Satz (14.6)

Sei R ein Ring, $I_1, \dots, I_m$ paarweise teilerfremde Ideale in R und $I = I_1 \cdot \dots \cdot I_m$. Dann gibt es einen **Isomorphismus** von Ringen

$$\bar{\phi} : R/I \longrightarrow (R/I_1) \times \dots \times (R/I_m)$$

mit

$$\bar{\phi}(a + I) = (a + I_1, \dots, a + I_m) \quad \text{für alle } a \in R.$$

Lemma (14.10)

Seien R und S Ringe. Dann gilt

- (i) $(R \times S)^\times = R^\times \times S^\times$
- (ii) Ist $\phi : R \rightarrow S$ ein Isomorphismus von Ringen, dann gilt $\phi(R^\times) = S^\times$. Insbesondere sind die Einheitengruppen $R^\times$ und $S^\times$ also isomorph.

Proposition (14.11)

Sind m, n teilerfremd und $m, n \geq 2$. Dann gilt für die Eulersche φ -Funktion die Rechenregel $\varphi(mn) = \varphi(m)\varphi(n)$.

Beweis von Prop. 14.11

geg: $m, n \in \mathbb{N}$ teilerfremd

bekannt: $\forall n \in \mathbb{N}: |(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$

Chinesischer Restsatz $\Rightarrow \exists$ Isomorphismus von Ringen

$$\mathbb{Z}/(mn)\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \quad \text{Lemma 14.10} \Rightarrow$$

$\exists$ Isom. von Gruppen $(\mathbb{Z}/(mn)\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^\times$

$$\cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times \Rightarrow \varphi(mn) = |(\mathbb{Z}/(mn)\mathbb{Z})^\times| =$$

$$|(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times| = |(\mathbb{Z}/m\mathbb{Z})^\times| \cdot |(\mathbb{Z}/n\mathbb{Z})^\times|$$

$$= \varphi(m) \cdot \varphi(n) \quad \square$$

Anwendungsbeispiel :

Satz 14.13

$$(\mathbb{Z}/15\mathbb{Z})^{\times} \cong (\mathbb{Z}/3\mathbb{Z})^{\times} \times (\mathbb{Z}/5\mathbb{Z})^{\times} \cong \mathbb{Z}/3\mathbb{Z} \text{ und } \mathbb{Z}/5\mathbb{Z}$$

↑ Chin. Restsatz

2.) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ Dies ist keine zyklische Gruppe, denn es gibt nur Elemente der Ordnungen 1, 2 und 4, kein Element der Ordnung 8.

□

Der Exponent einer Gruppe

Der **Exponent** $\exp(G)$ einer Gruppe G ist die kleinste Zahl $n \in \mathbb{N}$ mit der Eigenschaft $g^n = e$ für alle $g \in G$. Existiert keine natürliche Zahl mit dieser Eigenschaft, dann setzt man $\exp(G) = +\infty$.

Proposition (14.12)

Sei G eine endliche **abelsche** Gruppe vom Exponenten n . Dann existiert in G ein Element der Ordnung n .

Beweis von Prop 14.12

geg. endliche abelsche Gruppe G , $n = \exp(G)$

zzg: $\exists g \in G$ mit $\text{ord}(g) = n$

Hauptsatz über endl. abelsche Gruppen $\Rightarrow$ o. B. d. A.

$G = \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_r\mathbb{Z}$ mit $r, m_1, \dots, m_r \in \mathbb{N}$

Sei $l = \text{kgV}(m_1, \dots, m_r) \Rightarrow l \bar{a} = \bar{0} \quad \forall \bar{a} \in \mathbb{Z}/m_k\mathbb{Z}, 1 \leq k \leq r$

$\Rightarrow l g = 0_G \quad \forall g \in G \rightarrow n \leq l$

Beh. Für $g = (\bar{1}, \dots, \bar{1})$ gilt $\text{ord}(g) = l$ (Daraus folgt auch, dass $\exp(G) \geq l$ und insg. $n = \exp(G) = l$ gilt.)

