Universität Konstanz
Fachbereich Mathematik und Statistik
Wintersemester 2020 / 2021

Prof. Dr. Salma Kuhlmann
Dr. Lothar Sebastian Krapp
07. April 2021

Nachklausur zur Algebra I (B3)

Klausurnummer: Matrikelnummer: Pseudonym:

Aufgabe	1	2	3	4	5	6	$\sum$
erreichte Punktzahl							
Korrektor (Initialen)							
Maximalpunktzahl	10	10	10	10	10	10	60

Wichtige Hinweise:

1. Überprüfen Sie Ihren Klausurbogen auf **Vollständigkeit**, d.h. das Vorhandensein aller **6 Aufgaben**.
2. Bei jeder Aufgabe ist der **vollständige Lösungsweg** zu dokumentieren. Nicht ausreichend begründete Lösungen können zu Punktabzug führen!
3. Bearbeiten Sie die folgenden Aufgaben selbstständig und **ohne die Verwendung von Hilfsmitteln** außer Schreibzeug und Papier.
4. Verwenden Sie für Ihren Aufschrieb ausschließlich einen **dokumentenechten Stift**, also insbesondere **keinen Bleistift**! Aufschriebe mit Bleistift werden nicht gewertet. Graphen und Skizzen dürfen mit Bleistift erstellt werden.
5. Schreiben Sie auf jedes Blatt Ihre Matrikelnummer.
6. Schreiben Sie Ihre Antworten leserlich auf das Blatt unter die Aufgabenstellung oder, falls der Platz nicht ausreicht, unter Angabe der bearbeiteten Aufgabe, auf das weiße Arbeitspapier. Benutzen Sie für jede Aufgabe ein eigenes Blatt. (Das gelbe Konzeptpapier dient lediglich für eigene Notizen. In der Wertung wird ausschließlich das berücksichtigt, was auf dem Klausurbogen oder dem weißen Arbeitspapier steht.)
7. In Aufgaben, in denen Definitionen verlangt werden, dürfen Sie sämtliche Begriffe aus den Vorlesungen Lineare Algebra I und Lineare Algebra II der vergangenen beiden Semester als bekannt voraussetzen. Alle anderen von Ihnen vewendeten Begriffe und Notationen müssen definiert werden.
8. Sofern nicht anders vermerkt dürfen Sie jeweils alle **Definitionen, Notationen und Ergebnisse** (außer dem zu beweisenden Resultat selbst) aus der Vorlesung und den Übungen verwenden, solange Sie diese klar benennen.
9. Die Bearbeitungszeit beträgt **180 Minuten**.

Matrikelnummer: **Seite 1 zu Aufgabe 1**

erreichte Punktzahl: **Korrektor (Initialen):**

Aufgabe 1 (10 Punkte).

(a) (2 Punkte) Formulieren Sie den **Chinesischen Restesatz**.
(Sie dürfen alle in der Formulierung auftretenden Begriffe und Notationen als bekannt voraussetzen.)

(b) (3 Punkte) Seien $m, n \in \mathbb{N}$ teilerfremd. Zeigen Sie, dass $\mathbb{Z}_m \times \mathbb{Z}_n$ als Ring isomorph zu $\mathbb{Z}_{mn}$ ist.

(c) (5 Punkte) Finden Sie alle $x \in \mathbb{Z}$, für die

$$\begin{aligned} x &\equiv 2 \mod 3, \\ x &\equiv 3 \mod 4 \text{ und} \\ x &\equiv 2 \mod 5 \end{aligned}$$

gelten.

Lösung:

(a) Seien R ein kommutativer Ring mit 1 und seien $A_1, \dots, A_k \lhd R$. Dann ist die Abbildung

$$\varphi \colon R \to \textstyle\prod_{i=1}^{k}(R/A_i),\ r \mapsto (r + A_1, \dots, r + A_k)$$

ein Ringhomomorphismus mit $\ker(\varphi) = \bigcap_{i=1}^{k} A_i$. Weiterhin gilt: Wenn für alle $i \neq j$ die Ideale A_i und A_j teilerfremd sind, dann ist φ surjektiv. In diesem Fall gilt also:

