Henning Krause
Jan Geuenich

Algebra I
Probeklausur mit Lösungsvorschlag

WS 2017/18

Aufgabe 1 (4 Punkte):

Sei G eine endliche Gruppe mit einer Untergruppe H und einem Normalteiler N.

		Wahr	Falsch
(a)	Operiert G auf einer endlichen Menge X, so muss $\lvert G\rvert$ ein Teiler von $\lvert X\rvert$ sein.	$\square$	$\boxtimes$
(b)	Ist N eine 2-Sylowuntergruppe von G, so hat jedes Element in G/N ungerade Ordnung.	$\boxtimes$	$\square$
(c)	Ist G/N einfach, dann besitzt G abgesehen von N keinen echten nichttrivialen Normalteiler.	$\square$	$\boxtimes$
(d)	Sind N und G/N abelsch, so ist G stets abelsch.	$\square$	$\boxtimes$

Begründungen:

(a) Auf jeder Menge X ist durch $(g, x) \mapsto x$ eine (triviale) Operation von G gegeben.

(b) Es ist $|N| = 2^s$ und $|G| = 2^s m$ für ein ungerades m. Die Ordnung jedes Elements der Gruppe G/N teilt $|G/N| = |G|/|N| = m$ und ist daher ungerade.

(c) Die Gruppe $G = \mathbb{Z}/8\mathbb{Z}$ besitzt neben $N = 4\mathbb{Z}/8\mathbb{Z}$ noch $2\mathbb{Z}/8\mathbb{Z}$ als nichttrivialen Normalteiler. Dennoch ist $G/N \cong \mathbb{Z}/2\mathbb{Z}$ eine einfache Gruppe.

(d) Die Quaternionengruppe G hat einen Normalteiler N der Ordnung 4 und ist nicht abelsch. Als Gruppen der Ordnung höchstens 4 sind aber N und G/N abelsch.

Aufgabe 2 (4 Punkte):

Sei K ein Körper.

		Wahr	Falsch
(a)	Der Ring $K[X,Y]/(1-XY)$ ist faktoriell.	$\boxtimes$	$\square$
(b)	Jede Körpererweiterung vom Grad 2 ist separabel.	$\square$	$\boxtimes$
(c)	Jede Körpererweiterung vom Grad 2 ist normal.	$\boxtimes$	$\square$
(d)	Der Ring $K[X,Y]$ ist ein Hauptidealring.	$\square$	$\boxtimes$

Begründungen:

(a) Nach Sätzen 2.6.5 und 2.8.4 ist $K[X,Y]$ faktoriell. Aufgaben 10.3 und 10.4 zufolge ist dann auch $K[X,Y]/(1-XY)$ faktoriell.

(b) Wegen $\mathrm{Irr}(T, \mathbb{F}_2(T^2)) = X^2 - T^2 = (X-T)^2$ ist $\mathbb{F}_2(T)/\mathbb{F}_2(T^2)$ nicht separabel.

(c) Sei L/K eine Körpererweiterung vom Grad 2 und $\alpha \in L$. Da $X - \alpha$ ein Faktor von $f = \mathrm{Irr}(\alpha, K)$ in $L[X]$ und $\mathrm{grad}(f) \leq [L : K] = 2$ ist, zerfällt f in $L[X]$.

(d) Würde das Ideal (X,Y) von einem einzigen Element f erzeugt, hätten wir $X = gf$ und $Y = hf$ und somit $hX = gY$. Wegen der Irreduzibilität von X und Y müssten zudem g und h Einheiten sein. Das widerspricht aber der Tatsache, dass X und Y (als Polyome in Y mit Koeffizienten in $K[X]$) nicht denselben Grad besitzen.

Aufgabe 3 (2 + 2 + 2 + 2 Punkte):
Sei $\mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$ und sei Γ die Menge aller Matrizen

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

mit Einträgen $a, d \in 1 + 2\mathbb{Z}$, $b, c \in 2\mathbb{Z}$ und $ad - bc = 1$.

(a) Man zeige, dass Γ eine Untergruppe von $\mathrm{GL}_2(\mathbb{C})$ ist.

(b) Man zeige, dass die Vorschrift

$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, z\right) \mapsto \frac{az+b}{cz+d}$$

eine Gruppenoperation $\Gamma \times \mathbb{H} \to \mathbb{H}$ liefert.

(c) Man bestimme die Standgruppe Γ_i von $i \in \mathbb{H}$.

(d) Man beweise oder widerlege, dass die Gruppe Γ einfach ist.

Lösung:

(a) Sicher liegt $E = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ in Γ. Für $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ gilt wegen $\det(A) = ad - bc = 1$

$$A^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in \Gamma$$

und mit $A' = \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right) \in \Gamma$ wegen $aa', dd' \in 1+2\mathbb{Z}$, $bc', ab', bd', ca', dc', cb' \in 2\mathbb{Z}$ auch

$$AA' = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix} \in \Gamma\,.$$

Nach dem Untergruppenkriterium ist Γ deshalb eine Untergruppe von $\mathrm{GL}_2(\mathbb{C})$.