klar. Für jedes Vielfache k von l gilt $kg = 0_G$

umgekehrt: Sei $k \in \mathbb{Z}$ mit $kg = 0_G \Rightarrow k \cdot (1 + m_j \mathbb{Z}) = 0 + m_j \mathbb{Z}$

für $1 \leq j \leq r \Rightarrow k \in m_j \mathbb{Z} \Rightarrow k$ ist Vielfaches von $m_1, \dots, m_r$

$\Rightarrow k$ ist Vielfaches von $\text{kgV}(m_1, \dots, m_r) = l$
Insgesamt ergibt sich daraus die Behauptung,
da allgemein $l = \text{ord}(g) \Leftrightarrow (kg = 0_G \text{ genau}$
dann, wenn $k \in \mathbb{Z}$ ein Vielfaches von l ist $\forall k \in \mathbb{Z}$)
 $\square$

Satz (14.13)

Sei K ein Körper und U eine endliche Untergruppe der multiplikativen Gruppe $K^\times$. Dann ist U **zyklisch**. Insbesondere ist die multiplikative Gruppe eines endlichen Körpers immer eine zyklische Gruppe.

Folgerung (14.14)

Ist p eine Primzahl, dann gilt $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$.

Eine Zahl $a \in \mathbb{Z}$ mit der Eigenschaft $(\mathbb{Z}/p\mathbb{Z})^\times = \langle a + p\mathbb{Z} \rangle$ wird **Primitivwurzel modulo p** genannt.

Beweis von Satz 14.13:

geg: Körper K , $U \leq K^\times$ endliche Untergruppe
z.zg. U ist zyklisch. Sei $n = |U|$ und $d = \exp(U)$

Lagrange $\Rightarrow a^n = 1_K \quad \forall a \in U \Rightarrow d = \exp(U) \leq n$.

Nach Def. des Exponenten gilt $a^d = 1$ für alle
 $a \in U \Rightarrow$ jedes $a \in U$ ist Nullstelle von $x^d - 1 \in K[x]$

Da $x^d - 1$ als Pol vom Grad d über einem Körper höchstens d Nullstellen hat, muss auch $n \leq d$ gelten, insgesamt $d = n$. Prop. 14.12 $\xrightarrow{U \text{ endl. und abelsch}}$ Es gibt in U ein Element der Ordnung $d = n = |U|$.

Also ist U zyklisch. $\square$

F
D
Be
43
Das
ord
d h
mod
2¹⁴
3²¹
→

Erinnerung: Ist G eine Gruppe, $g \in G$, $n \in \mathbb{N}$.

Dann gilt: $n = \text{ord}(g) \Leftrightarrow g^n = e$ und $g^{n/p} \neq e$
für jeden Primteiler p von n

Beispiel: Bestimmung einer Primitivwurzel modulo 43

43 Primzahl $\Rightarrow (\mathbb{Z}/43\mathbb{Z})^\times$ ist zykl. von Ordn. $42 = 2 \cdot 3 \cdot 7$

Daraus folgt: $\forall a \in (\mathbb{Z}/43\mathbb{Z})^\times$ gilt

$$\text{ord}(a) = 42$$

d.h. a ist Primitivwurzel $\Leftrightarrow a^{21} \neq 1, a^{14} \neq 1, a^6 \neq 1$
($a^{42} = 1$ ist immer erfüllt)

modulo 43

$\bar{2}^{14} = \bar{1} \Rightarrow 2$ ist keine Primitivwurzel modulo 43

$$\bar{3}^{21} = \bar{42} \neq \bar{1}, \bar{3}^{14} = \bar{36} \neq \bar{1}, \bar{3}^6 = \bar{41} \neq \bar{1}$$

$\Rightarrow 3$ ist Primitivwurzel modulo 43

□

Lemma (14.15)

- (i) Sei p eine ungerade Primzahl und $m \in \mathbb{N}$. Dann gilt $(1+p)^{p^{m-1}} \equiv 1 \pmod{p^m}$ und $(1+p)^{p^{m-1}} \not\equiv 1 \pmod{p^{m+1}}$.
- (ii) Für alle $m \in \mathbb{N}$, $m \geq 2$ gilt $5^{2^{m-2}} \equiv 1 \pmod{2^m}$ und $5^{2^{m-2}} \not\equiv 1 \pmod{2^{m+1}}$.

