) = 5$. Ein weiterer Zwischenkörper von $L|\mathbb{Q}$ ist der fünfte Kreisteilungskörper $\mathbb{Q}(\zeta)$, denn $\zeta \in L$ nach Teil (a). Für diesen gilt laut Vorlesung $[\mathbb{Q}(\zeta):\mathbb{Q}] = \deg(\Phi_5) = \phi(5) = 5-1 = 4$, wo $\phi$ die Eulersche $\Phi$-Funktion bezeichnet. Damit gilt laut Gradformel, dass $5 = [\mathbb{Q}(\alpha):\mathbb{Q}]|[L:\mathbb{Q}]$ und $4 = [\mathbb{Q}(\zeta):\mathbb{Q}]|[L:\mathbb{Q}]$, also $\mathrm{kgV}(4,5) = 20|[L:\mathbb{Q}]$. Andererseits liefert die Gradformel, dass $[L:\mathbb{Q}] = [\mathbb{Q}(\alpha,\zeta):\mathbb{Q}] = [\mathbb{Q}(\alpha)(\zeta):\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha):\mathbb{Q}] \leq [\mathbb{Q}(\zeta):\mathbb{Q}][\mathbb{Q}(\alpha):\mathbb{Q}] = 4\cdot 5 = 20$. Insgesamt gilt also $[L:\mathbb{Q}] = 20$.
(c) Wir zeigen, dass die Galoisgruppe $G$ von $L|\mathbb{Q}$ eine nicht-abelsche Gruppe der Ordnung 20 ist. Da $L|\mathbb{Q}$ galoissch ist, gilt $20 = [L:\mathbb{Q}] = |G|$. Angenommen, $G$ wäre abelsch. Dann wäre jede Untergruppe $U \leq G$ bereits ein Normalteiler. Nach dem Hauptsatz der Galoistheorie wäre der zu $U$ vermöge der Galois-Korrespondenz gehörende Zwischenkörper $L^U$ von $L|\mathbb{Q}$ dann mit der Eigenschaft, dass $L^U|\mathbb{Q}$ normal ist. Da $20 = 2^2\cdot 5$ in Primfaktorzerlegung, gibt es mindestens eine 2-Sylowgruppe von $G$, im Zeichen $P$. Da $G$ abelsch ist, gilt $P \trianglelefteq G$ und da $1 < |P| = 4 < 20 = |G|$ ist $P$ ein nicht-trivialer Normalteiler. Nach der Galois-Korrespondenz gibt es dann genau einen Zwischenkörper $M$ von $L|\mathbb{Q}$, der $[M:\mathbb{Q}] = (G:P) = |G|/|U| = 20/4 = 5$ erfüllt. In Teil (b) haben wir bereits gesehen, dass $\mathbb{Q}(\alpha)$ diesem Erweiterungsgraderfordernis genügt. Andererseits ist $\mathbb{Q}(\alpha)|\mathbb{Q}$ nicht normal. Denn $f = \mu_{\mathbb{Q},\alpha}$. Wäre $\mathbb{Q}(\alpha)|\mathbb{Q}$ normal, so müsste $f$ bereits über $\mathbb{Q}(\alpha)$ in Linearfaktoren zerfallen, mit anderen Worten, für den Zerfällungskörper $L$ von $f$ über $\mathbb{Q}$ müsste $L \subseteq \mathbb{Q}(\alpha)$ gelten. Da aber $[L:\mathbb{Q}] = 20 > [\mathbb{Q}(\alpha):\mathbb{Q}] = 5$ ist die vorher genannte Inklusion unmöglich. Damit war die Annahme falsch, und es ist $\mathbb{Q}(\alpha)|\mathbb{Q}$ nicht normal. Somit ist $P$ kein Normalteiler von $G$. Damit haben wir den Widerspruch zur Annahme, dass $G$ abelsch wäre, und $G$ ist stattdessen nicht-abelsch.
(d) Wir zeigen, dass $G$ einen Normalteiler der Ordnung 5 hat. Aus der Vorlesung ist bekannt, dass $\mathbb{Q}(\zeta)|\mathbb{Q}$ eine Galois-Erweiterung ist, insbesondere also normal ist. Damit handelt es sich bei $\mathbb{Q}(\zeta)$ um einen Zwischenkörper von $L|\mathbb{Q}$, der zu einer Galoisgruppe $U := \mathrm{Gal}(L|\mathbb{Q}(\zeta)) \leq G$ korrespondiert, die sogar ein Normalteiler von $G$ ist. Wegen $[\mathbb{Q}(\zeta):\mathbb{Q}] = 4 = (G:U) = |G|/|U| = 20/|U|$, folgt $|U| = 5$. Damit haben wir mit $U$ einen Normalteiler der Ordnung 5 von $G$ gefunden. Da $5 = 5^1$ zudem die höchste 5-Potenz ist, die 5 teilt, haben wir mit $U$ überdies eine 5-Sylowgruppe von $G$ vorliegen, die Normalteiler von $G$ ist. Ein Korollar zum zweiten Sylowschen Satz liefert nun, dass $U$ die einzige 5-Sylowgruppe von $G$, und damit die einzige Untergruppe der Ordnung 5 vom $G$, ist.