(b) Seien $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ und $z \in \mathbb{H}$. Zunächst zeigen wir, dass tatsächlich $\frac{az+b}{cz+d} \in \mathbb{H}$ ist. Das ist äquivalent zu $w = (az+b)(c\overline{z}+d) \in \mathbb{H}$. Nun ist $w = acz\overline{z} + adz + bc\overline{z} + bd$ und es ergibt sich $w \in \mathbb{H}$ aus der Rechnung

$$\mathrm{Im}(w) = \tfrac{1}{2i}(w - \overline{w}) = \tfrac{1}{2i}((ad-bc)z - (ad-bc)\overline{z}) = \tfrac{1}{2i}(z - \overline{z}) = \mathrm{Im}(z) > 0\,.$$

Offensichtlich gilt $Ez = \frac{1z+0}{0z+1} = z$ und für $A' = \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right) \in \Gamma$ mit $A'z = \frac{a'z+b'}{c'z+d'}$ auch

$$\begin{aligned} A(A'z) &= \tfrac{a(A'z)+b}{c(A'z)+d} = \tfrac{a(a'z+b')+b(c'z+d')}{c(a'z+b')+d(c'z+d')} \\ &= \tfrac{(aa'+bc')z+(ab'+bd')}{(ca'+dc')z+(cb'+dd')} = (AA')z\,. \end{aligned}$$

(c) Wir behaupten $\Gamma_i = \{E, -E\}$. Zweifellos gilt $\{E, -E\} \subseteq \Gamma_i$.

Sei nun umgekehrt $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_i$. Dann gilt $\frac{ai+b}{ci+d} = i$, woraus $ai + b = -c + di$, also $c = -b$ und $d = a$ folgt. Hieraus ergibt sich $a^2 + b^2 = ad - bc = 1$ und wegen $a \in 1 + 2\mathbb{Z}$ schließt man $d = a \in \{1, -1\}$ und $c = b = 0$, also $A \in \{E, -E\}$.

(d) Die Grupe Γ ist nicht einfach, weil sie $\{E, -E\} \subseteq \mathrm{Z}(\Gamma)$ als echten nichttrivialen Normalteiler besitzt.

Aufgabe 4 (2 + 2 + 2 + 2 Punkte):

Wir fassen $\mathbb{Q}$ als Unterkörper von $\mathbb{R}$ auf.

(a) Man beweise oder widerlege, dass der Ring $\mathbb{R}[X]/(X^7 + 4X + 2)$ ein Körper ist.

(b) Man bestimme die Anzahl der Zwischenkörper der Erweiterung $\mathbb{F}_{3^{30}}/\mathbb{F}_{3^2}$.

(c) Man bestimme das Minimalpolynom von $1 + \sqrt{2}$ über $\mathbb{Q}$.

(d) Man bestimme alle Lösungen $x \in \mathbb{Z}$ des folgenden Systems von Kongruenzen:

$$\begin{aligned} x &\equiv 3 \pmod{4} \\ x &\equiv 2 \pmod{7} \\ x &\equiv 1 \pmod{11} \end{aligned}$$

Lösung:

(a) Der Ring $\mathbb{R}[X]/(X^7+4X+2)$ ist kein Körper, denn $f = X^7+4X+2$ ist reduzibel über $\mathbb{R}$. In der Tat hat f nach dem Zwischenwertsatz sogar eine Nullstelle in $\mathbb{R}$.

(b) Nach der Galoiskorrespondenz stimmt die Anzahl der Zwischenkörper von $\mathbb{F}_{3^{30}}/\mathbb{F}_{3^2}$ mit der Anzahl r der Untergruppen der Galoisgruppe $G = \mathrm{Gal}(\mathbb{F}_{3^{30}}/\mathbb{F}_{3^2})$ überein. Nun ist aber G nach Lemma 4.1.4 zyklisch von der Ordnung $\frac{30}{2} = 15$, also

$$r \;=\; \sharp\{d \in \mathbb{N} \,:\, d \mid 15\} \;=\; \sharp\{1, 3, 5, 15\} \;=\; 4\,.$$

(c) Das Polynom $(X - (1 + \sqrt{2}))(X - (1 - \sqrt{2})) = X^2 - 2X - 1$ besitzt $1 + \sqrt{2}$ als Nullstelle und hat Koeffizienten in $\mathbb{Q}$. Wegen $1 + \sqrt{2} \notin \mathbb{Q}$ ist es irreduzibel, also

$$\mathrm{Irr}(1 + \sqrt{2}, \mathbb{Q}) \;=\; X^2 - 2X - 1\,.$$

(d) Offenbar ist $x = 23$ eine Lösung. Nach dem chinesischen Restsatz ist daher $23+m\mathbb{Z}$ die Lösungsmenge mit $m = 4 \cdot 7 \cdot 11 = 308$.

