Universität Konstanz
Fachbereich Mathematik und Statistik
20. April 2017

Prof. Dr. Salma Kuhlmann
Gabriel Lehéricy
Simon Müller
Wintersemester 2016/2017

Nachklausur zur Algebra (B3)

Klausurnummer: 1

Matrikelnummer: Pseudonym:

Aufgabe	1	2	3	4	5	6	7	$\sum$
erreichte Punktzahl								
Korrektor (Initialen)								
Maximalpunktzahl	10	10	10	10	10	10	10	

Wichtige Hinweise:

1. Überprüfen Sie Ihren Klausurbogen auf **Vollständigkeit**, d.h. auf das Vorhandensein aller **7 Aufgaben**.
2. Von den 7 Aufgaben werden nur die **besten 6 gewertet**.
3. Bei jeder Aufgabe ist der **vollständige Lösungsweg** zu dokumentieren. Nicht ausreichend begründete Lösungen können zu Punktabzug führen!
4. Bearbeiten Sie die folgenden Aufgaben selbstständig und **ohne die Verwendung von Hilfsmitteln** außer Schreibzeug und Papier.
5. 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.
6. Schreiben Sie auf jedes Blatt Ihre Matrikelnummer.
7. 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.)
8. In Aufgaben, in denen Definitionen verlangt werden, müssen Sie besonders die unter der Frage kursiv geschriebenen Anweisungen beachten. Sie dürfen immer sämtliche Begriffe aus den Vorlesungen Lineare Algebra I des Wintersemesters 2015/2016 und Lineare Algebra II des Sommersemesters 2016 als bekannt voraussetzen. Begriffe aus der Vorlesung Algebra (B3) müssen in der Regel definiert werden, es sei denn, die Anweisung besagt etwas anderes.
9. Die Bearbeitungszeit beträgt **180 Minuten**.

Matrikelnummer: **Seite 1 zu Aufgabe 1**

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

Aufgabe 1 (10 Punkte).

(a) (2 Punkte) Definieren Sie **Primideal** und geben Sie die **Charakterisierung von Primidealen durch Faktorringe** an.

Dabei dürfen Sie die Begriffe „Ideal" und „Faktorring" sowie alle Begriffe aus den Vorlesungen Lineare Algebra I und II als bekannt voraussetzen. Alle anderen von Ihnen vewendeten Begriffe müssen definiert werden.

Sei R ein kommutativer Ring mit 1; ein ideal $I \lhd R$ ist ein Primideal, wenn folgendes gilt:

(1) I ist echt, d.h $I \neq R$

(2) Aus $ab \in I$ folgt $a \in I$ oder $b \in I$ für alle $a, b \in R$.

Ein Ideal $I \lhd R$ ist genau dann prim, wenn der Faktorring R/I ein Integritätsbereich ist.

(b) Zeigen Sie:

(a) (2 Punkte) Das von X und Y erzeugte Ideal in $\mathbb{Z}[X,Y]$ ist kein maximales Ideal von $\mathbb{Z}[X,Y]$

Sei I das Ideal. Betrachte $\phi : \mathbb{Z}[X,Y] \to \mathbb{Z}, f \mapsto f(0,0)$. f ist ein surjektiver Ringenhomomorphismus mit $\ker\phi = I$, also gilt $\mathbb{Z}[X,Y]/I \cong \mathbb{Z}$. $\mathbb{Z}[X,Y]/I$ ist also kein Körper, also ist I nicht maximal.

(b) (2 Punkte) Das von X und Y erzeugte Ideal in $\mathbb{Q}[X,Y]$ ist ein maximales Ideal von $\mathbb{Q}[X,Y]$.

Hier gilt $\mathbb{Q}[X,Y]/ < X,Y > \cong \mathbb{Q}$, also ist $\mathbb{Q}[X,Y]/ < X,Y >$ ein Körper und es folgt, daß $< X,Y >$ maximal ist.

Sie dürfen alle Definitionen, Notationen und Ergebnisse aus der Vorlesung und den Übungen verwenden, solange Sie diese klar benennen.

(c) (4 Punkte) Sei R ein kommutativer Ring mit 1, der endlich ist. Zeigen Sie, dass ein Ideal von R genau dann prim ist, wenn es maximal ist.

