Prof. Dr. Bernd Siebert

Nachklausur

Algebra
SS 2014

Bearbeitungszeit: 120 Minuten

Nachname: ____________________

Vorname: ____________________

Matrikelnr: ____________________

Es dürfen alle Vorlesungsunterlagen inklusive Übungsaufgaben und Lösungen verwendet werden. Untersagt ist jedoch die Benutzung von Büchern, eines Taschenrechners und anderer elektronischer Geräte. Jede zusätzliche beschriebene Seite muss mit Namen und Matrikelnummer beschriftet werden.

---

von den Korrektoren auszufüllen:

____

Note nach Klausurpunkten

1	2	3	4	5	6	7	8	9	10

$\sum$:

1. Die alternierende Gruppe A_4 ist die von den geraden Permutationen von S_4 gebildete Untergruppe. Zeige: $\langle(123)\rangle \subseteq A_4$ ist nicht normal.

(4 Punkte)

Lösung:
Die von dem 3-Zykel (123) erzeugte Untergruppe ist $\{1, (123), (132)\}$. Konjugation von (123) mit (12)(34) gibt (142), denn (12)(34) ist selbstinvers und

$$(12)(34)(123)(12)(34) = (142).$$

Da (142) nicht in $\langle(123)\rangle$ liegt, ist $\langle(123)\rangle$ nicht normal.

2. Sei G eine abelsche Gruppe, $T(G)$ ihre Torsionsuntergruppe und ϕ ein Homomorphismus $G \to \mathbb{R}$. Zeige: $T(G) \subseteq \ker \phi$.

(3 Punkte)

Lösung:
Sei $g \in T(G)$. Dann gibt es nach Definiton von $T(G)$ ein $n \in \mathbb{N} \setminus \{0\}$ mit $ng = 0$. Also gilt $\phi(0) = \phi(ng) = n\phi(g)$. Da $n \neq 0$ und $\mathbb{R}$ ein Integritätsbereich ist, also keine Nullteiler hat, folgt $\phi(g) = 0$.

3. Finde eine Kompositionsreihe der alternierenden Gruppe A_4. Zeigen Sie, dass die von Ihnen angegebene Reihe auch tatsächlich eine Kompositionsreihe ist.

(8 Punkte)

Lösung:
Die alternierende Gruppe A_4 besteht aus den geraden Permutationen von S_4 und $|A_4| = \frac{|S_4|}{2} = \frac{4!}{2} = 12$. Eine Kompositionsreihe ist durch

$$1 \trianglelefteq \langle (12)(13) \rangle \trianglelefteq \langle (12)(34), (13)(24) \rangle \trianglelefteq A_4$$

gegeben.

Die triviale Gruppe 1 ist offenbar normal in $\langle (12)(13) \rangle$. Das $\langle (12)(13) \rangle$ normal in $\langle (12)(34), (13)(24) \rangle$ ist, folgt, da $\langle (12)(13) \rangle$ zwei Elemente hat und $\langle (12)(34), (13)(24) \rangle$ vier, der Index von $\langle (12)(13) \rangle$ in $\langle (12)(34), (13)(24) \rangle$ also zwei ist.

Über die Slowsätze sieht man, das $\langle (12)(34), (13)(24) \rangle$ normal in A_4 ist: Die Anzahl der 3-Sylowgruppen ist entweder 1 oder 4. Da es in A_4 mehr als zwei Elemente der Ordnung 3 gibt, z.B $(123), (132)$ und (134), ist n_3 nicht 1. Es gibt also vier 3-Sylowgruppen in A_4. Damit folgt, dass es nur eine 2-Sylowgruppe in A_4 gibt, die normal in A_4 ist, denn die 3-Sylowgruppen bestehen insgesamt aus 8 Elementen der Ordnung 3 und somit bleiben wegen $|A_4| = 12$ noch 4 Elemente für die 2-Sylowgruppen. Diese ist durch $\langle (12)(34), (13)(24) \rangle$ gegeben, da beide Erzeuger Ordnung 2 haben.

Man sieht $\langle (12)(13) \rangle / 1 \cong \mathbb{Z}/2\mathbb{Z}$ und $\langle (12)(34), (13)(24) \rangle / \langle (12)(13) \rangle \cong \mathbb{Z}/2\mathbb{Z}$. Aus $[A_4 : \langle (12)(34), (13)(24)/ \rangle] = 4$ folgt auch $A_4 / \langle (12)(34), (13)(24)/ \rangle \cong \mathbb{Z}/3\mathbb{Z}$, die Faktorgruppen sind somit alle einfach.

