Lösungshinweise zur Algebra-Klausur vom 31.08.16

Aufgabe 1:

a) $f(x) = x^4 + x + 1$ hat keine Nullstelle in $\mathbb{F}_2$, kann also keinen Linearfaktor als Teiler haben. Falls $f(x)$ irreduzibel ist, so zerfällt $f(x)$ in zwei Polynome 2. Grades, die jeweils irreduzibel sind. $x^2 + x + 1$ ist einziges Polynom in $\mathbb{F}_2[x]$, das irreduzibel ist. Aber
$$(x^2 + x + 1)^2 = x^4 + x^2 + 1 \neq x^4 + x + 1,$$
also ist $f(x)$ irreduzibel.

b) $x^5 + 10x - 5$ ist nach Eisenstein mit $p = 5$ irreduzibel in $\mathbb{Z}[x]$. Mit dem Satz von Gauß folgt, dass $x^5 + 10x - 5$ irreduzibel in $\mathbb{Q}[x]$ ist.

c) $f(x) = x^4 - x^3 + 3x^2 - 2x + 2$ hat keine Nullstellen in Z, da diese Teiler von 2 sein müssen und ± 1 und ± 2 keine Nullstellen von $f(x)$ sind (da $f(1) = 3$, $f(2) = 18$, $f(-1) = 9$ und $f(-2) = 42$). Wenn f irreduzibel ist, dann ist
$$f(x) = (x^2 + ax + b)(x^2 + cx + d)$$
mit $a, b, c, d \in \mathbb{Z}$.

Ausmultiplizieren liefert
$$f(x) = x^4 + (c + a)x^3 + (b + ac + d)x^2 + (ad + bc)x + bd$$
und Koeffizientenvergleich ergibt folgendes lineares Gleichungssystem:
$$\begin{aligned} c + a &= -1, & ad + bc &= 2, \\ d + ac + b &= 3, & bd &= 2. \end{aligned}$$
O.B.d.A. sei $|b| < |d|$, dann ist entweder $\underbrace{b = 1,\ d = 2}_{\text{Fall 1}}$ oder $\underbrace{b = -1,\ d = -2}_{\text{Fall 2}}$.

In Fall 1 ergibt sich, dass $a = -1$ und $c = 0$ gilt, also folgt insgesamt
$$f(x) = (x^2 - x + 1)(x^2 + 2).$$
$x^2 - x + 1$ ist irreduzibel in $\mathbb{F}_2[x]$, also auch in $\mathbb{Z}[x]$. $x^2 + 2$ ist nach Eisenstein mit $p = 2$ irreduzibel in $\mathbb{Z}[x]$. Fall 2 muss nicht betrachtet werden, da die Zerlegung in irreduzible Polynome in $\mathbb{Q}[x]$ und damit auch in $Z[x]$ eindeutig ist.

Aufgabe 2:

a) Sei $U \leq G$ Untergruppe einer endlichen Gruppe G. Dann folgt $|U|$ teilt $|G|$.

b) G ist die endliche Vereinigung von Linksnebenklassen in U. Alle Linksnebenklassen haben die gleiche Anzahl an Elementen, da für festes $g \in G$ die Abbildung $U \to gU, x \mapsto g \cdot x$, bijektiv ist. Verschiedene Linksnebenklassen sind disjunkt, da die Äquivalenzklassen eine Äquivalenzrelation bilden. $1 \cdot U = U$ ist die triviale Nebenklasse, also gilt mit der Anzahl m an Linksnebenklassen von U, dass

$$|G| = m \cdot |U|.$$

c) Sei $U \leq \mathrm{A}_4$ mit $|U| = 6$. Als Untergruppe von Index 2 ist U normal in A_4. Die 3-Sylowgruppe S von U ist mit dem gleichen Argument normal in U. Da $U \trianglelefteq \mathrm{A}_4$, folgt $g^{-1}Sg \leq U$ und damit $g^{-1}Sg = S$ für alle $g \in \mathrm{A}_4$. Nach dem Sylowsatz hat A_4 genau eine p-Sylowgruppe. Aber A_4 hat 8 verschiedene Elemente der Ordnung 3, also kann es keine Untergruppe der Ordnung 6 geben.