(e) Wir zeigen nun, dass die 2-Sylowgruppen von $G$ isomorph zu $\mathbb{Z}/4\mathbb{Z}$ sind. Sei $P$ eine 2-Sylowgruppe von $G$. Dann gilt $|P| = 2^2 = 4$ und $P$ ist als Gruppe von Primzahlquadratordnung insbesondere abelsch. Nach dem Hauptsatz über endlich erzeugte (insbesondere also endliche) abelsche Gruppen gilt $P \simeq \mathbb{Z}/4\mathbb{Z}$ oder $P \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Wir spezialisieren uns zunächst darauf, $P = \mathrm{Gal}(L|\mathbb{Q}(\alpha))$ zu betrachten. Da je zwei 2-Sylowgruppen zueinander konjugiert sind, bleibt der Isomorphiertyp der 2-Sylowgruppen von dieser Einschränkung unberührt. Das fünfte Kreisteilungspolynom $\Phi_5$ ist aber nicht nur über $\mathbb{Q}$, sondern auch über $\mathbb{Q}(\alpha)$ irreduzibel, denn andernfalls gäbe es ein normiertes und irreduzibles Polynom $g \in \mathbb{Q}(\alpha)[x]$, sodass $g(\zeta) = 0$ und $g|\Phi_5$. Dann würde aber für $[L:\mathbb{Q}]$ gelten, dass $[L:\mathbb{Q}] = [L:\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha):\mathbb{Q}] = 5\deg(g) < 20$ im Widerspruch zu $[L:\mathbb{Q}] = 20$. Da mit $\zeta$ auch $\zeta^2$ Nullstelle des irreduziblen $\Phi_5 \in \mathbb{Q}(\alpha)[x]$ sind, setzen wir $P \ni \mathrm{id}|_{\mathbb{Q}(\alpha)} \to L$ nach

$L$ fort - zu einem $\sigma \in P$, indem wir $\sigma(\zeta) = \zeta^2$ setzen. Man sieht, dass $\sigma \neq \mathrm{id}$ und $\sigma^2(\zeta) = \zeta^4 \neq \zeta$, sodass $\mathrm{ord}(\sigma) > 2$ in $P$ gelten muss. Wegen $|P| = 4$ ist nur $\mathrm{ord}(\sigma) = 4$ möglich, also ist $P$ zyklisch von Ordnung 4. Mit dem $P = \mathrm{Gal}(L|\mathbb{Q}(\alpha))$ sind wie oben beschrieben bereits alle 2-Sylowgruppen von $G$ zyklisch von Ordnung 4. □

**Aufgabe 246 (F19T2A5)** Sei $L|\mathbb{Q}$ eine endliche Galoiserweiterung mit Galoisgruppe $G = \mathrm{Gal}(L|\mathbb{Q}) \simeq S_3 \times H$, wo $|H| = 88$.
(a) Wir zeigen, dass $M := L \cap \mathbb{Q}(\sqrt[5]{5}) = \mathbb{Q}$. Da $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[5]{5})$ und $\mathbb{Q} \subseteq L$, ist $\mathbb{Q} \subseteq M$ klar. Für die umgekehrte Inklusion bemerken wir, dass $f = x^5 - 5 \in \mathbb{Q}[x]$ normiert ist und $f(\sqrt[5]{5}) = 0$ gilt. Nach dem Eisensteinkriterium zur Primzahl 5 ist $f$ ferner über $\mathbb{Q}$ irreduzibel und somit insgesamt das Minimalpolynom von $\sqrt[5]{5}$ über $\mathbb{Q}$. Laut Vorlesung gilt $[\mathbb{Q}(\sqrt[5]{5}) : \mathbb{Q}] = \deg(f) = 5$. Da $M$ Zwischenkörper von $L|\mathbb{Q}$ ist, gilt nach der Gradformel einerseits $[M : \mathbb{Q}]|[L : \mathbb{Q}] = 6 \cdot 88$. Andererseits ist $M$ auch Zwischenkörper von $\mathbb{Q}(\sqrt[5]{5})|\mathbb{Q}$, sodass die Gradformel wiederum $[M : \mathbb{Q}]|[\mathbb{Q}(\sqrt[5]{5}) : \mathbb{Q}] = 5$ liefert. Somit gilt $[M : \mathbb{Q}]|\mathrm{ggT}(5, 6 \cdot 88) = 1$. Damit ist bereits $M = \mathbb{Q}$ aus Dimensionsgründen.