$$R/\bigcap_{i=1}^{k} A_i \simeq \prod_{i=1}^{k}(R/A_i).$$

(b) Wir wenden (a) für $R = \mathbb{Z}$, $k = 2$, $A_1 = m\mathbb{Z}$ und $A_2 = n\mathbb{Z}$ an. Bemerke zunächst, dass A_1 und A_2 teilerfremd sind: Sei $a \in \mathbb{Z}$. Nach dem euklidischen Algorithmus gibt es $b, c \in \mathbb{Z}$ mit $bm + cn = 1$, da m und n teilerfremd sind. Es gilt also

$$m(ab) + n(ac) = a.$$

Da $ab, ac \in \mathbb{Z}$ folgt schon $a \in m\mathbb{Z} + n\mathbb{Z}$. Nach (a) folgt

$$\mathbb{Z}/(m\mathbb{Z} \cap nZ) \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Letzteres ist isomorph zu $\mathbb{Z}_m \times \mathbb{Z}_n$ (siehe Beispiel 1.15).

Sei $d \in \mathbb{Z}$. Falls $d \in m\mathbb{Z} \cap n\mathbb{Z}$, dann gilt $m \mid d$ und $n \mid d$. Daraus folgt $mn = \mathrm{kgV}(m, n) \mid d$, also $d \in nm\mathbb{Z}$. Wir haben also $m\mathbb{Z} \cap n\mathbb{Z} \subseteq mn\mathbb{Z}$ gezeigt. Andererseits folgt aus $mn \mid d$ schon $m \mid d$ und $n \mid d$, also $mn\mathbb{Z} \subseteq m\mathbb{Z} \cap n\mathbb{Z}$.

Wir erhalten also $\mathbb{Z}/(m\mathbb{Z} \cap n\mathbb{Z}) = \mathbb{Z}/(mn\mathbb{Z}) \simeq \mathbb{Z}_{mn}$. Dies zeigt die Behauptung.

(c) Alle Lösungen sind von der Form $20a + 15b + 12c$ mit $a, b, c \in \mathbb{Z}$. Mit dem erweiterten euklidischen Algorithmus erhalten wir:

$$7 \cdot 3 + (-1) \cdot 20 = 1$$
$$4 \cdot 4 + (-1) \cdot 15 = 1$$
$$5 \cdot 5 + (-2) \cdot 12 = 1$$

Nun muss gelten:

$$20a \equiv 2 \mod 3$$
$$15b \equiv 3 \mod 4$$
$$12c \equiv 2 \mod 5$$

Eine Lösung ist also $x = 2 \cdot (-20) + 3 \cdot (-15) + 2 \cdot (-24) = -133$. Wegen $-133 \equiv 47 \mod 60$ sind alle anderen Lösungen also kongruent zu 47 modulo 60. Die Lösungsmenge ist also $47 + 60\mathbb{Z} = \{47 + 60z \mid z \in \mathbb{Z}\}$.

Lösung zu Aufgabe 1:

Seite 2 zu Aufgabe 1

Seite 3 zu Aufgabe 1

Fortsetzung der Lösung zu Aufgabe 1:

Seite 4 zu Aufgabe 1

Matrikelnummer: **Seite 1 zu Aufgabe 2**

erreichte Punktzahl: **Korrektor (Initialen):**

Aufgabe 2 (10 Punkte).

(a) (2 Punkte) Formulieren Sie das **Lemma von Gauß**.
(Sie dürfen alle in der Formulierung auftretenden Begriffe als bekannt voraussetzen.)

(b) (3 Punkte) Seien $p \in \mathbb{Z}[x]$, $A, B \in \mathbb{Q}[x]$ normierte Polynome mit $p = AB$ und $\deg(p) \geq 1$. Zeigen Sie, dass $A, B \in \mathbb{Z}[x]$ gilt.

(c) (5 Punkte) Entscheiden Sie, ob die folgenden Polynome irreduzibel sind:

(i) $p(x) = x^3 + 2x^2 + 1$ in $\mathbb{F}_3[x]$.
(ii) $q(x) = x^3 + 8x^2 - 3x + 301$ in $\mathbb{Q}[x]$.
(iii) $r(x) = 2x^4 + 18x^3 - 6$ in $\mathbb{Z}[x]$.
(iv) $s(x) = 4t^2x + 5t + \frac{1}{t}$ in $\mathbb{F}_7(t)[x]$.