Aufgabe 5 (4 + 4 Punkte):

Sei G eine endliche Gruppe. Ferner sei p eine Primzahl und $n > 2$ eine natürliche Zahl.

(a) Man zeige, dass die Anzahl der Elemente in G der Ordnung n gerade ist.

(b) Angenommen G ist eine p-Gruppe und N ist ein Normalteiler in G der Ordnung p. Man beweise, dass N im Zentrum von G enthalten ist.

Lösung:

(a) Sei $X = \{x \in G \mid \operatorname{ord}(x) = n\}$. Durch $(1 + 2\mathbb{Z}, x) \mapsto x^{-1}$ ist eine fixpunktfreie Gruppenoperation $\mathbb{Z}/2\mathbb{Z} \times X \to X$ gegeben, da $\operatorname{ord}(x^{-1}) = \operatorname{ord}(x)$, $(x^{-1})^{-1} = x$ und $x^{-1} \neq x$ für alle $x \in X$ gilt. Nach Aufgabe 5.3 (b) ist $|X|$ daher gerade.

(b) Die Gruppenoperation $G \times G \to G$ durch Konjugation schränkt sich ein zu einer Operation $G \times N \to N$, weil N ein Normalteiler in G ist. Für $N \subseteq \mathrm{Z}(G)$ ist zu zeigen, dass jede Bahn dieser eingeschränken Operation nur ein Element enthält. Hätte eine Bahn $|Gn'|$ mehr als ein Element, so wäre $|Gn'| = |G/G_{n'}| = |G|/|G_{n'}|$ ein Vielfaches von p, weil G ja eine p-Gruppe ist. Das widerspräche aber

$$p = |N| > |N| - 1 = \sum_{Gn \neq \{1\}} |Gn| \,.$$

Aufgabe 6 (4 + 4 Punkte):

Sei K ein Körper und L ein Zerfällungskörper von $f \in K[X]$ über K.

(a) Sei $n = \operatorname{grad}(f) \geq 0$. Man zeige, dass $n!$ vom Grad $[L : K]$ geteilt wird.

(b) Im Fall $\mathbb{Q} = K \subseteq L \subseteq \mathbb{C}$ und $f = X^4 - 4$ bestimme man eine $\mathbb{Q}$-Basis von L.

Lösung:

(a) Im Fall $n = 0$ ist $L = K$ und die Aussage stimmt. Sei nun $n > 0$.

Zunächst betrachten wir den Fall, in dem f irreduzibel ist. Wähle dann eine Nullstelle $\alpha \in L$ von f und schreibe $f = (X - \alpha)g$. Per Induktion wird $(n-1)!$ von $[L : K(\alpha)]$ geteilt, weil g den Grad $n-1$ und L als Zerfällungskörper besitzt. Also wird $n!$ wegen $[K(\alpha) : K] = n$ von $[L : K] = [L : K(\alpha)] \cdot [K(\alpha) : K]$ geteilt.

Im Fall, in dem f reduzibel ist, schreibe $f = gh$ mit Polynomen $g, h \in K[X]$ vom Grad kleiner n. Sei $s = \operatorname{grad}(g)$ und E der Zerfällungskörper von g über K mit $E \subseteq L$. Dann ist $\operatorname{grad}(h) = n - s$ und L ein Zerfällungskörper von h über E. Per Induktion wird $(n-s)!$ von $[L : E]$ und $s!$ von $[E : K]$ geteilt. Also wird $n!$ wegen $(n-s)! \cdot s! \mid n!$ von $[L : K] = [L : E] \cdot [E : K]$ geteilt.

(b) Die Nullstellen von f in $\mathbb{C}$ sind $\pm\sqrt{2}$ und $\pm i\sqrt{2}$. Folglich haben wir $L = \mathbb{Q}(i, \sqrt{2})$. Wegen $i \notin \mathbb{Q}$ und $\sqrt{2} \notin \mathbb{Q}(i)$ ist $\operatorname{Irr}(i, \mathbb{Q}) = X^2 + 1$ und $\operatorname{Irr}(\sqrt{2}, \mathbb{Q}(i)) = X^2 - 2$. Nach Satz 3.2.6 ist $X = \{1, i\}$ eine Basis von $\mathbb{Q}(i)$ über $\mathbb{Q}$ und $Y = \{1, \sqrt{2}\}$ eine Basis von L über $\mathbb{Q}(i)$. Also ist $XY = \{1, i, \sqrt{2}, i\sqrt{2}\}$ eine Basis von L über $\mathbb{Q}$.