Sie dürfen alle Definitionen, Notationen und Ergebnisse aus der Vorlesung und den Übungen verwenden, solange Sie diese klar benennen.

Wir wissen schon aus der Vorlesung: maximal$\Rightarrow$ prim. Wir zeigen jetzt die andere Richtung

Sei $I \lhd R$ ein Primideal. Dann ist R/I ein Integritätsbereich. Wir wissen aus ÜB1, daß jeder endliche Integritätsbereich ein Körper ist, also ist R/I ein Körper, also ist I maximal.

Lösung zu Aufgabe 1:

Seite 2 zu Aufgabe 1

Matrikelnummer: **Seite 3 zu Aufgabe 1**

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

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) Definieren Sie den Begriff **Hauptidealring**. Welchen Zusammenhang gibt es zwischen euklidischen Ringen, Hauptidealringen und faktoriellen Ringen?

Dabei dürfen Sie die Begriffe „Ideal", „euklidischer Ring" und „faktorieller Ring" sowie alle Begriffe aus den Vorlesungen Lineare Algebra I und II als bekannt voraussetzen. Alle anderen von Ihnen vewendeten Begriffe müssen definiert werden.

Ein Hauptidealring ist ein Integritätsbereich R, in dem jedes Ideal ein Hauptideal ist. Ein Ideal $I \lhd R$ heißt Hauptideal, wenn es $a \in R$ gibt mit $I = aR$.

Es gilt: R euklidisch$\Rightarrow$ R Hauptidealbereich $\Rightarrow$ R faktoriell.

Sei $R := \mathbb{Z}[\sqrt{-2}] = \{n + im\sqrt{2} \mid n, m \in \mathbb{Z}\}$ und $N(z) = z\bar{z}$ für alle $z \in R$. Wir erinnern daran, dass (R, N) euklidisch ist.

(b) (4 Punkte) Zeigen Sie, dass $1 - i\sqrt{2}$ irreduzibel in R ist.

Sie dürfen alle Definitionen, Notationen und Ergebnisse aus der Vorlesung und den Übungen verwenden, solange Sie diese klar benennen.

Sei $1 - i\sqrt{2} = ab$ mit $a, b \in R$. Es gilt dann $N(a)N(b) = N(1 - i\sqrt{2}) = 3$, also gilt o.E. $N(a) = 1$. Schreibe $a = n + i\sqrt{2}m$ mit $n, m \in \mathbb{Z}$, es gilt dann $n^2 + 2m^2 = 1$, also muß $n \in \{-1, 1\}$ und $m = 0$ gelten, also ist $a = \pm 1$ eine Einheit in R.

(c) (4 Punkte) Sei $I \neq \{0\}$ ein Ideal von R. Zeigen Sie, dass der Ring R/I endlich ist.

Hinweis: Sie können zunächst bemerken, dass $\{b \in R \mid N(b) < N(a)\}$ endlich ist für alle $a \in R$.

Sie dürfen alle Definitionen, Notationen und Ergebnisse aus der Vorlesung und den Übungen verwenden, solange Sie diese klar benennen.

Wir wissen, daß (R, N) euklidisch ist, also ist R ein Hauptidealring. Es gibt also $a \in R$ mit $I = aR$. Sei jetzt $A := \{b \in R \mid N(b) < N(a)\}$. Wir zeigen, daß die Abbildung $\phi : A \to R/I, b \mapsto b + I$ surjektiv ist. Sei $b + I \in R/I$, also $b \in R$. Weil (R, N) euklidisch ist, gibt es $r \in A$ und $q \in R$ mit $b = aq + r$, und es gilt dann $b + I = r + I$, also $b + I = \phi(r) \in \phi(A)$.

Da ϕ surjektiv ist, gilt dann $\sharp(R/I) \leq \sharp A$. Es genügt also zu zeigen, daß A endlich ist. Es ist aber klar, daß es nur endlich viele Paare $(n, m) \in \mathbb{Z}^2$ gibt mit $n^2 + 2m^2 < N(a)$.

Lösung zu Aufgabe 2:

Seite 2 zu Aufgabe 2

Matrikelnummer: **Seite 3 zu Aufgabe 2**

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

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) Geben Sie das **Lemma von Gauss** und das **Eisensteinsche Kriterium** an.