4. Sei A ein kommutativer Ring und $\mathfrak{m} \subseteq A$ ein maximales Ideal. Sei jedes Element von $1+\mathfrak{m} := \{1+a \mid a \in \mathfrak{m}\}$ eine Einheit von A. Zeige: A besitzt nur ein maximales Ideal.

(3 Punkte)

Lösung:
Sei $x \in A \setminus \mathfrak{m}$. Da $\mathfrak{m}$ maximal ist, ist $(x) + \mathfrak{m} = A$. Es gibt also $y \in A, n \in m$ mit $yx + n = 1$. Nach Voraussetzung ist also xy eine Einheit. Also ist auch x eine Einheit.

Es ist also jedes Element in $A \setminus \mathfrak{m}$ eine Einheit. Somit enthält jedes nicht in $\mathfrak{m}$ enthaltene Ideal eine Einheit, ist also gleich A und somit nicht maximal. Also ist m das einzige maximale Ideal von A.

5. Der Ring $\mathbb{Z}[i]$ ist definiert als die Menge

$$\mathbb{Z}[i] = \{a + b \cdot i \in \mathbb{C} | a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$$

versehen mit der Addition und Multiplikation komplexer Zahlen. Zeige

$$\mathbb{Z}[i]^\times = \{1, -1, i, -i\},$$

wobei $\mathbb{Z}[i]^\times$ die Einheitengruppe von $\mathbb{Z}[i]$ ist.

(3 Punkte)

Lösung:
Die Elemente $\{1, -1, i, -i\}$ sind offenbar Einheiten. Sei umgekehrt w eine Einheit von $\mathbb{Z}[i]$. Dann gilt $wz = 1$ für ein $z \in \mathbb{Z}[i] \setminus \{0\}$. Dann gilt auch $wz\overline{wz} = 1$, also $|wz|^2 = |w|^2|z|^2 = 1$. Es folgt $w\overline{w} = |w|^2 = 1$. Schreibt man $w = x + iy$, dann ist $w^2 = x^2 + y^2 = 1$. Das bedeutet, dass entweder $x = \pm 1, y = 0$ oder $x = 0, y = \pm 1$ ist. Insgesamt gilt also $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$.

6. Schreibe $f = X^3Y + X^3Z + Y^3Z + Y^3X + Z^3X + Z^3Y$ als Polynom in den elementarsymmetrischen Polynomen $s_1, s_2, s_3 \in \mathbb{Q}[X, Y, Z]$.

(5 Punkte)

Lösung:
Es ist $s_1 = X + Y + Z$, $s_2 = XY + YZ + XZ$ und $s_3 = XYZ$. Ordne f lexikographisch (wie im Skript 13.6). In dieser Ordnung ist X^3Z der grösste Term. Man rechnet

$$f_1 = f - s_1^2 s_2 = -2X^2Y^2 - 2X^2Z^2 - 2Y^2Z^2 - 5XYZ^2 - 5X^2YZ - 5XY^2Z.$$

Das grösste Monom in f_1 ist $-2X^2Y^2$. Damit rechne man weiter

$$f_2 = f - s_1^2 s_2 + 2s_2^2 = -X^2YZ - XY^2Z - XYZ^2.$$

Die rechte Seite des letzten Ausdrucks ist $-s_1 s_3$. Somit gilt

$$f = s_1^2 s_2 - 2s_2^2 - s_1 s_3.$$

7. Sei $f = X^2 + 1 \in \mathbb{F}_3[X]$ und $g = X^2 + X + 2 \in \mathbb{F}_3[X]$. Bestimme $h \in \mathbb{F}_3[X]$ so, dass

$$\begin{aligned} \mathbb{F}_3[X]/(f) &\to \mathbb{F}_3[X]/(g) \\ x &\mapsto h \end{aligned}$$

ein Isomorphismus ist.