(b) Wir zeigen nun, dass es einen Zwischenkörper $K$ von $L|\mathbb{Q}$ gibt, sodass $[K : \mathbb{Q}] = 8$ und $K$ der Zerfällungskörper eines Polynoms vom Grad 8 über $\mathbb{Q}$ ist. Als Zwischenkörper vom Erweiterungsgrad 8 über $\mathbb{Q}$ korrespondiert $K$ gemäß des Hauptsatzes der Galoistheorie zu einer Untergruppe $U$ von $G$, die Index 8 in $G$ hat, $(G : U) = 8$. Mit dem Satz von Lagrange sehen wir, dass $|G| = 6 \cdot 11$. Wir zeigen, dass eine solche Untergruppe existiert. Dazu betrachten wir Untergruppen $U$ der Form $S_3 \cdot V$, wobei $V$ eine Untergruppe von $H$ der Ordnung 11 sein soll. Da $U$ als äußeres direktes Produkt von Gruppen angesetzt wird, gilt $|U| = |S_3||V| = 6 \cdot 11$, wenn ein $V$ wie gewünscht existiert. Da $|H| = 2^3 \cdot 11$, suchen wir eine 11-Sylowgruppe von $H$. Sei $\nu$ die Anzahl der 11-Sylowgruppen von $H$. Nach dem dritten Sylowschen Satz folgt $\nu|8$ und $\nu \equiv 1 \bmod(11)$. Die erste Bedingung liefert $\nu < 9$, sodass die zweite Bedingung nur noch $\nu = 1$ zulässt. Somit gibt es genau eine 11-Sylowgruppe $V$ von $H$. Diese ist dann ein Normalteiler von $H$. Da $S_3$ trivialer Normalteiler von $S_3$ ist, gilt $S_3 \times V \trianglelefteq S_3 \times H$, denn für beliebiges $(a, b) \in S_3 \times V, (c, d) \in S_3 \times H$ ist $(c, d)^{-1} \cdot (a, b) \cdot (c, d) = (c^{-1}ac, d^{-1}bd) \in S_3 \times V$, da $S_3 \trianglelefteq S_3$ und $V \trianglelefteq H$. Nach einem Ergänzungssatz zum Hauptsatz der Galoistheorie ist der zu $S_3 \times V$ gehörige Zwischenkörper von $L|\mathbb{Q}$, nämlich der Fixkörper $K := L^{S_3 \times V}$, dergestalt, dass $K|\mathbb{Q}$ normal ist. Da $K$ als Zwischenkörper einer separablen Erweiterung ebenfalls eine separable Erweiterung $K|\mathbb{Q}$ liefert, ist $K|\mathbb{Q}$ auch eine endliche Galoiserweiterung. Als endliche und separable Erweiterung gibt es laut dem Satz vom primitiven Element ein $\alpha \in K$, sodass $K = \mathbb{Q}(\alpha)$. Sei $f = \mu_{\mathbb{Q},\alpha}$ das Minimalpolynom von $\alpha$ über $\mathbb{Q}$. Es ist $\deg(\mu_{\mathbb{Q},\alpha}) = [K : \mathbb{Q}] = (G : U) = |S_3 \times H|/|S_3 \times V| = 8$. Damit ist $f$ ein Polynom vom Grad 8 in $\mathbb{Q}[x]$. Da $\alpha$ eine Nullstelle von $f$ ist, zerfällt $f$ über $\mathbb{Q}(\alpha)$ bereits in Linearfaktoren. Das zeigt, dass der Zerfällungskörper von $f$ bereits $\mathrm{Zerf}(f) \subseteq \mathbb{Q}(\alpha) = K$ erfüllt. Andererseits ist $\alpha$ als Nullstelle von $f$ bereits in $\mathrm{Zerf}(f)$ enthalten. Somit gilt auch $\mathbb{Q}(\alpha) \subseteq \mathrm{Zerf}(f)$. Insgesamt haben wir also $K = \mathrm{Zerf}(f)$, d.h., es gibt einen Zwischenkörper $K$ mit den gewünschten Eigenschaften betreffend den Erweiterungsgrad von $K$ über $\mathbb{Q}$ und den Zerfällungskörpereigenschaft. □