Lösung:

(a) Sei R ein faktorieller Ring, sei $F = \mathrm{Quot}(R)$ und sei $p \in R[x]$. Wenn p reduzibel in $F[x]$ ist, so ist es reduzibel in $R[x]$:

Wenn es $A, B \in F[x]$ mit $\deg(A) \geq 1$, $\deg(B) \geq 1$ und $p = AB$ gibt, dann gibt es $r, s \in F \setminus \{0\}$ mit $rA, sB \in R[x]$ und $p = rAsB \in R[x]$.

(b) Falls $\deg(A) = 0$, so folgt $A = 1 \in \mathbb{Z}[x]$ und $B = p \in \mathbb{Z}[x]$. Analog kann die Aussage für den Fall $\deg(B) = 0$ zeigen. Seien also $\deg(A), \deg(B) \geq 1$. Nach dem Lemma von Gauß existieren $r, s \in \mathbb{Q} \setminus \{0\}$ mit $rA, sB \in \mathbb{Z}[x]$ und $p = rsAB$. Da A und B normiert sind, ist der Leitkoeffizient von rA gleich r und der Leitkoeffizient von sB gleich s. Daraus folgt $r, s \in \mathbb{Z}$. Nun ist der Leitkoeffizient von p gleich 1 und von $rsAB$ gleich rs. Daraus folgt $rs = 1$, also $r, s \in \mathbb{Z}^\times = \{-1, 1\}$. Es folgt, aus $rA, sB \in \mathbb{Z}[x]$ also schon $A, B \in \mathbb{Z}[x]$.

(c) (i) $p(x) = x^3 + 2x^2 + 1$ in $\mathbb{F}_3[x]$. Dieses Polynom hat keine Nullstellen in $\mathbb{F}_3$, da $p(0) = p(1) = -p(2) = 1$. Da p vom Grad 3 ist, zeigt dies, dass es irreduzibel ist.

(ii) $q(x) = x^3 + 8x^2 - 3x + 301$ in $\mathbb{Z}[x]$. Über $\mathbb{F}_3$ erhalten wir das Polynom $x^3 + 2x^2 + 1 = p(x)$. Da dieses irreduzibel ist, ist auch q irreduzibel in $\mathbb{Z}[x]$ nach dem Reduktionskriterium.

(iii) $r(x) = 2x^4 + 18x^3 - 6 = 2(x^4 + 9x^3 - 3)$ in $\mathbb{Z}[x]$. Da $2, x^4 + 9x^3 - 3 \notin \mathbb{Z}[x]^\times = \mathbb{Z}^\times = \{1, -1\}$, zeigt dies, dass r reduzibel ist.

(iv) $s(x) = 4t^2x + 5t + \frac{1}{t}$ in $\mathbb{F}_7(t)[x]$. Dieses Polynom ist vom Grad 1 und damit irreduzibel.

Lösung zu Aufgabe 2:

Seite 2 zu Aufgabe 2

Seite 3 zu Aufgabe 2

Fortsetzung der Lösung zu Aufgabe 2:

Seite 4 zu Aufgabe 2

Matrikelnummer: **Seite 1 zu Aufgabe 3**

erreichte Punktzahl: **Korrektor (Initialen):**

Aufgabe 3 (10 Punkte).

(a) (2 Punkte) Sei F ein Körper und sei $f \in F[x]$. Definieren Sie, was es bedeutet, dass f **separabel** ist.
(Sie dürfen den Begriff „Zerfällungskörper"als bekannt voraussetzen.)

(b) (5 Punkte) Sei K ein perfekter Körper. Beweisen Sie, dass jedes irreduzible Polynom in $K[x]$ separabel ist. Folgern Sie, dass jede algebraische Erweiterung von K separabel über K ist.

(c) (3 Punkte) Zeigen Sie, dass die folgenden Polynome separabel sind:

(i) $p(x) = x^{18} + 2x^{15} + x$ in $\mathbb{F}_3[x]$.
(ii) $q(x) = 2x^4 - 4x^2 + 2x - 2$ in $\mathbb{Q}[x]$.
(iii) $r(x) = x^3 - 3x + 5$ in $\mathbb{R}[x]$.