(5 Punkte)

Lösung:
Betrachte den Ringhomomorphismus $\phi : \mathbb{F}_3[X] \to \mathbb{F}_3[X]$, $X \mapsto X - 1$. Dieser ist surjektiv und bildet wegen $\phi(f) = (X-1)^2 + 1 = X^2 - 2X + 2 = X^2 + X + 1 = g$ f auf g ab, steigt also ab zu einem surjektivem Homomorphismus $\mathbb{F}_3[X]/(f) \to \mathbb{F}_3[X]/(g)$. Sowohl f als auch g sind irreduzibel, also sind beide Ringe sogar Körper. Offenbar ist diese induzierte Abbildung nicht die Nullabbildung, also schon ein Isomorphismus.

8. Sei $\alpha = \sqrt[3]{5}\sqrt{7}$ und ζ eine primitive dritte Einheitswurzel.

   i. Zeige, dass $L = \mathbb{Q}(\alpha, \zeta)$ der Zerfällungskörper von $f = X^6 - 5^2 \cdot 7^3$ ist.

   ii. Zeige, dass $\mathrm{Aut}(\mathbb{Q}(\alpha, \zeta)/\mathbb{Q}(\zeta)) \simeq \mathbb{Z}/6$. (Sie dürfen ohne Beweis benutzen, dass f irredizibel über $\mathbb{Q}(\zeta)$ ist.)

($3 + 4$ Punkte)

Lösung:

i. Die Nullstellen von f in $\mathbb{C}$ sind $\{\alpha, \zeta^2\alpha, \zeta\alpha, -\alpha, \zeta^2\alpha, -\zeta\alpha\}$. Als Unterkörper von $\mathbb{C}$ enthält der Zerfällungskörper L somit α und $\zeta = \alpha^{-1}\zeta\alpha$. Es folgt $\mathbb{Q}(\alpha, \zeta) \subseteq L$. Da f sechs Wurzeln in $\mathbb{Q}(\alpha, \zeta)$ besitzt, zerfällt f über $\mathbb{Q}(\alpha, \zeta)$ in Linearfaktoren. Somit gilt $L \subseteq \mathbb{Q}(\alpha, \zeta)$, also $L = \mathbb{Q}(\alpha, \zeta)$.

ii. First observe that $\mathbb{Q}(\zeta) = \mathbb{Q}(\xi)$ where ξ denotes the sixth root of unity. Then we can use Thm 20.2 in the script to define have an injective morphism

$$\mathrm{Aut}(\mathbb{Q}(\alpha, \zeta)/\mathbb{Q}(\zeta)) \hookrightarrow \mu_6 \simeq \mathbb{Z}/6$$

$$\Phi : \sigma \mapsto \frac{\sigma(\alpha)}{\alpha} \in \mu_6$$

To see that Φ is also surjective we use the fact that f is irreducible. So, we have $|\mathrm{Aut}(\mathbb{Q}(\alpha, \zeta)/\mathbb{Q}(\zeta))| = \deg f = 6$. Hence, surjectivity follows.

9. Sei G eine Gruppe. Für jede Primzahl p sei n_p die Anzahl der p-Sylowgruppen von G. Finde n_p für alle Primzahlen, die die Gruppenordnung teilen in den Fällen $|G| = 5 \cdot 7$ und $|G| = 5 \cdot 31$.

(4 Punkte)

Lösung:

i. Es ist $|G| = 35$, $n_7 = 1 \bmod 7$ und n_7 teilt 5, also ist $n_7 = 1$. Ebenso gilt: $n_5 = 1 \bmod 5$ und n_5 teilt 7, also $n_5 = 1$.

ii. Hier ist $n_{31} = 1 \bmod 31$ und teilt 5, also $n_{31} = 1$. Analog sieht man, dass n_5 gleich 1 oder 31 ist.

10. Sei K ein Körper und $c \in K$ algebraisch über K mit Minimalpolynom vom Grad 1 modulo 2, also $\mathrm{Irr}(c, K) = 1 \pmod 2$. Zeige, dass $K(c) = K(c^2)$ gilt.

(4 Punkte)

Lösung:
Es gilt $[K(c) : K(c^2)] \in \{1, 2\}$, denn $X^2 - c^2 = 0$ in $K(c^2)[X]$ hat c als Wurzel. Weiterhin ist

$$[K(c) : K] = [K(c) : K(c^2)][K(c^2) : K]$$

und somit folgt, da wegen $\mathrm{Irr}(c, K) = 1 \pmod 2$ der Grad $[K(c) : K]$ ungerade ist, $[K(c) : K(c^2)] = 1$. Also liegt c in $K(c^2)$, woraus die Gleichheit $K(c) = K(c^2)$ folgt.