Universität Konstanz
Fachbereich Mathematik und Statistik
Wintersemester 2020 / 2021

Prof. Dr. Salma Kuhlmann
Dr. Lothar Sebastian Krapp
12. März 2021

Klausur zur Algebra I (B3)

Klausurnummer: 1

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) Sei S ein kommutativer Ring mit $1 \neq 0$. Definieren Sie den Begriff eines **Hauptideals** in S. Was bedeutet es, dass S ein **Hauptidealbereich** ist?

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

(b) (5 Punkte) Zeigen Sie, dass jedes Primideal $P \neq \{0\}$ in einem Hauptidealbereich ein maximales Ideal ist.

(c) (3 Punkte) Finden Sie für die folgenden Ideale I_k von $\mathbb{Q}[x]$ ein Polynom $f_k \in \mathbb{Q}[x]$, das I_k erzeugt.

(i) $I_1 = \{f \in \mathbb{Q}[x] \mid f(-2) = f(\sqrt{3}) = 0\}$
(ii) $I_2 = \{f \in \mathbb{Q}[x] \mid f(2) = Df(2) = 0\}$
(iii) $I_3 = \{f \in \mathbb{Q}[x] \mid f(\sqrt{2}) = f(\sqrt{3}) = 0\}$

Lösung:

(a)
- Sei $a \in S$. Dann ist $\langle a \rangle = \{sa \mid s \in S\}$ das von a erzeugte Hauptideal in S.
- S ist ein Hauptidealbereich, wenn es ein Integritätsbereich ist und jedes Ideal in S ein Hauptideal ist. (Dass S ein Integritätsbereich ist, bedeutet, dass es nullteilerfrei ist, also für alle $a, b \in S$ mit $ab = 0$ schon $a = 0$ oder $b = 0$ gilt. Dieser Begriff wurde jedoch schon in der Linearen Algebra I/II eingeführt.)

(b) Sei R ein Hauptidealbereich und sei $P \lhd R$ prim mit $P \neq \{0\}$. Da R ein Hauptidealbereich ist, können wir $p \in R$ mit $P = \langle p \rangle$ wählen. Sei $M \lhd R$ maximal mit $P \subseteq M$ (siehe Proposition 2.9). Da R ein Hauptidealbereich ist, existiert $m \in R$ mit $M = \langle m \rangle$. Es folgt $p \in \langle m \rangle$. Also existiert $r \in R$ mit $rm = p$. Da P prim ist, folgt aus $rm \in P$ schon $r \in P$ oder $m \in P$.

- 1. Fall: $m \in \langle p \rangle$. Dann folgt schon $\langle m \rangle \subseteq \langle p \rangle$. Also ist P gleich M und damit maximal.
- 2. Fall: $r \in \langle p \rangle$. Dann gibt es $s \in R$ mit $r = ps$. Daraus folgt $p = rm = psm$. Durch Kürzen (was im Hauptidealbereich möglich ist) erhalten wir $1 = sm \in M$. Somit ist $m \in R^\times$ und damit $M = R$ (siehe Proposition 2.6 (i)). Dies ist ein Widerspruch dazu, dass M maximal, also insbesondere echt ist.

(c)
(i) $I_1 = \{f \in \mathbb{Q}[x] \mid f(-2) = f(\sqrt{3}) = 0\}$, $f_1(x) = (x+2)(x^2-3)$: Wir haben genau dann $f \in I_1$, wenn $(x+2) \mid f$ und $m_{\sqrt{3},\mathbb{Q}} \mid f$. Da $(x+2)$ und $m_{\sqrt{3},\mathbb{Q}}(x) = (x^2-3)$ wegen des Eisensteinkriteriums prim und damit teilerfremd in $\mathbb{Q}[x]$ sind, gilt also genau dann $f \in I_1$, wenn $f_1 \mid f$.