Lösung:

(a) f ist separabel, wenn $\deg(f) \geq 1$ und f nur einfache Nullstellen hat. Sei L der Zerfällungskörper von f über F. Dann ist $\alpha \in L$ eine einfache Nullstelle von f, falls $(x - \alpha) \mid f$, aber $(x - \alpha)^2 \nmid f$ in $L[x]$.

(b) Für den Fall $\mathrm{Char}(K) = 0$ ist diese Aussage klar: Jedes irreduzible Polynom ist dann schon separabel (siehe Korollar 13.11).

Sei also $\mathrm{Char}(K) = p \neq 0$ und sei $f \in K[x]$ mit $\deg(f) \geq 1$ irreduzibel. Nehme an, es wäre inseparabel. Ohne Einschränkung ist f normiert. Dann gilt $\mathrm{ggT}(f, Df) \neq 1$. Insbesondere haben f und Df einen gemeinsamen Teiler in $K[x]$. Da f irreduzibel, impliziert dies schon $Df = 0$. Damit gibt es ein $g \in K[x]$ mit $f(x) = g(x^p)$ (siehe Bemerkung 13.13). Setze

$$g(x) = \sum_{i=0}^{n} b_i x^i.$$

Da K perfekt ist, gibt es für jedes b_i ein $a_i \in K$ mit $a_i^p = b_i$. Dann ist

$$f(x) = \sum_{i=0}^{n} a_i^p x^{pi} = \left(\sum_{i=0}^{n} a_i x^i \right)^p$$

nach Anwendung des Frobenius-Homomorphismus. Insbesondere ist f reduzibel, ein Widerspruch.

Sei L/K eine algebraische Körpererweiterung und sei $\alpha \in L$. Dann ist $m_{\alpha,K}$ irreduzibel und damit separabel, woraus die letzte Behauptung folgt.

(c) (i) $p(x) = x^{18} + 2x^{15} + x$ in $\mathbb{F}_3[x]$: Wir haben $Dp(x) = 18x^{17} + 30x^{14} + 1 = 1$. Damit ist $\mathrm{ggT}(p, Dp) = 1$, also p ist separabel.

(ii) $q(x) = 2x^4 - 4x^2 + 2x - 2$ in $\mathbb{Q}[x]$: Betrachte $Q(x) = \frac{1}{2}q(x) = x^4 - 2x^2 + x - 1 \in \mathbb{Z}[x]$. In $\mathbb{F}_2$ wird dies zu $x^4 + x + 1$, was nach Übungen irreduzibel in $\mathbb{F}_2[x]$ ist. Nach dem Reduktionskriterium ist also Q irreduzibel über $\mathbb{Z}[x]$, nach dem Lemma von Gauß somit in $\mathbb{Q}[x]$. Also ist Q und somit auch q, welches dieselben Nullstellen wie Q hat, separabel.

(iii) $r(x) = x^3 - 3x + 5$ in $\mathbb{R}[x]$: Wir haben $Dr(x) = 3x^2 - 3 = 3(x+1)(x-1)$. Nun ist $r(1) \neq 0 \neq r(-1)$. Also haben r und Dr keine gemeinsamen Nullstellen und r ist separabel.

Lösung zu Aufgabe 3:

Seite 2 zu Aufgabe 3

Seite 3 zu Aufgabe 3

Fortsetzung der Lösung zu Aufgabe 3:

Seite 4 zu Aufgabe 3

Matrikelnummer: **Seite 1 zu Aufgabe 4**

erreichte Punktzahl: **Korrektor (Initialen):**

Aufgabe 4 (10 Punkte).

(a) (2 Punkte) Sei E/F eine Körpererweiterung. Definieren Sie $\mathrm{Gal}(E/F)$ und für $H \leq \mathrm{Gal}(E/F)$ den Ausdruck $\mathrm{Inv}(H)$.

(Sie dürfen den Begriff „Ringhomomorphismus“als bekannt voraussetzen.)

(b) (3 Punkte) Sei E/F eine Galois-Erweiterung. Zeigen Sie, dass E der Zerfällungskörper eines separablen Polynoms $p(x) \in F[x]$ ist.