Sie dürfen alle Definitionen der Vorlesung Algebra (B3) sowie alle Begriffe aus den Vorlesungen Lineare Algebra I und II als bekannt voraussetzen.

Lemma von Gauß: Sei R ein faktorieller Ring, K der Quotientenkörper von R und $f \in R[X]$. Wenn f reduzibel in $K[X]$ ist, ist f schon in $R[X]$ reduzibel.

Eisensteinsche Kriterium: Sei R ein Integritätsbereich, $\mathfrak{p}$ ein Primideal von R und $f = X^{n-1} + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in R[X]$. Falls $a_0, \ldots, a_{n-1} \in \mathfrak{p}$ und $a_0 \notin \mathfrak{p}^2$ gilt, ist f irreduzibel in $R[X]$.

(b) (4 Punkte) Bestimmen Sie in jedem der folgenden Fälle, ob das angegebene Polynom im angegebenen Ring irreduzibel ist:

(i) $f_1 = X^3 + 8X + 13$ in $\mathbb{Q}[X]$
Es gilt $f_1 \equiv X^3 - X + 1 \bmod 3$. Das hat keine Nullstelle in $\mathbb{F}_3$, also ist es irreduzibel in $\mathbb{F}_3$ (weil es vom deg≤ 3 ist), also ist es irreduzibel in $\mathbb{Z}$ nach dem Reduktionskriterium. Nach dem Lemma von Gauß ist es auch irreduzibel in $\mathbb{Q}[X]$

(ii) $f_2 = 3X^4 + 6X^2 + 9X + 6$ in $\mathbb{Z}[X]$
3 ist ein Teiler von f_2, also ist f_2 reduzibel.

(iii) $f_3 = X^7 + 21X^5 + 28X^2 + 14X + 21$ in $\mathbb{Q}[X]$
Eisenstein mit $p = 7$+Lemma von Gauß zeigt, daß f_3 irreduzibel ist.

(iv) $f_4 = \frac{1}{6}X^5 + \frac{1}{2}X^4 + 3X + 2$ in $\mathbb{Q}[X]$
Eisenstein mit $p = 3$+Lemma von Gauß zeigt, daß $6f_4$ irreduzibel in $\mathbb{Q}[X]$ ist, also ist f_4 auch irreduzibel in $\mathbb{Q}[X]$.

Sie dürfen alle Definitionen, Notationen und Ergebnisse aus der Vorlesung und den Übungen verwenden, solange Sie diese klar benennen.

(c) (4 Punkte) Sei $f := X^5 + 6X^3 + 9X + 1 - i\sqrt{2}$. Zeigen Sie, dass f irreduzibel in $\mathbb{Q}[\sqrt{-2}]$ ist, wobei $\mathbb{Q}[\sqrt{-2}] = \{r + i\sqrt{2}s \mid r, s \in \mathbb{Q}\}$ ist.

Hinweis: Benutzen Sie Aufgabe 2.

Sie dürfen alle Definitionen, Notationen und Ergebnisse aus der Vorlesung und den Übungen verwenden, solange Sie diese klar benennen.

Wir wissen, daß $1 - i\sqrt{2}$ irreduzibel in $R := \mathbb{Z}[\sqrt{-2}]$ ist (Aufgabe 2). Weil (R, N) euklidisch ist, ist dann $1 - i\sqrt{2}$ auch prim in R. Es gilt auch $1 - i\sqrt{2} \mid 6, 1 - i\sqrt{2} \mid 9$ und $(1 - i\sqrt{2})^2 \nmid 1 - i\sqrt{2}$ in R. Nach Eisenstein ist also f irreduzibel in R. Wir wissen aus einem Übungsblatt, daß $\mathbb{Q}[\sqrt{-2}] = Quot(R)$. Nach dem Lemma von Gauß ist dann f irreduzibel in $\mathbb{Q}[\sqrt{2}]$ (R ist faktoriell, weil er euklidisch ist).

Lösung zu Aufgabe 3:

Seite 2 zu Aufgabe 3

Matrikelnummer: **Seite 3 zu Aufgabe 3**

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

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) Definieren Sie den Begriff **normale Körpererweiterung**.

Sie dürfen den Begriff „algebraische Körpererweiterung" sowie alle Begriffe aus den Vorlesungen Lineare Algebra I und II als bekannt voraussetzen. Alle anderen von Ihnen vewendeten Begriffe müssen definiert werden.