Aufgabe 3:

Sei $G^{(0)} := G$ und $G^{(1)} = G'$ die Kommutatoruntergruppe. Für $i = 1, 2, \ldots$ sei $G^{(i)} = (G^{(i-1)})'$. Eine Gruppe G heißt auflösbar, falls $G^{(r)} = \{1_G\}$ für ein $r \in \mathbb{N}$ gilt.

Für eine Gruppe G der Ordnung $135 = 3^3 \cdot 5$ sei S eine 3-Sylowgruppe von G. Nach Lagrange gilt $\mathrm{N}_G(S) = S$ oder $\mathrm{N}_G(S) = G$. Für $\mathrm{N}_G(S) = S$ folgt nach dem Sylowsatz, dass die Anzahl der 3-Sylowgruppen $5 \equiv 1 \mod 3$ wäre, ein Widerspruch. Also ist $\mathrm{N}_G(S) = G$ und damit S normal in G. S ist als 3-Gruppe auflösbar. G/S hat Ordnung 5 und ist als abelsche Gruppe ebenfalls auflösbar. Da S und G/S auflösbar sind, folgt, dass G auflösbar ist.

Aufgabe 4:

a) Sei G abelsche Gruppe der Ordnung $|G| = 36 = 2^2 \cdot 3^2$. Es gibt zwei abelsche nicht-isomorphe Gruppen der Ordnung p^2, nämlich C_{p^2} und $C_p \times C_p$. Als abelsche Gruppe ist G direktes Produkt seiner Sylowgruppen.

$$\begin{aligned} &G \cong C_9 \times C_4, && G \cong C_9 \times C_2 \times C_2, \\ &G \cong C_3 \times C_3 \times C_4, && G \cong C_3 \times C_3 \times C_2 \times C_2. \end{aligned}$$

In Elemenentarteilerform erhalten wir

$$\begin{aligned} &G \cong C_{36}, && G \cong C_{18} \times C_2, \\ &G \cong C_{12} \times C_4, && G \cong C_6 \times C_6. \end{aligned}$$

b) $G = S_3 \times S_3$ ist ein Gegenbeispiel.

Aufgabe 5:

Sei $a, b \in \varphi^{-1}(J)$, das heißt es existieren $x, y \in J$ mit $\varphi(a) = x$ und $\varphi(b) = y$. Zunächst zeigen wir, dass $a + b \in \varphi^{-1}(J)$. Es gilt

$$\varphi(a+b) \overset{\varphi \text{ Homom.}}{=} \varphi(a) + \varphi(b) = x + y \in J,$$

da J Ideal ist. Analog folgt für $r \in R$, dass

$$\varphi(ra) = r\varphi(a) = rx \in J$$

gilt. Zusätzlich gilt, dass wegen $0_R \in \varphi^{-1}(J)$ das Ideal nicht leer ist. Also ist $\varphi^{-1}(J)$ ein Ideal in R.

Aufgabe 6:

L ist Zerfällungskörper von $(x^2-3)(x^2-5)$. Da keine Nullstelle mehrfach auftritt ist L eine Galoiserweiterung. Es ist $\sqrt{15} \in L$, aber $\sqrt{15} \notin \mathbb{Q}[\sqrt{3}]$ bzw. $\sqrt{15} \notin \mathbb{Q}[\sqrt{5}]$, da sonst $\sqrt{5} \in \mathbb{Q}[\sqrt{3}]$ bzw. $\sqrt{3} \in \mathbb{Q}[\sqrt{5}]$ liegen würde, ein Widerspruch.

Es ist $\dim_{\mathbb{Q}} L = 4$, also folgt $\operatorname{Aut}(L, \mathbb{Q}) \cong C_2 \times C_2$ oder $\operatorname{Aut}(L, \mathbb{Q}) \cong C_4$.

Nach dem Hauptsatz der Galois-Theorie gibt es eine Bijektion zwischen der Menge der Zwischenkörpern von L und der Menge der Untergruppen von $\operatorname{Aut}(L, \mathbb{Q})$. L hat mindestens 5 Teilkörper, also folgt $\operatorname{Aut}(L, \mathbb{Q}) \cong C_2 \times C_2$ (die zyklische Gruppe C_4 hat nur 3 Untergruppen).