**Aufgabe 247 (F17T2A5)** Sei $K|\mathbb{Q}$ eine Galois-Erweiterung mit nicht-abelscher Galoisgruppe der Ordnung 55. Wir zeigen, dass es genau einen echten Zwischenkörper $M$ von $K|\mathbb{Q}$ gibt, sodass $M|\mathbb{Q}$ galoissch ist. Bezeichne mit $G$ die Galoisgruppe von $K|\mathbb{Q}$. Es ist $|G| = 5 \cdot 11$ und wir bezeichnen mit $\nu_p$ für eine Primzahl $p$ die Anzahl der $p$-Sylowgruppen von $G$. Für die einzigen beiden Primteiler 5 und 11 von $|G|$ finden wir mithilfe des dritten Sylowschen Satzes $\nu_5|11$ und $\nu_5 \equiv 1 \bmod(5)$ sowie $\nu_{11}|5$ und $\nu_{11} \equiv 1 \bmod(5)$. Es ist $\nu_{11} < 6$ und somit nach der zweiten Bedingung $\nu_{11} = 1$. Damit hat $G$ nur eine 11-Sylowgruppe $P$, die nach dem zweiten Sylowschen Satz ein Normalteiler von $G$ ist. Für $\nu_5$ sind die Fälle $\nu_5 = 1$ und $\nu_5 = 11$ zu unterscheiden, die unmittelbar aus den Bedingung an $\nu_5$ laut dem dritten Sylowschen Satz (s.o.) resultieren. Falls $\nu_5 = 1$, dann gibt es auch nur eine 5-Sylowgruppe von $G$, bezeichnet mit $Q$, die ebenfalls ein Normalteiler von $G$ ist. Da $\mathrm{ggT}(|P|, |Q|) = \mathrm{ggT}(5, 11) = 1$, gilt $P \cap Q = \{e_G\}$. Wegen $P, Q \trianglelefteq G$ ist das innere direkte Produkt $PQ \leq G$ und es gilt $|PQ| = |P||Q| = 5 \cdot 11 = 55$. Damit ist bereits $PQ = G$. Da ferner $PQ \simeq P \times Q$ isomorph zum äußeren direkten Produkt von $P \& Q$ ist, ist $G \simeq P \times Q$. Da $P$ und $Q$ von Primzahlordnung jeweils sind, sind $P, Q$ selbst jeweils zyklisch, also insbesondere abelsch. Damit ist $G \simeq P \times Q \simeq \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/55\mathbb{Z}$, wobei die letztgenannte Isomorphie aus dem Chinesischen Restsatz für Gruppen folgt, wenn wir $\mathrm{ggT}(5, 11) = 1$ beachten. Also ist $G$ isomorph zu einer zyklischen Gruppe der Ordnung 55, also selbst zyklisch. Da $G$ dann abelsch ist, haben wir einen Widerspruch zur Voraussetzung, dass $G$ nicht-abelsch ist. Somit kann der Fall $\nu_5 = 1$ nicht auftreten und es gilt stattdessen $\nu_5 = 11$. Sei nun $M := K^P$ der Fixkörper von der 11-Sylowgruppe $P$ von $G$. Da $P \trianglelefteq G$, ist $M|\mathbb{Q}$ nach einem Ergänzungssatz zum Hauptsatz der Galoistheorie normal. Da $M$ zudem Zwischenkörper der endlichen Galoiserweiterung $K|\mathbb{Q}$ ist, ist $M|\mathbb{Q}$ separabel. Also ist $M|\mathbb{Q}$ galoissch. Da $[M : \mathbb{Q}] = (G : P) = |G|/|P| = 5$, handelt es sich bei $M$ um einen echten Zwischenkörper von $K|\mathbb{Q}$. Wir müssen zeigen, dass dies auch der einzige Zwischenkörper mit den geforderten Eigenschaften ist. Angenommen, $M'$ sei ein weiterer, von $M$ verschiedener echter Zwischenkörper von $K|\mathbb{Q}$, sodass $M'|\mathbb{Q}$ galoissch ist. Dann ist $M'|\mathbb{Q}$ insbesondere normal, und $P' := \mathrm{Gal}(L|M') \trianglelefteq G$ nach dem Hauptsatz der Galoistheorie und zugehörigem Ergänzungssatz. Insbesondere ist dann $|P'|$ ein echter Teiler der Gruppenordnung $|G|$. Somit ist nur möglich, dass $|P'| = 11$ oder $|P'| = 5$. Im ersten Fall, ist $P'$ auch eine 11-Sylowgruppe von $G$. Dann ist $P' = P$, da $P$ die einzige 11-Sylowgruppe von $G$ ist. Damit aber die Untergruppen von $G$ bijektiv zu den Zwischenkörpern von $K|\mathbb{Q}$ korrespondierem, ist $M' = K^{P'} = K^P = M$, im Widerspruch dazu, dass $M' \neq M$. Falls $|P'| = 5$, dann ist $P'$ eine 5-Sylowgruppe von $G$. Da $P' \trianglelefteq G$, ist nach der bereits oben genannten Folgerung aus dem zweiten Sylowschen Satz $P'$ auch die einzige 5-Sylowgruppe von $G$. Es gilt also $\nu_5 = 1$, im Widerspruch zu unserem Ergebnis von weiter oben, dass $\nu_5 = 11 \neq 1$. Somit war die Annahme, es gäbe einen weiteren von $M$ verschiedenen Zwischenkörper $M'$ von $K|\mathbb{Q}$ mit der Eigenschaft, dass $M'|\mathbb{Q}$ galoissch ist, falsch. Damit ist der oben definierte Zwischenkörper $M$ tatsächlich der einzige Zwischenkörper, der den Anforderungen der Aufgabenstellung genügt. □

**Aufgabe 248 (H19T1A2)** Sei $f \in \mathbb{Q}[x]$ ein irreduzibles Polynom, das sowohl reelle als auch echt-komplexe Nullstellen hat. Zu zeigen ist, dass $\mathrm{Gal}(f|\mathbb{Q})$ nicht-

abelsch ist. Sei $N \subseteq \mathbb{C}$ die Nullstellenmenge von $f$ in $\mathbb{C}$. Dann ist $\mathrm{Gal}(f|\mathbb{Q}) = \mathrm{Gal}(L|\mathbb{Q})$, wobei $L = \mathbb{Q}(N)$ der Zerfällungskörper von $f$ über $\mathbb{Q}$ ist. Da $f$ Polynom ist, ist $|N| < \infty$ und somit eine endliche Menge von über $\mathbb{Q}$ algebraischen Elementen. Da $L$ Zerfällungskörper eines Polynoms aus $\mathbb{Q}[x]$ ist, ist $L|\mathbb{Q}$ normal. Da die Erweiterung $L|\mathbb{Q}$ von endlich vielen, über $\mathbb{Q}$ algebraischen Elementen erzeugt wird, ist $L|\mathbb{Q}$ endlich und algebraisch. Da $\mathrm{char}(\mathbb{Q}) = 0$, ist $L|\mathbb{Q}$ separabel, also ist $L|\mathbb{Q}$ in der Tat galoissch. Seien nun $\alpha \in \mathbb{R}$ und $\beta \notin \mathbb{R}$ zwei Nullstelle von $f$. Dann ist $\alpha, \beta \in L$ und es ist $\mathbb{Q}(\alpha)$ und $\mathbb{Q}(\beta)$ jeweils ein Zwischenkörper von $L|\mathbb{Q}$. Da $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$ und $\mathbb{Q}(\beta) \ni \beta \notin \mathbb{R}$ handelt es sich hierbei um verschiedene Zwischenkörper von $L|\mathbb{Q}$. Sei $\iota : \mathbb{C} \to \mathbb{C}, z \mapsto \bar{z}$ die komplexe Konjugation und $\sigma := \iota|_L$ die Einschränkung dieser auf $L$. Da $L|\mathbb{Q}$ galoissch ist, beschränkt sich $\sigma$ zu einem $\mathbb{Q}$-Automorphismus von $L$. Zudem setzen wir $\tau : \mathbb{Q} \to \mathbb{C}, x \mapsto x$ nach $L$ durch $\tau(\alpha) = \beta, \tau(\beta) = \alpha$ fort (und $\tau(x) = x$ für alle $x \in N \setminus \{\alpha, \beta\}$). Auch $\tau$ beschränkt sich zu einem $\mathbb{Q}$-Automorphismus von $L$, da $L|\mathbb{Q}$ normal ist. Nun ist $\sigma(\tau(\alpha)) = \sigma(\beta) = \bar{\beta}$ aber $\tau(\sigma(\alpha)) = \tau(\alpha) = \beta$, da $\alpha \in \mathbb{R}$. Da $\beta \notin \mathbb{R}$ gilt $\beta \neq \bar{\beta}$, sodass $\sigma \circ \tau \neq \tau \circ \sigma$. Damit ist die Galoisgruppe von $f$ nicht-abelsch. □