(c) (5 Punkte) Sei $K = \mathbb{Q}(\sqrt{3}, \sqrt{5})$. Zeigen Sie, dass $K/\mathbb{Q}$ eine Galois-Erweiterung ist und dass $\mathrm{Gal}(K/\mathbb{Q})$ isomorph zur kleinschen Vierergruppe V ist.

Lösung:

(a) $\mathrm{Gal}(E/F) = \{\mu \in \mathrm{Aut}(E) \mid \forall a \in F\colon \mu(a) = a\}$. Hierbei ist Aut die Menge aller bijektiven Ringhomomorphismen von E nach E.

$\mathrm{Inv}(H) = \{a \in E \mid \forall \sigma \in G\colon \sigma(a) = a\}$.

(b) E/F ist normal und endlich, also ist E der Zerfällungskörper von endlich vielen Polynomen $p_1, \dots, p_n \in F[x]$. Ohne Einschränkung können wir annehmen, dass die p_i paarweise verschieden, normiert und irreduzibel über F sind. Somit ist jedes p_i das Minimalpolynom über F von einem $\alpha_i \in E$. Da E/F separabel ist, ist jedes p_i separabel. Da die p_i verschieden sind, haben sie auch keine gemeinsamen Nullstellen. Das Produkt $p_1 \cdots p_n$ ist somit auch separabel und E ist sein Zerfällungskörper. Dies zeigt die Behauptung.

(c)
- Wir zeigen, dass K der Zerfällungskörper des Polynoms $p(x) = (x^2-3)(x^2-5) \in \mathbb{Q}[x]$ ist. Bemerke zunächst, dass $p(x) = x^4 - 8x^2 + 15$ separabel ist: Betrachte hierzu $Dp(x) = 4x^3 - 16x = 4x(x+2)(x-2)$. Nun sind x^2-3 und x^2-5 in $\mathbb{Q}[x]$ irreduzibel und damit prim (z.B. mit Eisenstein für $p=3$ und $p=5$), also sind $p(x)$ und $Dp(x)$ teilerfremd in $\mathbb{Q}[x]$.
  Die Nullstellen von p in $\mathbb{C}$ sind $\pm\sqrt{3}$ und $\pm\sqrt{5}$. Diese sind schon alle in K enthalten. Weiterhin gilt $K = \mathbb{Q}(\sqrt{3}, -\sqrt{3}, \sqrt{5}, -\sqrt{5})$, weshalb K schon der Zerfällungskörper von p ist.
- Wir haben $[K : \mathbb{Q}] \leq [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}][\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2 \cdot 2 = 4$. Mit (i) folgt somit $|\mathrm{Gal}(K/\mathbb{Q})| \leq 4$. Betrachte nun die Elemente von $\mathrm{Gal}(K/\mathbb{Q})$.
  Betrachte zunächst $\mathrm{Gal}(K/\mathbb{Q}(\sqrt{3})) \subseteq \mathrm{Gal}(K/\mathbb{Q})$ und $\mathrm{Gal}(K/\mathbb{Q}(\sqrt{5})) \subseteq \mathrm{Gal}(K/\mathbb{Q})$. Nach Vorlesung existiert nun ein $\sigma \in \mathrm{Gal}(K/\mathbb{Q}(\sqrt{5}))$ mit $\sigma(\sqrt{5}) = -\sqrt{5}$ und auch ein $\tau \in \mathrm{Gal}(K/\mathbb{Q}(\sqrt{5}))$ mit $\sigma(\sqrt{3}) = -\sqrt{3}$. Bemerke nun

	id	σ	τ	$\sigma\tau$
$\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$
$\sqrt{5}$	$\sqrt{5}$	$\sqrt{5}$	$-\sqrt{5}$	$-\sqrt{5}$.