Eine Körpererweiterung L/K heißt normal, falls folgendes gilt:

(a) L/K ist algebraisch.

(b) L ist der Zerfällungskörper einer Familie $\mathscr{F}$ von Polynomen in $K[X]$.

Sei $\mathscr{F} \subseteq K[X]$. Ein Zerfällungskörper von $\mathscr{F}$ ist eine Körpererweiterung E von K, so daß folgendes gilt:

(a) Jedes $f \in \mathscr{F}$ zerfällt in lineare Faktoren in $E[X]$.

(b) $E = K(\{\alpha \in E \mid \exists f \in \mathscr{F} f(\alpha) = 0\})$.

(b) (4 Punkte) Sei K die normale Hülle von $\mathbb{Q}(\sqrt{\sqrt{3}+1})/\mathbb{Q}$. Bestimmen Sie $[K : \mathbb{Q}]$.

Sie dürfen alle Definitionen, Notationen und Ergebnisse aus der Vorlesung und den Übungen verwenden, solange Sie diese klar benennen.

Wir suchen zunächst das Minimalpolynom von $\alpha := \sqrt{\sqrt{3}+1}$. Es gilt $f(\alpha) = 0$ mit $f = (X^2-1)^2 - 3 = X^4 - 2X^2 - 2$. Einsenstein mit $p = 2$+Lemma von Gauß zeigt, dass f irreduzibel über $\mathbb{Q}$ ist, also ist f das Minimalpolynom von α. Nach Definition der normalen Hülle ist K der Zerfällungskörper von f. Bemerke: weil f symmetrisch ist, gilt $f = (X-\alpha)(X+\alpha)(X-\beta)(X+\beta)$, wobei $\beta \in \mathbb{C}$ eine andere Nullstellse von f ist. Es ist also $K = \mathbb{Q}(\alpha, \beta)$. Nach dem Gradsatz gilt $[K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]$. Es gilt $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f) = 4$. Wir suchen also $[K : \mathbb{Q}(\alpha)]$.

Bemerke: $(X-\alpha)(X+\alpha)$ ist ein Teiler von f in $\mathbb{Q}(\alpha)$, also gilt $(X-\beta)(X+\beta) \in \mathbb{Q}(\alpha)[X]$; insbesondere ist $\beta^2 \in \mathbb{Q}(\alpha)$. Daraus folgt $[K : \mathbb{Q}(\alpha)] \leq 2$. Außerdem gilt $(X-\alpha)(X+\alpha)(X-\beta)(X+\beta) = X^4 - 2X^2 - 2$, also $\alpha^2\beta^2 = -2$. Weil $\alpha \in \mathbb{R}$ gilt, muß dann $\beta \in \mathbb{C}\backslash\mathbb{R}$ gelten. Weil $\mathbb{Q}(\alpha) \subset \mathbb{R}$ ist, gilt also $\beta \notin \mathbb{Q}(\alpha)$, also muß $[K : \mathbb{Q}(\alpha)] = 2$ gelten.

Es gilt also $[K : \mathbb{Q}] = 8$.

(c) (4 Punkte) Sei L/K eine algebraische Körpererweiterung, $\alpha, \beta \in L$, f das Minimalpolynom von α über K und g das Minimalpolynom von β über K. Zeigen Sie, dass f genau dann irreduzibel über $K(\beta)$ ist, wenn g irreduzibel über $K(\alpha)$ ist.

Sie dürfen alle Definitionen, Notationen und Ergebnisse aus der Vorlesung und den Übungen verwenden, solange Sie diese klar benennen.

Es genügt, eine Richtung zu zeigen. Wir nehmen an, daß f irreduzibel über $K(\beta)$ ist. Dann gilt $[K(\alpha, \beta) : K(\beta)] = \deg(f)$ (weil f das Minimalpolynom von α über $K(\beta)$ ist), $[K(\beta) : K] = \deg(g)$ (weil g das Minimalpolynom von β über K ist) und $[K(\alpha) : K] = \deg(f)$ (weil f das Minimalpolynom von α über K ist). Jetzt benutzen wir den Gradsatz:

$$\begin{aligned}
[K(\alpha,\beta):K(\alpha)]\deg(f) &= [K(\alpha,\beta):K(\alpha)][K(\alpha):K] \\
&\overset{\text{Gradsatz}}{=} [K(\alpha,\beta):K] \\
&\overset{\text{Gradsatz}}{=} [K(\alpha,\beta):K(\beta)][K(\beta):K] \\
&= \deg(f)\deg(g)
\end{aligned}$$

Daraus folgt $[K(\alpha,\beta):K(\alpha)] = \deg(g)$. Das bedeutet, daß g das Minimalpolynom von β über $K(\alpha)$ ist; insbesondere ist g irreduzibel über $K(\alpha)$.