(ii) $I_2 = \{f \in \mathbb{Q}[x] \mid f(2) = Df(2) = 0\}$, $f_2(x) = (x-2)^2$: Wir haben genau dann $f \in I_2$, wenn 2 eine doppelte Nullstelle von f ist. Also genau dann ist $f \in I_2$, wenn $f_2 \mid f$.

(iii) $I_3 = \{f \in \mathbb{Q}[x] \mid f(\sqrt{2}) = f(\sqrt{3}) = 0\}$, $f_3(x) = (x^2-2)(x^2-3)$. Die Argumentation läuft wie in (i), da f_3 das Produkt der Minimalpolynome von $\sqrt{2}$ und $\sqrt{3}$ über $\mathbb{Q}$ ist.

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) Sei R ein Integritätsbereich. Formulieren Sie das **Eisensteinkriterium** für Polynome in $R[x]$.
(Sie dürfen alle in der Formulierung auftretenden Begriffe als bekannt voraussetzen.)

(b) (3 Punkte) Sei K ein Körper und sei $f \in K[x]$ mit $\deg(f) \in \{2,3\}$. Zeigen Sie, dass f genau dann irreduzibel in $K[x]$ ist, wenn f keine Nullstelle in K hat. Zeigen Sie zudem, dass diese Äquivalenz im Allgemeinen für $\deg(f) \geq 4$ nicht gilt.

(c) (5 Punkte) Zeigen Sie, dass die folgenden Polynome irreduzibel sind:

(i) $p(x) = -5x^7 + 75x^4 + 15x^3 - 30$ in $\mathbb{Q}[x]$.
(ii) $q(x) = x^3 + 5x^2 + 6x + 4$ in $\mathbb{Q}[x]$.
(iii) $r(x,y) = x^4 + x^2y^2 - x^2 - y + 1$ in $\mathbb{Q}[x,y]$.

Lösung:

(a) Sei $P \lhd R$ prim, $n \in \mathbb{N}$ und $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in R[x]$. Falls $a_{n-1}, \ldots, a_1, a_0 \in P$, aber $a_0 \notin P^2$, dann ist $f(x)$ irreduzibel in $R[x]$.

(b) Habe f eine Nullstelle $\alpha \in K$. Dann gilt $(x - \alpha) \mid f$, also $f = (x - \alpha)g$ für ein $g \in K[x]$. Nun ist $\deg(g) = \deg(f) - 1 \geq 1$, also $g \notin K[x]^\times = K^\times$. Damit ist f reduzibel.

Sei f nun reduzibel. Dann gibt es $g, h \in K[x] \setminus K$ mit $f = gh$. Damit ist insbesondere $\deg(g), \deg(h) \geq 1$ und wegen $\deg(f) \leq 3$ folgt schon $\deg(g) = 1$ oder $\deg(h) = 1$. Falls $\deg(g) = 1$, ist g von der Form $ax + b \in K[x]$ mit $a \neq 0$. Insbesondere hat f dann die Nullstelle $-ba^{-1}$. Analoges folgt, für den Fall $\deg(h) = 1$.

Gegenbeispiel für $\deg(f) \geq 4$: Das Polynom $f(x) = (x^2+1)(x^2+2) \in \mathbb{R}[x]$ ist offensichtlich reduzibel, hat aber keine Nullstellen in $\mathbb{R}$, da es strikt positiv ist.

(c) (i) $p(x) = -5x^7 + 75x^4 + 15x^3 - 30$ in $\mathbb{Q}[x]$ ist irreduzibel. Multipliziere zunächst mit der Einheit $-\frac{1}{5}$ und erhalte $P(x) = x^7 - 15x^4 - 3x^3 + 6$. Wende nun das Eisensteinkriterium für $p = 3$ an: 3 teilt alle Koeffizienten außer dem Leitkoeffizienten und $3^2 = 9$ teilt nicht den konstanten Koeffizienten. Damit ist $P(x)$ irreduzibel in $\mathbb{Z}[x]$ und nach dem Lemma von Gauß auch in $\mathbb{Q}[x]$. Da P und p assoziiert in $\mathbb{Q}[x]$ sind, ist auch p irreduzibel in $\mathbb{Q}[x]$.