**Aufgabe 249 (F15T1A5)** (a) Sei $f \in \mathbb{Q}[x]$ ein irreduzibles Polynom vom Grad $n \geq 1$ und $K$ ein Zerfällungskörper von $f$ sowie $G := \mathrm{Gal}(K|\mathbb{Q})$. Wir zeigen: Ist $G$ abelsch, so ist $|G| = n$. Zunächst ist $K|\mathbb{Q}$ normal, da $K$ der (bis auf Isomorphie eindeutige) Zerfällungskörper des Polynoms $f$ ist. Sei $N$ die Nullstellenmenge von $f$ in $\mathbb{C}$. Da $\deg(f) = n < \infty$, ist $N$ endlich und jedes Element aus $N$ ist algebraisch. Als von endlich vielen über $\mathbb{Q}$ algebraischen Elementen erzeugte Erweiterung, ist $K = \mathbb{Q}(N)|\mathbb{Q}$ dann algebraisch und endlich. Da $\mathrm{char}(\mathbb{Q}) = 0$ ist die Körpererweiterung $K|\mathbb{Q}$ laut Vorlesung separabel. Insgesamt haben ist $K|\mathbb{Q}$ galoissch. Angenommen, $|G| > n$, aber $G$ ist abelsch. Es ist $[K : \mathbb{Q}] = |G| = n$ und $\alpha$ eine Nullstelle von $f$. Zudem können wir $\beta \in K$ so wählen, dass $\beta \notin \mathbb{Q}(\alpha)$, denn $\deg(\mu_{\mathbb{Q}(\alpha)}) \leq \deg(f) = n < [K : \mathbb{Q}]$. Nach dem Fortsetzungssatz gibt es ein $\sigma \in G$ mit $\sigma(\alpha) = \beta$. Wir betrachten nun $\tau \in \mathrm{Gal}(K|\mathbb{Q}(\alpha))$ beliebig. Dann gilt $\tau(\beta) = \tau(\sigma(\alpha)) = \sigma(\tau(\alpha)) = \sigma(\alpha) = \beta$, wobei wir verwendet haben, dass $G$ nach Voraussetzung abelsch ist. Die soeben bewiesene Gleichung zeigt, dass $\beta \in K^{\mathrm{Gal}(K|\mathbb{Q}(\alpha))} = \mathbb{Q}(\alpha)$, im Widerspruch dazu, dass $\beta \notin \mathbb{Q}(\alpha)$. Somit war die Annahme, $|G| > n$ falsch, und es gilt $|G| \leq n$. Wir zeigen nun, dass auch $|G| < n$ nicht möglich ist. Denn dann ist einerseits $[K : \mathbb{Q}] = |G| < n$ und andererseits für $\alpha \in K$ eine Nullstelle von $f$ ist $f$ bis auf eine multiplikative Einheit das Minimalpolynom von $\alpha$. Somit ist $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f) = n$. Da $\mathbb{Q}(\alpha)$ ein Zwischenkörper von $K|\mathbb{Q}$ ist, gilt $[\mathbb{Q}(\alpha) : \mathbb{Q}] | [K : \mathbb{Q}]$, also insbesondere $n = [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq [K : \mathbb{Q}] = |G|$! Das ist ein Widerspruch zur Annahme, $|G| < n$. Damit ist nur $|G| = n$ möglich.
(b) Sei $L = \mathbb{Q}(\sqrt{2}, i)|\mathbb{Q}$. Wir bestimmen zunächst den Erweiterungsgrad $[L : \mathbb{Q}]$. Es ist $f = x^2 - 2 \in \mathbb{Q}[x]$ normiert und nach dem Eisensteinkriterium zur Primzahl $p = 2$ irreduzibel über $\mathbb{Q}$. Zudem ist $f(\sqrt{2}) = 0$, sodass $f$ das Minimalpolynom von $\sqrt{2}$ über $\mathbb{Q}$ ist. Es gilt dann $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = \deg(f) = 2$. Es ist $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$. Das Polynom $g = x^2 + 1 \in \mathbb{Q}[x]$ hat die beiden Nullstellen $i$ und $-i$, ist also als Polynom vom Grad 2 über $\mathbb{R}$ und damit erst recht über den Teilkörper $\mathbb{Q}(\sqrt{2})$ irreduzibel. Damit ist $g$ das Minimalpolynom von $i$ über $\mathbb{Q}(\sqrt{2})$ und es gilt $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})] = \deg(g) = 2$. Mithilfe der Gradformel finden wir $[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2^2 = 4$. Da

