Aufgabe 1.

i) Zeige, daß das Polynom $f = X^4 + 17X^3 + 23X^2 - 5X + 1$ irreduzibel in $\mathbb{Q}[X]$ ist. *(3 Punkte)*
ii) Zeige, daß das Polynom $g = X^2 + Y^2 - 1$ irreduzibel in $\mathbb{Q}[X, Y]$ ist. *(3 Punkte)*

i) Reduktion modulo 2 liefert das Polynom $X^4 + X^3 + X^2 + X + 1 \in (\mathbb{Z}/2\mathbb{Z})[X]$. Dieses ist irreduzibel, denn es hat weder 0 noch 1 als Nullstelle (d.h. keine Faktoren vom Grad 1 oder 3) und ist nicht durch das einzige irreduzible Polynom vom Grad 2, nämlich $X^2 + X + 1$, teilbar. – ii) Betrachte das Polynom im faktoriellen Ring $\mathbb{Q}[Y][X]$. Dort erfüllt es die Bedingungen des Eisensteinkriteriums (etwa das irreduzible Polynom $Y - 1$ teilt den konstanten Term $Y^2 - 1$ nur einmal) und ist damit irreduzibel in $\mathbb{Q}(Y)[X]$ und damit, da normiert und daher primitiv, auch in $\mathbb{Q}[Y][X] = \mathbb{Q}[Y, X]$.

Aufgabe 2. Es sei $\zeta := e^{2\pi i/15} \in \mathbb{C}$ und $K := \mathbb{Q}(\zeta)$. Es sei L der Zerfällungskörper von $X^{15} - 2$ über K. Bestimme $[L : K]$ und alle Zwischenkörper der Erweiterung $K \subset L$. *(6 Punkte)*

Wegen Charakteristik 0 ist alles separabel, also ist L/K eine Galoiserweiterung. Außerdem ist $L = K(a)$ mit $a = \sqrt[15]{2}$, denn die $\zeta^i a$ mit $0 \leqslant i < 15$ sind (genügend viele und damit) genau die Nullstellen von $X^{15} - 2$, und sie liegen alle in L. Da $X^{15} - 2$ nach Eisenstein irreduzibel über $\mathbb{Q}$ ist, folgt $[\mathbb{Q}(a) : \mathbb{Q}] = 15$. Aber $[K : \mathbb{Q}] = \varphi(15) = \varphi(3) \cdot \varphi(5) = 2 \cdot 4 = 8$, und nach dem Gradsatz folgt $[L : K] = 15$, da 8 und 15 teilerfremd sind.
Jeder K-Automorphismus $\varphi : L \to L$ ist genau gegeben durch $\varphi(a) = \zeta^i a$ mit einem beliebigen, eindeutigen $0 \leqslant i < 15$. Der Automorphismus φ_0 mit $\varphi_0(a) = \zeta a$ hat dann die Eigenschaft $\varphi_0^i(a) = \zeta^i a$, also Ordnung 15 und ist damit ein Erzeuger der Galoisgruppe $\mathrm{Aut}(L/K)$, die also zyklisch ist. Eine zyklische Gruppe der Ordnung 15 hat laut Vorlesung genau vier Untergruppen, nämlich jeweils eine mit $1, 3, 5, 15$ Elementen, und nach dem Hauptsatz der Galoistheorie hat L/K damit genau vier Zwischenkörper vom Grad $15, 5, 3, 1$. Die äußeren sind trivial (nämlich L und K), die zwei inneren findet man per Hand: nämlich a^5 und a^3 haben Minimalpolynome $X^3 - 2$ bzw. $X^5 - 2$ über $\mathbb{Q}$ (Eisenstein) und damit, nach dem selben Argument wie oben, auch über K. Also sind $K(a^3)$ und $K(a^5)$ die beiden noch fehlenden Zwischenkörper.

Aufgabe 3. Zeige, daß jede Gruppe der Ordnung 56 auflösbar ist. *(6 Punkte)*

Es ist $56 = 7 \cdot 2^3$. Nach Sylowsätzen gibt es genau eine oder acht 7-elementige Untergruppen und genau eine oder sieben 8-elementige Untergruppen. Daß es von beiden mehr als nur eine gibt, kann nicht sein: denn acht 7-elementige Untergruppe verbrauchen (nebst dem neutralen) $8 \cdot 6 = 48$ Elemente der Gruppe, da sie alle disjunkt-oder-gleich sind. Das läßt nur 8 Elemente (inkl. neutralem Element) übrig, die also nur noch für genau eine 8-elementige Untergruppe reicht. Eine 56-elementige Gruppe hat also einen 7-elementigen oder einen 8-elementigen Normalteiler, mit 8- bzw. 7-elementigem Quotienten. Aber Gruppen von Primzahlpotenzordnung sind nach Übungen auflösbar.