Lösung zu Aufgabe 4:

Seite 2 zu Aufgabe 4

Matrikelnummer: **Seite 3 zu Aufgabe 4**

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

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) Geben Sie die **Bahngleichung** an.

Sie dürfen die Begriffe „Gruppenaktion" und „Index einer Untergruppe" sowie alle Begriffe aus den Vorlesungen Lineare Algebra I und II als bekannt voraussetzen. Alle anderen von Ihnen vewendeten Begriffe müssen definiert werden.

Sei G eine endliche Gruppe, die auf einer endlichen Menge S operiert. Es gilt: $|S| = \sum_{i=1}^{n} [G : Stab_{x_i}]$. Dabei ist $\{x_1, \ldots, x_n\}$ ein Vertretersystem der Bahnen der Aktion von G auf S und $Stab_{x_i} = \{g \in G \mid g.x_i = x_i\}$ für alle i. Eine Bahn ist eine Menge der Form $\{g.x \mid g \in G\}$ für ein $x \in S$.

(b) (4 Punkte) Sei G eine Gruppe der Ordnung 77, die auf einer Menge X der Ordnung 48 operiert. Zeigen Sie, dass diese Aktion einen Fixpunkt hat, d.h, dass es ein $x \in X$ existiert, so dass $g.x = x$ für alle $g \in G$.

Sie dürfen alle Definitionen, Notationen und Ergebnisse aus der Vorlesung und den Übungen verwenden, solange Sie diese klar benennen.

Wir nehmen an, daß die Aktion keinen Fuxpunkt hat. Bahngleichung: $48 = |X| = \sum_{i=1}^{n} [G : Stab_{x_i}]$. Nach Lagrange muß $[G : Stab_{x_i}] \mid 77$ gelten, und weil die Aktion keinen Fixpunkt hat muß auch $[G : Stab_{x_i}] \neq 1$ gelten. Es gilt also $48 = 11k + 7l$ mit $k, l \in \mathbb{N}$. Man prüft leich, daß dies unmöglich ist.

(c) (4 Punkte) Sei G eine endliche Gruppe und $H \lhd G$. Sei p die kleinste Primzahl, die $|G|$ teilt. Zeigen Sie: falls $|H| = p$, ist H im Zentrum von G enthalten.

Hinweis: Betrachten Sie eine Aktion von G auf H

Sie dürfen alle Definitionen, Notationen und Ergebnisse aus der Vorlesung und den Übungen verwenden, solange Sie diese klar benennen.

Weil H normal in G ist, können wir die Aktion durch Konjugation von G aus H betrachten. Bahngleichung: $p = |H| = \sum_{i=1}^{n} [G : C(x_i)]$. Nach Lagrange muß $[G : C(x_i)] \mid |G|$ gelten. Es gilt aber auch $[G : C(x_i)] < p$ (wenn $[G : C(x_i)] = p$ wäre, gäbe es dann nur eine G-Konjugationsklasse in H. Das ist aber unmöglich, weil die Klasse von 1 $\{1\}$ ist). Nach annahme muß also $[G : C(x_i)] = 1$ gelten für alle i. Das impliziert auch $n = p$ und $H = \{x_1, \ldots, x_n\}$. Es gilt also $C(x) = G$ für alle $x \in H$, also ist x im Zentrum von G.

Lösung zu Aufgabe 5:

Seite 2 zu Aufgabe 5

Matrikelnummer: **Seite 3 zu Aufgabe 5**

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

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) (2 Punkte) Geben Sie den **Satz von Lagrange** und den **ersten Sylow-Satz** an.