$i, \sqrt{2}$ algebraisch über $\mathbb{Q}$ sind, ist die Erweiterung $L|\mathbb{Q}$ eine endliche und algebraische Erweiterung. Da zudem $\text{char}(\mathbb{Q}) = 0$, ist $L|\mathbb{Q}$ separabel. Nach dem Satz vom primitiven Element, gibt es also ein $\alpha \in L$, sodass $L = \mathbb{Q}(\alpha)$. Wir zeigen, dass $\alpha = \sqrt{2}+i$ ein primitives Element der Erweiterung $L|\mathbb{Q}$ ist. Denn $\sqrt{2}+i \in L$ einerseits und andererseits ist $\alpha^{-1} = (\sqrt{2}+i)^{-1} = \sqrt{2}-i \in \mathbb{Q}(\alpha)$. Mit $\sqrt{2}+i, \sqrt{2}-i \in \mathbb{Q}(\alpha)$ ist auch $\sqrt{2} = 0.5(\alpha+\alpha^{-1})$ und $i = 0.5(\alpha-\alpha^{-1}) \in \mathbb{Q}(\alpha)$. Damit haben wir $\mathbb{Q}(\alpha) \supseteq L$ nachgewiesen. Insgesamt gilt $L = \mathbb{Q}(\alpha)$. Nun bestimmen wir das Minimalpolynom von $\alpha$ über $\mathbb{Q}$. Es gilt die Implikation $\alpha = \sqrt{2}+i \Rightarrow (\alpha-\sqrt{2})^2 = -1 \Rightarrow \alpha^2+3 = 2\sqrt{2}\alpha \Rightarrow \alpha^4-2\alpha^2+9 = 0$. Damit ist $\alpha$ Nullstelle von $p = x^4-2x^2+9 \in \mathbb{Q}[x]$. $p$ ist irreduzibel über $\mathbb{Q}$, denn andernfalls wäre das Minimalpolynom $q$ von $\alpha$ ein echter Teiler von $p$ in $\mathbb{Q}[x]$ mit $\deg(q) < \deg(f)$. Da aber $\deg(q) = [L:\mathbb{Q}] = 4$, ist dies unmöglich. Somit ist $f$ irreduzibel über $\mathbb{Q}$. Da $f$ zudem normiert ist und per Konstruktion $\alpha$ als Nullstelle hat, ist $f$ das Minimalpolynom von $\alpha$. Die übrigen Nullstellen von $f$ sind gegeben durch $-\sqrt{2}+i, -\sqrt{2}-i$ und $\sqrt{2}-i$, wie man leicht durch Nachrechnen verifiziert. Diese liegen jeweils in $L$. Somit ist $\mathbb{Q}(N) = \mathbb{Q}(\alpha)$, wenn $N$ die Nullstellenmenge von $p$ bezeichnet. Damit ist $L$ bereits der Zerfällungskörper von $p$ und $L|\mathbb{Q}$ ist somit normal. Da $L|\mathbb{Q}$ normal und separabel ist, ist $L|\mathbb{Q}$ galoissch. Für die Ordnung der Galoisgruppe $G = \text{Gal}(L|\mathbb{Q})$ gilt laut Vorlesung $|G| = [L:\mathbb{Q}] = 4$. Als Gruppe von Primzahlquadratordnung ist $G$ abelsch. Nach dem Hauptsatz über endlich erzeugte abelsche Gruppe ist $G$ dann entweder vom isomorphietyp $G \simeq \mathbb{Z}/4\mathbb{Z}$ oder $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Wir zeigen, dass $G \simeq \mathbb{Z}/4\mathbb{Z}$ nicht möglich ist. Denn als zyklische Gruppe hat $G$ andernfalls zu jedem Teiler $d$ der Gruppenordnung 4 genau eine Untergruppe der Ordnung $d$. Speziell für $d = 2$ hat $G$ also genau eine Untergruppe der Ordnung 2. Diese korrespondiert laut dem Hauptsatz der Galoistheorie zum (einzigen) Zwischenkörper $M$ von $L|\mathbb{Q}$ mit Erweterungsgrad $[M:\mathbb{Q}] = 4/2 = 2$. Andererseits sind $\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(i)$ zwei verschiedene Zwischenkörper von $\mathbb{Q}(\sqrt{2}, i) = L$, die jeweils den Erweiterungsgrad 2 über $\mathbb{Q}$ besitzen. Wegen des Hauptsatzes der Galoistheorie sind somit $\text{Gal}(L|\mathbb{Q}(i))$ und $\text{Gal}(L|\mathbb{Q}(\sqrt{2}))$ zwei verschiedene Untergruppen von $G$ vom Index 2, also von Ordnung $4/2 = 2$. Das ist ein Widerspruch dazu, dass $G$ nur eine derartige Untergruppe besitzt. Also war die Annahme $G \simeq \mathbb{Z}/4\mathbb{Z}$ falsch und $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ stattdessen. Insbesondere ist $G$ abelsch, nicht aber zyklisch. Damit ist die Aufgabe beendet. □