Beweis von Lemma 14.15, nur Teil (i)

p ungerade Primzahl, $m \in \mathbb{N}$, $2 \leq m$.

$$(1+p)^{p^{m-1}} \equiv 1 \pmod{p^m}, \quad (1+p)^{p^{m-1}} \not\equiv 1 \pmod{p^{m+1}} \quad (*)$$

Beweis durch vollst. Induktion

Induktionsanfang ($m=1$) Die Behauptung lautet

$$1+p \equiv 1 \pmod{p}, \quad 1+p \not\equiv 1 \pmod{p^2} \quad (\text{offensichtlich})$$

Induktionsschritt $m \rightarrow m+1$ Ind.-V. $\Rightarrow$

$$(1+p)^{p^{m-1}} = 1+kp^m \quad \text{für ein } k \in \mathbb{Z} \text{ mit } p \nmid k$$

$$\Rightarrow (1+p)^{p^m} = \left((1+p)^{p^{m-1}} \right)^p = (1+kp^m)^p \stackrel{\text{binomischer}}{=} \text{Lehrsatz}$$

$$1 + k \cdot p^{m+1} + \sum_{j=2}^p \binom{p}{j} k^j p^{mj} \quad \binom{p}{j} = \frac{p!}{j!(p-j)!} \begin{array}{l} \leftarrow \text{teilbar durch } p \\ \leftarrow \text{nicht teil-} \\ \text{bar durch } p \end{array}$$

Für $2 \leq j \leq p-1$ gilt $p \mid \binom{p}{j} \Rightarrow \binom{p}{j} k^j p^{mj}$ teilbar durch p^{mj+1} , $m_j+1 \geq 2m+1 \geq m+2 \Rightarrow \binom{p}{j} k^j p^{mj} \equiv 0 \pmod{p^{m+2}}$ für $1 \leq j \leq p-1$

letzter Summand: $k^p p^{pm}$, $pm \geq 3m \geq m+2$

$$\Rightarrow k^p p^{pm} \equiv 0 \pmod{p^{m+2}} \quad \text{also insgesamt:}$$

$$(1+p)^{p^m} \equiv 1 + k p^{m+1} \pmod{p^{m+2}} \xrightarrow{pk} (1+p)^{p^m} \equiv 1 \pmod{p^{m+1}}$$

$$(1+p)^{p^m} \not\equiv 1 \pmod{p^{m+2}}$$

□

Satz (14.16)

- (i) Für jede ungerade Primzahl p und jedes $m \in \mathbb{N}$ ist $(\mathbb{Z}/p^m\mathbb{Z})^\times$ eine zyklische Gruppe der Ordnung $p^{m-1}(p-1)$.
- (ii) Es gilt $(\mathbb{Z}/2\mathbb{Z})^\times = \{\bar{1}\}$ und $(\mathbb{Z}/4\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z}$.
Für alle $m \geq 3$ existiert jeweils ein Isomorphismus $(\mathbb{Z}/2^m\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{m-2}\mathbb{Z}$.

Beweis von Satz 14.16, nur Teil (i)

geg. ungerade Primzahl p , $m \in \mathbb{N}$, $m \geq 2$

z.zg. $(\mathbb{Z}/p^m\mathbb{Z})^\times$ ist zyklisch von Ordnung $p^{m-1}(p-1)$

zeige zunächst: In der Gruppe existiert ein Element der Ordnung $p-1$ und ein Element der Ordnung p^{m-1}

Sei $a \in \mathbb{Z}$ eine p -te Einheitswurzel modulo p .