(ii) Das Polynom q hat keine Nullstellen in $\mathbb{Z}$: Das Polynom q hat keine Nullstellen in $\mathbb{Z}$: Betrachte $q_3(x) = x^3 + 2x^2 + 1 \in \mathbb{F}_3[x]$. Für dieses gilt $q_3(0) = q_3(1) = -q_3(2) = 1$. Da q_3 keine Nullstellen in $\mathbb{F}_3$ hat, hat q keine Nullstellen in $\mathbb{Z}$. Nach (b) ist es damit irreduzibel in $\mathbb{Z}[x]$ und nach dem Lemma von Gauß damit auch in $\mathbb{Q}[x]$.

(iii) Betrachte $r(x,y) = x^4 + x^2y^2 - x^2 - y + 1 = x^4 + (y+1)(y-1)x^2 - (y+1)$ in $\mathbb{Q}[y][x]$. Das Polynom $y + 1$ ist Prim in $\mathbb{Q}[y]$, da es vom Grad 1 ist. Weiterhin teilt $y + 1$ alle Koeffizienten von $r(x,y)$ außer dem Leitkoeffizienten und $(y+1)^2$ teilt nicht den konstanten Koeffizienten $-(y+1)$ (da dieser prim ist und somit nur von 1, sich selbst und dazu Assoziierten geteilt wird). Mit dem Eisensteinkriterium erhalten wir, dass $r(x,y)$ irreduzibel in $\mathbb{Q}[y][x]$ ist.

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).
Sei K/F eine Körpererweiterung.

(a) (2 Punkte) Beschreiben Sie, wie K als F-**Vektorraum** aufgefasst werden kann. Definieren Sie den **Grad** der Körpererweiterung K/F.

(b) (3 Punkte) Sei $[K : F] = p$ mit $p \in \mathbb{N}$ prim. Zeigen Sie: Für jedes $\alpha \in K \setminus F$ gilt $F(\alpha) = K$.

(c) (5 Punkte) Berechnen Sie die Grade der folgenden Körpererweiterungen:

(i) $\mathbb{R}(\zeta)/\mathbb{R}$ für jede Nullstelle $\zeta \in \mathbb{C}$ von $p(x) = x^4 + 3x^2 + 2 \in \mathbb{R}[x]$.

(ii) $\mathbb{Q}(\sqrt[3]{5})/\mathbb{Q}$.

(iii) $\mathbb{Q}(\sqrt[3]{25})/\mathbb{Q}$.

Lösung:

(a) Der Grad $[K : F]$ ist die Dimension von K als F-Vektorraum. Die Skalarmultiplikation ist hierbei durch $\lambda v = \lambda \cdot_K v$ für alle $\lambda \in F$ und alle $v \in K$ gegeben.

(b) Da K/F eine endliche Körpererweiterung ist, ist sie algebraisch. Nach der Multiplikativität der Körpergrade gilt

$$p = [K : F] = [K : F(\alpha)][F(\alpha) : F].$$

Da $\alpha \notin F$ folgt $[F(\alpha) : F] > 1$: Aus $[F(\alpha) : F] = 1$ würde folgen, dass $F(\alpha)$ durch 1 als F-Vektorraum erzeugt ist, also $F(\alpha) = \mathrm{span}_F(1) = F$. Da dies nicht der Fall ist, haben wir $[F(\alpha) : F] > 1$.

Weiterhin folgt aus $[F(\alpha) : F] \mid p$, dass $[F(\alpha) : F] = p$ und damit $[K : F(\alpha)] = 1$. Dies impliziert $K = F(\alpha)$ mit demselben Argument wie zuvor.

(c) Bemerke, dass für eine Körpererweiterung K/F und $\alpha \in K$ stets $[F(\alpha) : F] = \deg m_{\alpha,F}(x)$ gilt (Proposition 10.6).