Sie dürfen alle Definitionen der Vorlesung Algebra B3 sowie alle Begriffe aus den Vorlesungen Lineare Algebra I und II als bekannt voraussetzen.

Satz von Lagrange: Sei G eine endliche Gruppe und $H \leq G$ eine Untergruppe. Dann ist $|H|$ ein Teiler von $|G|$ und es gilt $[G : H] = \frac{|G|}{|H|}$.

Erster Sylow-Satz: Sei G eine endliche Gruppe, $p \in \mathbb{N}$ eine Primzahl und $k \in \mathbb{N}$, so daß $p^k \mid |G|$. Dann besitzt G eine Untergruppe der Ordnung p^k.

(b) Sei G eine Gruppe der Ordnung 440. Zeigen Sie:

(i) (2 Punkte) G besitzt eine normale Untergruppe H der Ordnung 11.
$|G| = 440 = 11.5.2^3$. Sei s_{11} die Anzahl der 11-Sylow-Untergruppen von G. Nach dem zweiten Sylow-Satz, gilt $s_{11} \equiv 1 \bmod 11$ und $s_{11} \mid 40$, also $s_{11} \in \{1, 2, 4, 5, 8, 10, 20, 40\}$. Es gilt also $s_{11} = 1$. Sei also H die Einzige 11-Sylow-Untergruppe; H ist normal in G.

(ii) (3 Punkte) G besitzt genau eine Untergruppe der Ordnung 55.

Hinweis: Wenden Sie den Satz des Verband-Isomorphismus (Lattice Isomorphism theorem) auf G/H an.
Sie dürfen alle Definitionen, Notationen und Ergebnisse aus der Vorlesung und den Übungen verwenden, solange Sie diese klar benennen.
Sei $\hat{G} = G/H$. Es gilt $|\hat{G}| = 40 = 5.2^3$. Die Anzahl der 5-Sylow Untergruppen von $\hat{G}$ ist ein Teiler von 8 und ist $\equiv 1 \bmod 5$ (zweiter Sylow-Satz), also gibt es genau eine 5-Sylow-Untergruppe $\hat{F}$. Nach dem Verband-Isomorphismus gibt es eine eindeutige Untergruppe F von G mit $H \leq F \leq G$ und $F/H = \hat{F}$. Es gilt $|F| = |H|.|\hat{F}| = 55$.
Sei jetzt $F' \leq G$ eine andere Untergruppe der Ordnung 55. Weil $11 \mid |F'|$ gilt, enthält F' eine 11-Sylow-Untergruppe (erster Sylow-Satz). H ist aber die einzige 11-Sylow-Untergruppe von G, also gilt $H \leq F'$. Außdem ist $|F'/H| = 5$, also $F'/H = \hat{F}$. F ist aber die einzige Untergruppe von G mit dieser Eigenschaft, also gilt $F = F'$.

(c) (3 Punkte) Seien $p < q$ Primzahlen mit $p \nmid q - 1$. Zeigen Sie, dass jede Gruppe der Ordnung pq zyklisch ist.

Sie dürfen alle Definitionen, Notationen und Ergebnisse aus der Vorlesung und den Übungen verwenden, solange Sie diese klar benennen.

Sei G eine Gruppe der Ordnung pq. Wegen $p < q$ folgt aus dem zweiten Sylow-Satz, daß es genau eine Untergruppe $H_p \leq G$ der Ordnung p gibt. Wegen $p \nmid q - 1$ folgt aus dem zweiten Sylow-Satz, daß es genau eine Untergruppe $H_q \leq G$ der Ordnung q gibt. Sei $x \in G \backslash (H_q \cup H_p)$. Nach Lagrange gilt $|x| \mid |G| = pq$. Wenn $|x| = p$ gälte, wäre $< x >$ eine neue p-Sylow-Untergruppe von G, was unmöglich ist; ähnlich gilt $|x| \neq q$. Es muß also $|x| = pq$ gelten.

Lösung zu Aufgabe 6:

Seite 2 zu Aufgabe 6

Matrikelnummer: **Seite 3 zu Aufgabe 6**

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

Fortsetzung der Lösung zu Aufgabe 6:

Seite 4 zu Aufgabe 6

Matrikelnummer: **Seite 1 zu Aufgabe 7**

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

Aufgabe 7 (10 Punkte).

(a) (3 Punkte) Geben Sie den **Hauptsatz der Galoistheorie** an.

