Universität Konstanz
Fachbereich Mathematik und Statistik
13. März 2017

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

Klausur zur Algebra (B3)-Lösungen

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 **maximales Ideal**. Geben Sie die **Charakterisierung von maximalen Idealen 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 $M \lhd R$ heißt maximal, falls es folgende Eigenschaften erfüllt:

- M ist echt, also $M \neq R$
- Für alle Ideale $I \lhd R$ mit $M \subseteq I \subseteq R$ muss $M = I$ oder $I = R$ gelten.

Ein Ideal $M \lhd R$ ist genau dann maximal, wenn der Faktorring R/M ein Körper ist.

(b) Sei $I =< 2, X >$ das von 2 und X erzeugte Ideal in $\mathbb{Z}[X]$. Zeigen Sie:

(i) (3 Punkte) I ist ein maximales Ideal

Wir betrachten den Faktorring $Z[X]/I$. Sei

$$\begin{aligned}\phi :&\mathbb{Z}[X] \to \mathbb{F}_2\\ &f \mapsto f(0) \bmod 2\end{aligned}$$

Man sieht sofort, dass ϕ ein surjektiver Ringhomomorphismus ist. Wir zeigen jetzt, dass $Ker(\phi) = I$. Man sieht, dass X und 2 in $Ker(\phi)$ liegen, und weil $Ker(\phi)$ ein Ideal von $\mathbb{Z}[X]$ ist, muss dann $I \subseteq Ker(\phi)$ gelten. Umgekehrt: Sei $f = a_0 + a_1X + \cdots + a_nX^n \in Ker(\phi)$. Dann gilt $a_0 \equiv 0 \bmod 2$, also gibt es $b \in \mathbb{Z}$, so dass $f = 2b + X(a_1 + a_2X + \cdots + a_nX^{n-1})$, also $f \in I$.
Nach dem Homomorphiesatz gilt also $\mathbb{Z}[X]/I \cong \mathbb{F}_2$. $\mathbb{Z}[X]/I$ ist also ein Körper, also ist I ein maximales Ideal.

(ii) (2 Punkte) I ist kein Hauptideal

Wir nehmen an, dass ein $a \in \mathbb{Z}[X]$ existiert mit $< 2, X >=< a >$. Es gilt insbesondere $a \mid 2$. Wegen der Formel $\deg(fg) = \deg(f) + \deg(g)$ muss $\deg(a) \leq \deg(2)$ gelten, also $a \in \mathbb{Z}$. Wegen $X \in < a >$ gilt ausserdem $af = X$ für ein $f \in \mathbb{Z}[X]$. Sei b der Leitkoeffizient von f. Dann muss $ab = 1$ gelten, also $a \in \{-1, 1\}$. Es folgt, dass $I = \mathbb{Z}[X]$. Nach (i) ist aber I ein maximales Ideal, also insbesondere ein echtes Ideal von $\mathbb{Z}[X]$: Widerspruch.

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

(c) (3 Punkte) Sei R ein kommutativer Ring mit 1 und P ein Primideal von R. Seien I, J Ideale von R, so dass $I \cap J \subseteq P$. Zeigen Sie, dass $I \subseteq P$ oder $J \subseteq P$ gilt.

Wir nehmen an, dass $I \nsubseteq P$, also gibt es ein $x \in I \setminus P$. Wir zeigen, dass $J \subseteq P$. Sei $y \in J$. Weil I, J Ideale sind, gilt $xy \in I \cap J$, also nach Voraussetzung $xy \in P$. Weil P prim ist, muss $x \in P$ oder $y \in P$ gelten; nach Annahme ist aber $x \in P$ ausgeschlossen, also gilt $y \in P$.

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

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 **euklidischer Ring**

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

Eine Norm auf einem Ring R ist eine Abbildung von R nach $\mathbb{N}$.