Aufgabe 4.

i) Finde einen Unterkörper $K \subset \mathbb{C}$ mit $[K : \mathbb{Q}] = 3$, so daß $K/\mathbb{Q}$ nicht galoissch ist. *(3 Punkte)*
ii) Finde einen Unterkörper $L \subset \mathbb{C}$ mit $[L : \mathbb{Q}] = 3$, so daß $L/\mathbb{Q}$ galoissch ist. *(3 Punkte)*

i) Es tut $K = \mathbb{Q}(\sqrt[3]{2})$: das Minimalpolynom ist $X^3 - 2$ (irreduzibel nach Eisenstein), es zerfällt aber nicht über K, denn sogar in $\mathbb{R} \supset K$ besitzt es nur eine einzige Nullstelle (Eindeutigkeit der reellen dritten Wurzel). – ii) Nimm etwa den Kreisteilungskörper $M = \mathbb{Q}(\zeta_7)$. Er ist galoissch über $\mathbb{Q}$ mit Galoisgruppe $\cong \mathbb{Z}/6\mathbb{Z}$ nach Vorlesung. Eine Untergruppe vom Index 3 (ist dann automatisch normal und) korrespondiert zu einem Zwischenkörper $K \subset L \subset M$ mit L/K galoissch vom Grad 3.

Aufgabe 5. Es sei L/K eine endliche Körpererweiterung.

i) Ist K vollkommen, so auch L. *(2 Punkte)*
ii) Ist L/K separabel, so besitzt die Erweiterung nur endlich viele Zwischenkörper. *(4 Punkte)*

i) Zu zeigen ist nur, daß jede endliche Erweiterung M/L separabel ist. Aber nach der Gradformel ist M/K endlich und nach Voraussetzung separabel, aber das impliziert Separabilität von M/L (denn für jedes $a \in M$ ist das Minimalpolynom von a über L ein Teiler des [separablen!] Minimalpolynoms von a über K). – ii) Falls L/K sogar galoissch ist, folgt die Behauptung aus dem Hauptsatz der Galoistheorie, denn die Galoisgruppe besitzt als endliche Gruppe nur endlich viele Untergruppen. Wir reduzieren nun auf diesen Fall, indem wir eine Erweiterung M/L konstruieren, so daß M/K Galoissch ist (und sind dann fertig): Sei $a \in L$ ein primitives Element, d.h. $L = K(a)$. Sei $F \in K[X]$ das Minimalpolynom von a und $M \supset L$ ein Zerfällungskörper von F über K. Da F separabel ist, ist M/K Galoissch. – Eine ganz andere Argumentation ginge so: Sei wieder $a \in L$ ein primitives Element und $K \subset P \subset L$ ein Zwischenkörper. Dann wird P erzeugt durch die Koeffizienten des Minimalpolynoms von a über P (das muß man zeigen!), also durch die Koeffizienten eines gewissen normierten Teilers von F (etwa über einem algebraischen Abschluß von K). Aber F hat überhaupt nur endlich viele Teiler, da der Polynomring $K[X]$ ja faktoriell ist, und daraus folgt die Behauptung.

Zusatzaufgabe. Es sei G eine endliche Gruppe, die nur genau eine (bezüglich der Inklusion) maximale echte Untergruppe besitzt. Zeige: Dann ist G zyklisch, und $|G|$ ist eine Primzahlpotenz. *(6 Extrapunkte)*

Ein Element $g \in G$ liegt genau dann in einer maximalen echten Untergruppe, wenn es überhaupt in einer echten Untergruppe liegt, wenn also $\langle g \rangle \neq G$ ist. Ist nun U die einzige maximale echte Untergruppe, so ist $G \setminus U$ nichtleer, und jedes Element dieser Menge muß die Gruppe G erzeugen. Also ist G zyklisch, isomorph zu einem $\mathbb{Z}/n\mathbb{Z}$. Es bleibt n zu bestimmen: da die Untergruppen von $\mathbb{Z}/n\mathbb{Z}$ eineindeutig den Teilern von n entsprechen, besitzt n nur einen einzigen maximalen (bzgl. der Teilbarkeitsrelation) echten Teiler. Wäre n aber durch zwei verschiedene Primzahlen p, q teilbar, so wären sowohl n/p als auch n/q maximale echte Teiler von n, Widerspruch. Also besitzt n nur einen Primteiler und ist damit eine Primzahlpotenz.

(Extraplatz zum Weiterschreiben)

(Extraplatz zum Weiterschreiben)