(i) $[\mathbb{R}(\zeta) : \mathbb{R}] = 2$ für jede Nullstelle $\zeta \in \mathbb{C}$ von $p(x) = x^4 + 3x^2 + 2 \in \mathbb{R}[x]$: Wir faktorisieren $p(x) = (x^2 + 1)(x^2 + 2)$ und sehen, dass keine Nullstelle von p in $\mathbb{R}$ liegt, da beide quadratischen Faktoren strikt positiv sind. Daher sind beide Primfaktoren irreduzibel und jede Nullstelle von p hat ein Minimalpolynom über $\mathbb{R}$ vom Grad 2. Daraus folgt schon die Behauptung.

(ii) $[\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = 3$. Wir haben $m(x) := m_{\sqrt[3]{5},\mathbb{Q}}(x) = x^3 - 5$. Offensichtlich ist $\sqrt[3]{5}$ eine Nullstelle von m. Weiterhin können wir das Eisensteinkriterium für $p = 5$ anwenden und erhalten so, dass m irreduzibel in $\mathbb{Z}[x]$ und mit dem Lemma von Gauß damit in $\mathbb{Q}[x]$ ist.

(iii) $[\mathbb{Q}(\sqrt[3]{25}) : \mathbb{Q}] = 3$. Wir bemerken zunächst, dass $\mathbb{Q}((\sqrt[3]{5})^2) = \mathbb{Q}(\sqrt[3]{25}) \subseteq \mathbb{Q}(\sqrt[3]{5})$. Für die Behauptung genügt es zu zeigen, dass schon Gleichheit gilt. Mit (b) genügt es zu zeigen, dass $\sqrt[3]{25} \notin \mathbb{Q}$. Dies kann man mit einem Standardargument zeigen (z.B. ähnlich dem Beweis, dass $\sqrt{2}$ irrational ist).

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) (3 Punkte) Formulieren Sie den **Hauptsatz der Galoistheorie**.
(Sie dürfen alle auftretenden Begriffe und Notationen als bekannt voraussetzen.)

(b) (2 Punkte) Sei K/F eine Galois-Erweiterung mit abelscher Galoisgruppe $\mathrm{Gal}(K/F)$. Zeigen Sie, dass jeder Zwischenkörper der Erweiterung K/F eine Galois-Erweiterung von F ist.

(c) (5 Punkte) Sei $p(x) = (x^2+1)(x^2-2) \in \mathbb{Q}[x]$ und sei K der Zerfällungskörper von $p(x)$. Bestimmen Sie die Galoisgruppe $\mathrm{Gal}(K/\mathbb{Q})$ und geben Sie alle Zwischenkörper der Erweiterung $K/\mathbb{Q}$ an.

Lösung:

(a) Sei E/F eine Galois-Erweiterung mit $G = \mathrm{Gal}(E/F)$. Sei Γ die Menge der Untergruppen von G und sei Σ die Menge der Zwischenkörper von E/F. Dann sind die Abbildungen

$$H \mapsto \mathrm{Inv}(H),\ K \mapsto \mathrm{Gal}(E/K)$$

bijektiv und invers zueinander. Weiterhin:

(1) Für alle $H_1, H_2 \in \Gamma$ gilt genau dann $H_1 \supseteq H_2$, wenn $\mathrm{Inv}(H_1) \subseteq \mathrm{Inv}(H_2)$.
(2) Für alle $H \in \Gamma$ gilt $|H| = [E : \mathrm{Inv}(H)]$ und $[G : H] = [\mathrm{Inv}(H) : F]$.
(3) $H \in \Gamma$ ist genau dann normal in G, wenn $\mathrm{Inv}(H)$ normal über F ist. In diesem Fall gilt

$$\mathrm{Gal}(\mathrm{Inv}(H)/F) \cong G/H.$$

(b) Sei L ein Zwischenkörper von K/F. Wir müssen zeigen, dass L/F normal, separabel und endlich ist. Endlichkeit folgt daraus, dass K endlich über F ist und damit ebenso jede Zwischenerweiterung (z.B. wegen der Multiplikativität der Körpergrade). Weiterhin ist L separabel über F, weil K es schon ist: Für $\alpha \in L$ ist $\alpha \in K$ und damit ist $m_{\alpha,F}$ separabel.