Sie dürfen alle Definitionen der Vorlesung Algebra (B3) sowie alle Begriffe aus den Vorlesungen Lineare Algebra I und II als bekannt voraussetzen.

Sei L/K eine Galoiserweiterung mit Galoisgruppe G. Die Abbildung $H \mapsto Inv(H)$ ist eine Bijektion zwischen der Menge aller Untergruppen von G und der Menge aller Zwischenkörper der Erweiterung L/K. Ihr Inverses ist $E \mapsto Gal(L/E)$. Ausserdem gilt für alle Untergruppen H, H_1, H_2 von G:

(1) $H_1 \subseteq H_2 \Leftrightarrow Inv(H_2) \subseteq Inv(H_1)$

(2) $|H| = [L : Inv(H)], [G : H] = [Inv(H) : K]$

(3) H ist normal in G genau dann, wenn $Inv(H)$ eine normale Erweiterung von K ist. In diesem Fall gilt $Gal(Inv(H)/K) \cong G/H$

(b) (4 Punkte) Sei K der Zerfällungskörper von $X^4 - 16X^2 + 4 \in \mathbb{Q}[X]$. Berechnen Sie $Gal(K/\mathbb{Q})$.

Sie dürfen ohne Beweis annehmen, dass $X^4 - 16X + 4$ irreduzibel über $\mathbb{Q}$ ist

Sie dürfen alle Definitionen, Notationen und Ergebnisse aus der Vorlesung und den Übungen verwenden, solange Sie diese klar benennen.

Wir suchen zunächst $[K : \mathbb{Q}]$. Weil $f := X^4 - 16X^2 + 4$ symmetrisch ist, gilt $f = (X - \alpha)(X + \alpha)(X - \beta)(X + \beta)$ mit $\alpha, \beta \in \mathbb{C}$. Nach Koeffizientenvergleich gilt $\alpha^2\beta^2 = 4$, also gilt o.E. $\beta = \frac{2}{\alpha}$, also $\beta \in \mathbb{Q}(\alpha)$. Daraus folgt $K = \mathbb{Q}(\alpha)$ und daher $[K : \mathbb{Q}] = \deg(f) = 4$.

Weil f separabel ist, ist $K/\mathbb{Q}$ galoissch, also ist $|G| = [K : \mathbb{Q}] = 4$. Es gilt also entweder $G = C_4$ oder $G = V_4$ (kleinsche Vierergruppe).

Sei $\tau, \sigma : K \to K$ die Automorphismen mit $\tau(\alpha) = \beta$ und $\sigma(\alpha) = -\beta$ (sie existieren, weil $\alpha, \beta, -\beta$ das gleiche Minimalpolynom über $\mathbb{Q}$ haben, siehe ÜB13). Mit $\beta = \frac{2}{\alpha}$ berechnet man $\tau^2(\alpha) = \sigma^2(\alpha) = \alpha$. G enthält also zwei Elemente der Ordnung 2, also ist $G \neq C_4$, also $G = V_4$.

(c) (3 Punkte) Sei K ein Körper, f ein irreduzibles separables Polynom in $K[X]$ und L der Zerfällungskörper von f. Wir nehmen an, dass $Gal(L/K)$ abelsch ist. Zeigen Sie, dass die Körpererweiterung $K(\alpha)/K$ galoissch ist für alle $\alpha \in L$.

Sie dürfen alle Definitionen, Notationen und Ergebnisse aus der Vorlesung und den Übungen verwenden, solange Sie diese klar benennen.

Da f separabel ist, ist L/K galoissch. Setze $G := Gal(L/K)$. Sei $H := Gal(L/K(\alpha))$. H ist eine Untergruppe von G. Da G abelsch ist, ist H normal in G. Nach dem Fundamentalsatz ist dann $Inv(H) = K(\alpha)$ eine normale Erweiterung von K. Weil L/K separabel ist, ist $K(\alpha)/K$ auch separabel, also ist $K(\alpha)/K$ galoissch.

Lösung zu Aufgabe 7:

Seite 2 zu Aufgabe 7

Matrikelnummer: **Seite 3 zu Aufgabe 7**

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

Fortsetzung der Lösung zu Aufgabe 7:

Seite 4 zu Aufgabe 7