Betrachte die Ordnung r des Elements $a + p^m\mathbb{Z}$ in $(\mathbb{Z}/p^m\mathbb{Z})^\times$.

$$(a + p^m\mathbb{Z})^r = 1 + p^m\mathbb{Z} \Rightarrow a^r + p^m\mathbb{Z} = 1 + p^m\mathbb{Z}$$

$$\Rightarrow a^r \equiv 1 \pmod{p^m} \Rightarrow a \equiv 1 \pmod{p} \Rightarrow (a + p\mathbb{Z})^r =$$

$1+p\mathbb{Z}$ in $(\mathbb{Z}/p\mathbb{Z})^\times$. Da $a+p\mathbb{Z}$ in $(\mathbb{Z}/p\mathbb{Z})^\times$ die Ordnung $p-1$ hat (da a Primitivwurzel modulo p) $\Rightarrow (p-1) \mid r$
 $\Rightarrow \exists l \in \mathbb{N}$ mit $r = l \cdot (p-1)$. Setze $b = a^l + p^m\mathbb{Z}$. Dann ist
 $b = (a+p\mathbb{Z})^l$ in $(\mathbb{Z}/p^m\mathbb{Z})^\times$ ein Element der Ordnung
 $\frac{l(p-1)}{d} = p-1$.

Sei nun $c = (1+p) + p^m\mathbb{Z} \in (\mathbb{Z}/p^n\mathbb{Z})^\times$. Lemma 14.15 $\rightarrow$
 $(1+p)^{p^{m-1}} \equiv 1 \pmod{p^m}$, $(1+p)^{p^{n-2}} \not\equiv 1 \pmod{p^m} \Rightarrow$
 $c^{p^{m-1}} = 1 + p^n\mathbb{Z}$, $c^{p^{n-2}} \neq 1 + p^n\mathbb{Z} \Rightarrow c$ ist in $(\mathbb{Z}/p^n\mathbb{Z})^\times$
 ein Element der Ordnung p^{m-1} ($\Rightarrow$ Beh.)

Sei $U = \langle b \rangle$, $V = \langle c \rangle$. Beh.

$(\mathbb{Z}/p^m\mathbb{Z})^\times$ ist ein inneres direktes Produkt
von U und V

klar: $U \trianglelefteq (\mathbb{Z}/p^m\mathbb{Z})^\times$, $V \trianglelefteq (\mathbb{Z}/p^m\mathbb{Z})^\times$,
da $(\mathbb{Z}/p^m\mathbb{Z})^\times$ eine abelsche Gruppe ist

$|U| = \text{ord}(b) = p-1$, $|V| = \text{ord}(c) = p^{m-1}$

sind teilerfremd $\Rightarrow U \cap V = \{1 + p^m\mathbb{Z}\}$

Es gilt $U \leq UV \Rightarrow p-1$ teilt $|UV|$

ebenso: $V \leq UV \Rightarrow p^{m-1}$ teilt $|UV|$

g
Z
Wir
den
(i)
(ii)
(iii)
und

$\mathbb{Z}$

$$\Rightarrow \text{kgV}(p-1, p^{m-1}) = p^{m-1}(p-1) \text{ teilt } |UV|$$

$$\Rightarrow |UV| \geq p^{m-1}(p-1) = \varphi(p^m) = |(\mathbb{Z}/p^m\mathbb{Z})^\times|$$

$$UV \subseteq (\mathbb{Z}/p^m\mathbb{Z})^\times \Rightarrow UV = (\mathbb{Z}/p^m\mathbb{Z})^\times (\Rightarrow \text{Beh.})$$