Nach dem Hauptsatz der Galois-Theorie gibt es $H \leq G$ mit $L = \mathrm{Inv}(H)$. Da G abelsch ist, ist H normal in G und damit ist L normal über F (wieder nach dem Hauptsatz).

(c) Wir berechnen zunächst

$$K = \mathbb{Q}(\mathrm{i}, -\mathrm{i}, \sqrt{2}, -\sqrt{2}) = \mathbb{Q}(\sqrt{2}, \mathrm{i}) \subseteq \mathbb{C}.$$

Die Galois-Gruppe enthält die folgenden beiden Automorphismen, welche $\mathbb{Q}$ fixieren:

$$\sigma\colon \mathrm{i} \mapsto -\mathrm{i}, \sqrt{2} \mapsto \sqrt{2}$$

und

$$\tau\colon \mathrm{i} \mapsto \mathrm{i}, \sqrt{2} \mapsto -\sqrt{2}.$$

Weiterhin gilt

$$\sigma\tau\colon \mathrm{i} \mapsto -\mathrm{i}, \sqrt{2} \mapsto -\sqrt{2}.$$

Damit enthält $G = \mathrm{Gal}(K/\mathbb{Q})$ mindestens 4 Elemente: id, σ, τ und $\sigma\tau$. Da K als Zerfällungskörper eines separablen Polynoms (p hat vier einfache Nullstellen, wie oben explizit aufgeführt) galois über $\mathbb{Q}$ ist, gilt nach dem Hauptsatz der Galois-Theorie

$$|G| = [K : \mathbb{Q}] = 4.$$

Damit ist $G = \{\mathrm{id}, \sigma, \tau, \sigma\tau\}$.

Nach dem Hauptsatz der Galois-Theorie gibt es eine bijektive Korrespondenz zwischen den Untergruppen von G und den Zwischenkörpern von $K/\mathbb{Q}$. Nach Lagrange kann G Untergruppen der Ordnung 1, 2 und 4 besitzen. (Erstere und letztere sind $\{\mathrm{id}\}$ und G.) Die Untergruppen der Ordnung 2 sind von Elementen der Ordnung 2 erzeugt. Bemerke hierfür

$$\sigma^2 = \tau^2 = (\sigma\tau)^2 = \mathrm{id}.$$

Damit hat G drei Untergruppen der Ordnung 2, nämlich jeweils die von σ, τ bzw. $\sigma\tau$ erzeugte.

Es gibt also 5 verschiedene Zwischenkörper: $\mathbb{Q} = \mathrm{Inv}(G)$, $\mathbb{Q}(\sqrt{2}) = \mathrm{Inv}(\langle\sigma\rangle)$, $\mathbb{Q}(\mathrm{i}) = \mathrm{Inv}(\langle\tau\rangle)$, $\mathbb{Q}(\sqrt{2}\mathrm{i}) = \mathrm{Inv}(\langle\sigma\tau\rangle)$ und $K = \mathrm{Inv}(\{\mathrm{id}\})$.

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).
Sei G eine Gruppe und sei $H \leq G$.

(a) (2 Punkte) Sei $a \in G$. Definieren Sie die **linke Nebenklasse** von a bezüglich H. Definieren Sie, was es bedeutet, dass H ein **Normalteiler** von G ist.

(b) (5 Punkte) Zeigen Sie: Es gilt $H \trianglelefteq N_G(H) \leq G$, und für alle $B \leq G$ mit $H \leq B$ ist genau dann $H \trianglelefteq B$, wenn $B \leq N_G(H)$.