  Da aber $|\mathrm{Gal}(K/\mathbb{Q})| \leq 4$, beschreibt dies bereits die gesamte Gruppe (und es gilt $|\mathrm{Gal}(K/\mathbb{Q})| = 4$), also

$$\mathrm{Gal}(K/\mathbb{Q}) = \{\mathrm{id}, \sigma, \tau, \sigma\tau\}.$$

  Betrachte nun die Verknüpfungstabellen von $\mathrm{Gal}(K/\mathbb{Q})$ bzw. V:

	id	σ	τ	$\sigma\tau$
id	id	σ	τ	$\sigma\tau$
σ	σ	id	$\sigma\tau$	τ
τ	τ	$\sigma\tau$	id	σ
$\sigma\tau$	$\sigma\tau$	τ	σ	id

	(1)	$(12)(34)$	$(13)(24)$	$(14)(23)$
(1)	(1)	$(12)(34)$	$(13)(24)$	$(14)(23)$
$(12)(34)$	$(12)(34)$	(1)	$(14)(23)$	$(13)(24)$
$(13)(24)$	$(13)(24)$	$(14)(23)$	(1)	$(12)(34)$
$(14)(23)$	$(14)(23)$	$(13)(24)$	$(12)(34)$	(1)

Damit ist durch die Bijektion $\mathrm{id} \mapsto (1)$, $\sigma \mapsto (12)(34)$, $\tau \mapsto (13)(24)$ und $\sigma\tau \mapsto (14)(23)$ ein Gruppenisomorphismus zwischen $\mathrm{Gal}(K/\mathbb{Q})$ und V gegeben.
(Alternativ kann man zeigen, dass $\mathrm{Gal}(K/\mathbb{Q})$ kommutativ, nicht-zyklisch und von der Ordnung 4 ist und V (bis auf Isomorphie) die einzige Gruppe mit diesen Eigenschaften ist.)

Lösung zu Aufgabe 4:

Seite 2 zu Aufgabe 4

Seite 3 zu Aufgabe 4

Fortsetzung der Lösung zu Aufgabe 4:

Seite 4 zu Aufgabe 4

Matrikelnummer: **Seite 1 zu Aufgabe 5**

erreichte Punktzahl: **Korrektor (Initialen):**

Aufgabe 5 (10 Punkte).

(a) (2 Punkte) Sei G eine Gruppe und sei

$$1 = G_0 \leq G_1 \leq \ldots \leq G_s = G$$

eine Normalreihe. Definieren Sie, was es bedeutet, dass diese Normalreihe eine **Kompositionsreihe** ist.

(Sie dürfen den Begriff „Normalteiler" als bekannt voraussetzen.)

(b) (5 Punkte) Formulieren und beweisen Sie den Satz von **Jordan–Hölder**.

(c) (3 Punkte) Ermitteln Sie eine Kompositionsreihe von der 6-Diedergruppe D_6.

Lösung:

(a) Diese Reihe ist eine Kompositionsreihe, falls alle Faktorgruppen einfach sind. Eine Faktorgruppe ist durch G_{i+1}/G_i für $i \in \{0, \ldots, s-1\}$ gegeben. Hierbei ist $G_{i+1}/G_i = \{gG_i \mid g \in G_{i+1}\}$ mit $gG_i = \{gh \mid h \in G_i\}$. Weiterhin ist eine Gruppe $A \neq \{1\}$ einfach, falls ihre einzigen Normalteiler A und $\{1\}$ sind.

(b) Satz von Jordan–Hölder: Sei G eine endliche Gruppe mit $G \neq \{1\}$. Dann hat G eine Kompositionsreihe und alle Kompositionsreihen von G sind äquivalent.

(1) Beweis der ersten Aussage per Induktion nach Ordnung der Gruppe $|G| = n$:
Für den Fall $n = 2$ ist G isomorph zu $\mathbb{Z}_2$ und damit schon selbst einfach. Also ist $\{1\} \trianglelefteq G$ die einzige Kompositionsreihe.
Sei $n \in \mathbb{N}$ beliebig, aber fest. Für alle nicht-trivialen Gruppen, deren Ordnung höchstens n ist, gebe es eine Kompositionsreihe. Sei G eine Gruppe mit $|G| = n+1$. Fall G einfach ist, sind wir wie im Induktionsanfang fertig. Andernfalls besitzt G eine nicht-triviale echte einfache Gruppe, also $\{1\} \neq N_0 \trianglelefteq G$ mit $N_0 \neq G$. Falls N_0 keine maximale solche Gruppe ist, gibt es $N_1 \neq G$ mit $\{1\} \neq N_1 \trianglelefteq G$. Da G endlich ist, kann dieser Prozess nur endlich lange weitergeführt werden. Somit erhalten wir eine maximale nicht-triviale echte Untergruppe N von G.
Nun ist G/N einfach: Nach dem Korrespondenzsatz ist jede normale Untergruppe von G/N von der Form A/N für ein $A \trianglelefteq G$ mit $N \leq A$. Da N maximal war, muss schon $A = N$ oder $A = G$ gelten, in welchen Fall entweder $A/N = G/N$ oder $A/N = N/N =$ (also trivial) ist.
Da $|N| < |G| = n+1$, folgt nach Induktionsvoraussetzung, dass N eine Kompositionsreihe