Aus der Beh. folgt

$$(\mathbb{Z}/p^m\mathbb{Z})^\times \cong U \times V \stackrel{\substack{\text{u.v.} \\ \text{zyklisch}}}{=} \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{m-1}\mathbb{Z}$$

$$p-1, p^{m-1} \text{ teilerfremd} \quad \mathbb{Z}/p^{m-1}(p-1)\mathbb{Z}$$

Chin. RS für Gruppen

Also ist $(\mathbb{Z}/p^m\mathbb{Z})^\times$ zyklisch. □

Anwendungsbeispiel: $48 = 16 \cdot 3 = 2^4 \cdot 3$

$$\rightarrow (\mathbb{Z}/48\mathbb{Z})^{\times} \cong (\mathbb{Z}/16\mathbb{Z})^{\times} \times (\mathbb{Z}/3\mathbb{Z})^{\times}$$

$$\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

$\mathbb{Z}$

□

§ 15. Endliche und algebraische Körpererweiterungen

Bereits in § 9 haben wir die Begriffe „Teilkörper“, „Erweiterungskörper“ und „Körpererweiterung“ eingeführt.

Definition (15.1)

Sei $L|K$ eine Körpererweiterung. Ein **Zwischenkörper** von $L|K$ ein Teilkörper von L , der zugleich Erweiterungskörper von K ist.

Satz (15.2)

Sei $\tilde{L}|K$ eine Körpererweiterung und $S \subseteq \tilde{L}$ eine Teilmenge. Dann gibt es einen eindeutig bestimmten **Zwischenkörper** L von $\tilde{L}|K$ mit den Eigenschaften

- (i) $L \supseteq S$
- (ii) Für jeden weiteren Zwischenkörper L' von $\tilde{L}|K$ mit $L' \supseteq S$ gilt $L' \supseteq L$.

Insgesamt ist L also der **kleinste** Zwischenkörper von $L|K$ mit der Eigenschaft $L \supseteq S$.

Wir bezeichnen den Körper L mit $K(S)$ und nennen ihn den von der Teilmenge S über K **erzeugten** Teilkörper von $\tilde{L}$.

Proposition (15.3)

Sei $\tilde{L}|K$ eine Körpererweiterung, und seien S und T beliebige Teilmengen von $\tilde{L}$. Dann gilt

$$K(S \cup T) = K(S)(T).$$

Proposition (15.4)

Sei $\tilde{L}|K$ eine Körpererweiterung und $a \in \tilde{L}$. Dann gilt

$$K(a) = \left\{ \frac{f(a)}{g(a)} \mid f, g \in K[x], g(a) \neq 0 \right\}.$$

Beweis von Prop. 15.3

geg: Körpererweiterung $\tilde{L} | K$, $S, T \subseteq \tilde{L}$

z.zg: $K(S \cup T) = K(S)(T)$

Wir überprüfen, dass $K(S)(T)$ die definierenden Eigenschaften von $K(S \cup T)$ hat, also

(i) $K(S)(T)$ ist Zwischenkörper von $\tilde{L} | K$

(ii) $K(S)(T) \supseteq S \cup T$

(iii) Ist L' ein bel. Zwischenkörper von $\tilde{L} | K$

mit $L' \supseteq S \cup T$, dann folgt $L' \supseteq K(S)(T)$

zu li) $K(S)$ ist Teilkörper von $\tilde{L}$ (wg. $S \subseteq \tilde{L}$)

$\Rightarrow K(S)(T)$ ist Teilkörper von $\tilde{L}$ (wg. $T \in \tilde{L}$)

außerdem: $K(S) \supseteq K \Rightarrow K(S)(T) \supseteq K(S) \supseteq K$

insg. $K(S)(T)$ ist Zwischenkörper von $\tilde{L} | K$.

zu lii) $K(S)(T) \supseteq K(S) \supseteq S \} \Rightarrow K(S)(T) \supseteq S \cup T$
 $K(S)(T) \supseteq T$

zu liii) Sei L' wie angeg. L' Zwischenkörper von $\tilde{L} | K$,

$L' \supseteq S \Rightarrow L' \supseteq K(S)$

L' ist somit Zwischenkörper von $\tilde{L} | K(S)$, außerdem

L' ist somit Zwischenkörper von $L | K(S)$, außerdem

$$\text{gilt } L' \supseteq T \Rightarrow L' \supseteq K(S)(T)$$

□