(c) (3 Punkte) Berechnen Sie für alle Untergruppen $A \leq S_3$ ihren Normalisator $N_{S_3}(A)$.
(Bitte führen Sie eine Fallunterscheidung nach der Ordnung von A durch.)

Lösung:

(a)
- Linke Nebenklasse: $aH = \{ah \mid h \in H\}$.
- H ist ein Normalteiler von G, wenn für alle $g \in G$ und $h \in H$ gilt:

$$ghg^{-1} \in H.$$

(b) Offensichtlich ist $1 \in N_G(H)$, da $1H1^{-1} = H$. Seien $a, b \in N_G(H)$. Dann gilt

$$ab^{-1}H(ab^{-1})^{-1} = a(b^{-1}Hb)a^{-1} = aHa^{-1} = H.$$

Hierbei ist $b^{-1}Hb = H$, da $H = bHb^{-1}$ gilt. Daraus folgt schon $ab^{-1} \in N_G(H)$ und somit ist $N_G(H)$ eine Teilgruppe von G.

Sei nun $g \in N_G(H)$ und sei $h \in H$. Dann gilt $gHg^{-1} = H$ und damit insbesondere $ghg^{-1} \in H$. Dies zeigt, dass H normal in $N_G(H)$ ist.

Wir haben $H \leq B \leq G$.

Es gelte $H \trianglelefteq B$. Sei $b \in B$. Dann gilt schon $bHb^{-1} = H$. Insbesondere ist also $b \in N_G(H)$.

Sei umgekehrt B eine Teilgruppe von $N_G(H)$. Sei $b \in B$. Dann ist nach Definition von $N_G(H)$ schon $bHb^{-1} = H$ erfüllt. Dies zeigt schon $bhb^{-1} \in H$ für alle $h \in H$ und damit ist $H \trianglelefteq B$.

(c) Wir haben in (b) gezeigt, dass $N_G(H)$ die größte Untergruppe von G ist, in der H normal ist. Sei $A \leq S_3$ und $n = |A|$.

$n = 1$: Dann ist A die triviale Gruppe $A = \{1\} \leq S$. Diese ist normal in S und damit $N_G(A) = S_3$.

$n = 2$: Dann ist A zyklisch von der Ordnung 2, also $A = \langle (ab) \rangle$ für $a, b \in \{1, 2, 3\}$ mit $a < b$. Dies ist nicht normal in S_3: Betrachte beispielsweise $a = 1$ $b = 2$, also $A = \{(12)\}$. Dann ist

$$(123)A(123)^{-1} = \{(23)\} \neq A.$$

Dies kann ebenso für die Zykel (13) und (23) mit der gleichen Konjugation gezeigt werden. Nun ist $N_G(A)$ die größte Untergruppe von G, in der A normal ist. Da $|S_3| = 6$, hat S_3 nur Untergruppen der Ordnungen 1, 2, 3 und 6 (nach Lagrange). Die einzigen Untergruppen von G, die die Gruppe A

der Ordnung 2 enthalten können, haben also Ordnung 2 und 6 (wieder nach Lagrange). Da A nicht normal in S_3 ist, folgt schon, dass $N_G(A)$ Ordnung 2 haben muss, also $N_G(A) = A$.

$n = 3$: Dann gilt $[G : A] = \frac{|G|}{|A|} = \frac{6}{3} = 2$. Damit ist nach den Übungen A normal in G und somit $N_G(A) = S_3$.

$n = 6$: Dann ist $A = S_3$ und offensichtlich normal in sich selbst, also $N_G(A) = S_3$.

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 in der Formulierung auftretenden Begriffe und Notationen als bekannt voraussetzen.)

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

(c) (5 Punkte) Sei G eine Gruppe der Ordnung 495. Zeigen Sie, dass G einen Normalteiler der Ordnung 5 oder der Ordnung 11 besitzt.