$C_2 \times C_2$ hat genau 5 Untergruppen, also hat L nach dem Hauptsatz genau 5 Teilkörper. Diese sind:

$$\begin{tikzcd}
 & L \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}[\sqrt{3}] \arrow[dr, dash] & \mathbb{Q}[\sqrt{5}] \arrow[d, dash] & \mathbb{Q}[\sqrt{15}] \arrow[dl, dash] \\
 & \{1\} &
\end{tikzcd}$$

Das Element $z = \sqrt{3} + \sqrt{5}$ erzeugt L, da $\mathbb{Q}[\sqrt{3} + \sqrt{5}] \subseteq L$ und

$$\begin{aligned}
&(\sqrt{3} + \sqrt{5})(\sqrt{3} - \sqrt{5}) = -2 \\
&\Rightarrow \sqrt{3} - \sqrt{5} \in \mathbb{Q}[\sqrt{3} + \sqrt{5}] \\
&\Rightarrow \sqrt{3} \text{ und } \sqrt{5} \in \mathbb{Q}[\sqrt{3} + \sqrt{5}] \\
&\Rightarrow \mathbb{Q}[\sqrt{3} + \sqrt{5}] = L.
\end{aligned}$$

Aufgabe 7:

Für die Würfelverdopplung muss $\sqrt[3]{2}$ aus $\mathbb{Q}$ konstruiert werden. $f(x) = x^3 - 2$ ist irreduzibel nach Eisenstein mit $p = 2$ in $\mathbb{Z}[x]$ bzw. mit Gauß in $\mathbb{Q}[x]$. Da $f(\sqrt[3]{2}) = 0$, ist f Minimalpolynom zu $\sqrt[3]{2}$. Es gilt dann $\dim_{\mathbb{Q}}(\mathbb{Q}[\sqrt[3]{2}]) = 3$.

Damit $\sqrt[3]{2}$ konstruierbar ist, muss $\mathbb{Q}[\sqrt[3]{2}]$ in einem Körper L mit $\dim_{\mathbb{Q}} L = 2^m$ liegen. Nach der Gradformel folgt $3|2^n$, ein Widerspruch.

Aufgabe 8:

Nach Eisenstein ist $f(x) = x^5 - 4x + 2$ irreduzibel. Sei L der Zerfällungskörper von f. Da f irreduzibel ist, operiert $\mathrm{Aut}(L, \mathbb{Q})$ transitiv auf den Nullstellen von f. 5 ist Teiler von $|\mathrm{Aut}(L, \mathbb{Q})|$, also hat $\mathrm{Aut}(L, \mathbb{Q})$ als Untergruppe von S_5 einen 5-Zykel σ.

f hat genau 3 reelle Nullstellen, die invariant unter komplexer Konjugation sind. Also induziert die komplexe Konjugation in $\mathrm{Aut}(L, \mathbb{Q})$ eine Transposition τ, die die beiden komplexen Nullstellen vertauscht.

Da je zwei Transpositionen zueinander konjugiert sind, können wir o.B.d.A. annehmen, dass $\tau = (1, 2)$. σ operiert transitiv auf $\{1, \ldots, 5\}$, also gibt es ein $1 \leq i \leq 5$, sodass $\sigma^i(1) = 2$ ergibt. Da p eine Primzahl ist, erzeugen σ und σ^i die gleiche Untergruppe, wir können also o.B.d.A. annehmen, dass $\sigma(1) = 2$ ist. Nach Konjugation mit einer geeigneten Permuation von $\{3, 4, 5\}$ können wir zusätzlich voraussetzen, dass $\sigma = (1, 2, 3, 4, 5)$. Jede Transposition wird erzeugt, da $(i, i + 1) = \sigma^{i-1}\tau\sigma^{1-i}$ gilt. Die Menge der Transpositionen erzeugt S_5.

Die symmetrische Gruppe S_5 enthält A_5 als nicht auflösbaren Normalteiler, also lässt sich $f(x)$ nicht durch Radikale lösen.