**Aufgabe 250** Sei $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}, i)$.
(a) Wir zeigen, dass $[L:\mathbb{Q}] = 8$. Mittels Eisensteinkriterium zu den Primzahlen $p = 2$ und $q = 3$ verifiziert man leicht, dass $f_2 = x^2-2, f_3 = x^2-3 \in \mathbb{Q}[x]$ jeweils irreduzibel über $\mathbb{Q}$ sind. Das Polynom $g = x^2+1 \in \mathbb{Q}[x]$ hat die beiden komplexen Nullstellen $\pm i$ und ist als Polynom vom Grad 2 mangels Nullstellen in $\mathbb{Q}$ über den rationalen Zahlen irreduzibel. Es gilt $f_p(\sqrt{p}) = 0$ für $p \in \{2,3\}$. Da $f_2, f_3, g$ jeweils normiert und irreduzibel über $\mathbb{Q}$ sind und die Nullstellen $\sqrt{2}, \sqrt{3}, i$ (jeweils) besitzen, handelt es sich in bei jedem der Polynome um die zu diesen Nullstellen gehörigen Minimalpolynome. Somit ist $[\mathbb{Q}(\alpha):\mathbb{Q}] = 2$ für $\alpha \in \{\sqrt{2}, \sqrt{3}, i\}$. Da 2 und 3 zwei verschiedene, quadratfreie positive Ganzzahlen sind, ist $[\mathbb{Q}(\sqrt{2}, \sqrt{3}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{2}):\mathbb{Q}][\mathbb{Q}(\sqrt{3}):\mathbb{Q}] = 4$. Da $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{R}$, ist $p$ ebenfalls über $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ irreduzibel, also das Minimalpolynom von $i$ über diesem Körper. Somit ist $[L:\mathbb{Q}] = [L:\mathbb{Q}(\sqrt{2}, \sqrt{3})][\mathbb{Q}(\sqrt{2}, \sqrt{3}):\mathbb{Q}] = 2 \cdot 4 = 8$, wie behauptet.

(b) Wir zeigen, dass $L|\mathbb{Q}$ galoissch ist. Da $L|\mathbb{Q}$ von den drei, über $\mathbb{Q}$ algebraischen Elementen $\sqrt{2}, \sqrt{3}, i$ erzeugt wird, ist $L|\mathbb{Q}$ endlich und algebraisch. Da $\mathrm{char}(\mathbb{Q})$, folgt insgesamt, dass $L|\mathbb{Q}$ endlich und separabel ist. Zudem ist $L$ der Zerfällungskörper von $F = (x^2+1)(x^2-2)(x^2-3) \in \mathbb{Q}[x]$, denn dieses Polynom hat gerade die Nullstellenmenge $N = \{\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}, -i, i\} \subseteq L$. Damit ist $L|\mathbb{Q}$ auch normal. Als normale und separable Erweiterung von endlichen Erweiterungsgrad 8 handelt es sich bei $L|\mathbb{Q}$ um eine endliche galoissche Erweiterung.
(c) Wir zeigen, dass $G := \mathrm{Gal}(L|\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^3$. Für die Galoisgruppe $G$ gilt in jedem Fall $|G| = 8$. Somit ist $G$ eine 2-Gruppe. Durch $\sigma(\sqrt{2}) = -\sqrt{2}, \sigma(\sqrt{3}), \sigma(i) = i$ ist ein $\sigma \in G$ festgelegt. Analog verfahren erhalten wir $\tau, \rho \in G$, indem wir $\tau(\sqrt{3}) = -\sqrt{3}$ bzw $\rho(i) = -i$ fordern und die verbleibenden $\sqrt{2}, i$ bzw. $\sqrt{2}, \sqrt{3}$ von $\tau$ bzw. $\rho$ jeweils fixiert werden. Es ist leicht zu sehen, dass $\mathrm{ord}(\sigma) = \mathrm{ord}(\rho) = \mathrm{ord}(\tau) = 2$ und $\langle \sigma, \rho, \tau \rangle$ eine abelsche Gruppe ist, die drei Untergruppen der Ordnung 2 besitzt. Somit ist nur $\langle \sigma, \rho, \tau \rangle \simeq (\mathbb{Z}/2\mathbb{Z})^3$ möglich. Wegen $G \geq \langle \sigma, \rho, \tau \rangle$ gilt bereits Gleichheit aus Ordnungsgründen. Infolge der Transitivität von Gruppenisomorphien ist $G \simeq (\mathbb{Z}/2\mathbb{Z})^3$. $\square$