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) Nach dem Satz von Cauchy (oder auch nach dem ersten Sylowsatz) gibt es $x, y \in G$ mit $|x| = p$ und $|y| = q$. Setze $H = \langle xy \rangle$. Da $|H| \mid |G|$ nach dem Satz von Lagrange, muss $|H|$ schon Ordnung 1, p, q oder pq haben. Betrachte $(xy)^q = x^q y^q = x^q$. Das Element x^q hat Ordnung $\frac{p}{\mathrm{ggT}(p,q)} = p$. Damit enthält H ein Element der Ordnung p, also $p \mid |H|$. Analog können wir $(xy)^p = y^p$ betrachten und erhalten $q \mid |H|$. Es folgt, dass $|H| = pq$ sein muss, also $H = G$. Damit ist G zyklisch.

(c) $|G| = 495 = 3^2 \cdot 5 \cdot 11$. Seien s_5 und s_{11} die Anzahlen der Sylow-5- bzw. Sylow-11-Untergruppen von G und seien $B_5, B_{11} \leq G$ eine jeweils solche Sylow-Untergruppe, also $|B_5| = 5$ und $|B_{11}| = 11$. Dann gilt nach (a):

$$s_{11} \mid [G : B_{11}] = \frac{|G|}{|B_{11}|} = 45$$

und

$$s_{11} \equiv 1 \mod 11.$$

Aus ersterem folgt $s_{11} \in \{1, 5, 9, 45\}$. Falls $s_{11} = 1$, dann gilt wegen (a) für alle $g \in G$ schon $gB_{11}g^{-1} = B_{11}$ und damit ist B_{11} normal in G.

Sei also $s_{11} \neq 1$. Wegen

$$5 \equiv 5 \mod 11$$

und

$$9 \equiv 9 \mod 11$$

folgt schon $s_{11} = 45$, da

$$45 \equiv 1 \mod 11.$$

Es gibt also 45 verschiedene Sylow-11-Untergruppen von G. Nun hat jede dieser Gruppen die Ordnung 11, ist also zyklisch und von der Ordnung 11 (siehe Korollar 16.4).

Seien H_1 und H_2 zwei Sylow-11-Untergruppen von G mit $H_1 \neq H_2$. Nach Vorlesung (Beweis von Korollar 16.4) werden H_1 und H_2 jeweils von jedem nicht-trivialen Element erzeugt. Angenommen $H_1 \cap H_2 \neq \{1\}$, dann gäbe es $x \neq 1$ mit $x \in H_1 \cap H_2$. Aber dann ist schon $H_1 = \langle x \rangle = H_2$, ein Widerspruch. Also muss $H_1 \cap H_2 = \{1\}$ gelten.

Wir haben also gezeigt, dass je zwei verschiedene Sylow-11-Untergruppen trivialen Schnitt haben. Sei $\{H_1, \ldots, H_{45}\}$ die Menge aller verschiedenen Sylow-11-Untergruppen. Dann sind $H_1 \setminus \{1\}, \ldots, H_{45} \setminus \{1\}$ disjunkt. Insbesondere gilt

$$|G| \geq \left| \bigcup_{i=1}^{45} (H_i \setminus \{1\}) \right| = \sum_{i=1}^{45} |H_i \setminus \{1\}| = 45 \cdot 10 = 450.$$

Analog erhalten wir wegen (a): $s_5 \mid [G : B_5] = 99$, also $s_5 \in \{1, 9, 11, 99\}$, und

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

also $s_5 \in \{1, 11\}$. Wäre $s_5 = 11$, dann gäbe es mit gleicher Argumentation wie oben

$$11 \cdot 4 = 44$$

nicht-triviale Elemente in Sylow-5-Untergruppen. Insgesamt hätten wir also 494 nicht-triviale Elemente von G, die in Sylow-11- und Sylow-5-Untergruppen lägen. Da diese Elemente alle Ordnung 5 oder 11 haben, würde dies bedeuten, dass es kein Element der Ordnung 3 in G gibt, ein Widerspruch zum Satz von Cauchy. Mit gleicher Argumentation wie oben ist dann schon B_5 normal in G.

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