$$1 = G_0 \leq G_1 \leq \ldots \leq G_{s-1} := N$$

besitzt. Dann ist

$$1 = G_0 \leq G_1 \leq \ldots \leq G_{s-1} \leq G_s = G$$

eine Kompositionsreihe von G, da $G_s/G_{s-1} = G/N$ einfach ist.

(2) Beweis der zweiten Aussage: Nach dem Korrespondenzsatz haben Kompositionsreihen keine echte Verfeinerungen: wenn $G_i \trianglelefteq N \trianglelefteq G_{i+1}$, dann $N/G_i \trianglelefteq G_{i+1}/G_i$; und wenn G_{i+1}/G_i einfach ist, dann gilt $N = G_i$ oder $N = G_{i+1}$. Nach dem Verfeinerungssatz von Schreier haben zwei beliebige Kompositionsreihen äquivalente Verfeinerungen. Somit sind zwei beliebige Kompositionsreihen bereits äquivalent.

(c) Wir haben $|D_6| = 12$. Da $|r| = 6$ erhalten wir $|D_6/\langle r\rangle| = \frac{12}{6} = 2$. Damit ist $\langle r\rangle \trianglelefteq D_6$ und $D_6/\langle r\rangle \cong \mathbb{Z}_2$, also einfach. Da $3 \mid |\langle r\rangle|$, gibt es nach dem Satz von Cauchy ein $a \in \langle r\rangle$ mit $|a| = 3$ (nämlich $a = r^2$). Es folgt $|\langle r\rangle/\langle a\rangle| = \frac{6}{3} = 2$, also $\langle a\rangle \trianglelefteq \langle r\rangle$ und $\langle r\rangle/\langle a\rangle \cong \mathbb{Z}_2$, also einfach. Zuletzt ist $|\langle a\rangle| = 3$, also $\langle a\rangle \cong \mathbb{Z}_3$, also einfach. Damit ist

$$1 \leq \langle r^2\rangle \leq \langle r\rangle \leq D_6$$

eine Kompositionsreihe.

Lösung zu Aufgabe 5:

Seite 2 zu Aufgabe 5

Seite 3 zu Aufgabe 5

Fortsetzung der Lösung zu Aufgabe 5:

Seite 4 zu Aufgabe 5

Matrikelnummer: **Seite 1 zu Aufgabe 6**

erreichte Punktzahl: **Korrektor (Initialen):**

Aufgabe 6 (10 Punkte).

(a) (3 Punkte) Formulieren Sie den **zweiten Sylow-Satz**.
(Sie dürfen alle auftretenden Begriffe und Notationen als bekannt voraussetzen.)

(b) (2 Punkte) Seien $p, q \in \mathbb{N}$ (nicht notwendigerweise verschiedene) Primzahlen und sei G eine Gruppe der Ordnung pq. Zeigen Sie, dass G auflösbar ist.

(c) (5 Punkte) Sei G eine Gruppe der Ordnung 15. Zeigen Sie, dass für jede Primzahl $s \mid |G|$ jede Sylow-s-Teilgruppe von G normal ist. Folgern Sie, dass G zyklisch und isomorph zu $\mathbb{Z}_{15}$ ist.

Lösung:

(a) Sei $p \in \mathbb{N}$ prim und sei G eine endliche Gruppe.

(1) Zwei Sylow-p-Untergruppen H_1 und H_2 von G sind zueinander konjugiert, d.h. es existiert $a \in G$ mit $H_2 = aH_1a^{-1}$.

(2) Für jede Sylow-p-Untergruppe H von G ist die Anzahl h_p der Sylow-p-Untergruppen von G ist ein Divisor von $[G : H]$ und es gilt $h_p \equiv 1 \mod p$.

(3) Jede Untergruppe von G der Ordnung p^k ist in einer Sylow-p-Untergruppe von G enthalten.

(b) Ist $p = q$, so ist $|G| = p^2$, also abelsch (siehe Aufgabe 11.4), somit auch auflösbar (siehe Bemerkung 18.8). Nehmen wir also $p \neq q$ und ohne Einschränkung $p < q$ an. Seien s_p, s_q die Anzahlen der Sylow-p- bzw. Sylow-q-Teilgruppen. Dann gilt insbesondere $s_q \mid p$, d.h. $s_q \in \{1, p\}$ (p prim) sowie $s_q \equiv 1 \mod q$. Da $q > p$, folgt $s_q = 1$. Sei also H_q die eindeutig bestimmte Sylow-q-Teilgruppe. Wie in (b)(i) wissen wir, dass $H_q \trianglelefteq G$ normal ist. Außerdem ist $|H_q| = q$, d.h. H_q ist zyklisch und damit abelsch, d.h. auch auflösbar. Analog ist G/H_q der Ordnung p und damit auflösbar. Also ist auch G auflösbar (siehe Satz 19.7).

(c) (i) $|G| = 3 \cdot 5$. Seien s_3 und s_5 die Anzahlen der Sylow-3- bzw. Sylow-5-Untergruppen von G und seien B_3 und B_5 eine feste Sylow-3- bzw. Sylow-5-Untergruppe. Nach (a) gilt

$$s_5 \mid [G : B_5] = \frac{|G|}{|B_5|} = \frac{15}{5} = 3,$$

also $s_5 \in \{1, 3\}$, und

$$s_5 \equiv 1 \mod 5,$$

woraus schon $s_5 = 1$ folgt. Weiterhin gilt

$$s_3 \mid 5$$

und

$$s_3 \equiv 1 \mod 3,$$

woraus schon $s_3 = 1$ folgt (da 5 ungleich 1 modulo 3 ist). Damit sind B_3 und B_5 die einzigen jeweiligen Sylow-s-Untergruppen. Wieder nach (a) erhalten wir für alle $g \in G$ schon $gB_3g^{-1} = B_3$ und $gB_5g^{-1} = B_5$, also $B_3, B_5 \trianglelefteq G$, wie gewünscht.

(ii) Aus Teil (i) wissen wir, dass es genau eine Sylow-3- und eine Sylow-5-Untergruppe von G gibt. Jedes Element von G der Ordnung 3 muss in einer Sylow-3-Untergruppe liegen (wegen des ersten Sylow-Satzes) und damit schon in B_3. Ebenso muss jedes Element der Ordnung 5 in B_5 liegen. Nun hat wegen des Satzes von Lagrange jedes Element von G Ordnung 1, 3, 5 oder 15. Gäbe es kein Element der Ordnung 15, so würden alle Elemente schon in $\{1\}$, B_3 und B_5 liegen. Es folgt $|G| \leq |\{1\}| + |B_3| + |B_5| = 1 + 3 + 5 = 9$, ein Widerspruch.
Also gibt es $x \in G$ mit $|x| = 15$ und damit $\langle x \rangle = G$ (also G ist zyklisch). Somit ist $G = \{0, x, \ldots, x^{14}\}$ isomorph zu $\mathbb{Z}_{15}$ via $\varphi\colon x^i \mapsto i$: Offensichtlich gilt $\varphi(1) = \varphi(x^0) = 0$. Für $i, j \in \mathbb{Z}$ seien $k, r \in \mathbb{Z}$ mit $i + j = 15k + r$ und $r \in \{0, \ldots, 14\}$. Dann gilt

$$\varphi(x^{i+j}) = \varphi(x^{15k+r}) = \varphi(x^r) = r = 15k + r = i + j$$

in $\mathbb{Z}_{15}$. Also ist φ ein Homomorphismus Zuletzt ist φ offensichtlich surjektiv, da für $j \in \mathbb{Z}_{15}$ gilt $\varphi(x^j) = j$. Da beide Mengen endlich und gleichmächtig sind, ist φ schon injektiv und damit bijektiv.

Lösung zu Aufgabe 6:

Seite 2 zu Aufgabe 6

Seite 3 zu Aufgabe 6

Fortsetzung der Lösung zu Aufgabe 6:

Seite 4 zu Aufgabe 6