Ein euklidischer Ring ist ein Integritätsbereich R, der mit einer Norm N versehen ist, so dass Folgendes gilt: für alle $a, b \in R$ mit $b \neq 0$ gibt es $q, r \in R$, so dass:

- $a = bq + r$
- $N(r) < N(b)$ oder $r = 0$

Sei $R := \mathbb{Z}[i] = \{n + im \mid n, m \in \mathbb{Z}\}$ und $N : R \to \mathbb{N}$ die Abbildung $N(z) = \bar{z}z$, wobei $\bar{z}$ das Konjugierte von z als komplexe Zahl bezeichnet.

(b) (4 Punkte) Bestimmen Sie die Einheiten von R und zeigen Sie, dass $1 + i$ irreduzibel in R ist.

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

Man sieht, dass $\{1, -1, i, -i\}$ Einheiten in R sind. Wir zeigen, dass es keine andere Einheit gibt. Sei $a \in R$ eine Einheit. Weil $N(xy) = N(x)N(y)$ für alle $x, y \in R$ ist, gilt $N(a) \mid N(1) = 1$ (in $\mathbb{Z}$), also $N(a) = 1$. Wir schreiben $a = n + im$ mit $n, m \in \mathbb{Z}$. Es gilt $N(a) = n^2 + m^2$. $N(1) = 1$ impliziert also $a \in \{1, -1, i, -i\}$.

Seien $a, b \in R$ mit $ab = 1 + i$. Es gilt $N(ab) = N(1 + i) = 2$, also $N(a)N(b) = 2$. Es folgt, dass $N(a) = 1$ oder $N(b) = 1$, OE $N(a) = 1$, also $a \in \{1, -1, i, -i\}$, also ist a eine Einheit.

(c) (4 Punkte) Zeigen Sie, dass (R, N) ein euklidischer Ring ist. *Dabei dürfen Sie ohne Beweis benutzen, dass* $Quot(R) = \mathbb{Q}[i] = \{r + is \mid r, s \in \mathbb{Q}\}$.

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

Seien $a, b \in R$. Wir suchen ein $c \in R$, so dass $N(a - bc) < N(b)$, d.h $N(\frac{a}{b} - c) < 1$. Wir schreiben $\frac{a}{b} = r + is$ mit $r, s \in \mathbb{Q}$ (das ist möglich, weil $Quot(R) = \mathbb{Q}[i]$) und $c = n + im$ mit $n, m \in \mathbb{Z}$. Es gilt $N(\frac{a}{b} - c) = (r - n)^2 + (s - m)^2$. Wir können immer n und m so wählen, dass $|r - n|, |s - m| \leq \frac{1}{2}$ gilt, und es gilt dann $N(\frac{a}{b} - c) \leq \frac{1}{4} + \frac{1}{4} < 1$. Wir haben also $a = bc + (a - bc)$ mit $c, a - bc \in R$ und $N(a - bc) < N(b)$.

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 in $K[X]$ reduzibel ist, ist f schon in $R[X]$ reduzibel, d.h: wenn $f = gh$ mit $g, h \in K[X]$ und $\deg(g), \deg(h) \geq 1$, dann gibt es $a, b \in K$ mit $ag, bh \in R$ und $f = agbh$.

Eisensteinsche Kriterium: Sei R ein Integritätsbereich, P ein Primideal von R, $n \geq 1$ eine natürliche Zahl und $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in R[X]$. Falls $a_0, \ldots a_n$ in P liegen und $a_0 \notin P^2$ gilt, ist dann 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) $f_1 = 5X^7 + 10X^4 + 20X + 10$ in $\mathbb{Z}[X]$

Dieses Polynom ist nicht irreduzibel in $\mathbb{Z}[X]$, weil $f_1 = 5(X^7 + 2X^4 + 4X + 2)$ gilt, und 5, $X^7 + 2X^4 + 4X + 2$ keine Einheiten in $\mathbb{Z}[X]$ sind.

(ii) $f_2 = 4X^4 + 8X^2 + 16X + 8$ in $\mathbb{Q}[X]$

f_2 ist genau dann irreduzibel in $\mathbb{Q}[X]$, wenn $X^4 + 2X^2 + 4X + 2$ irreduzibel in $\mathbb{Q}[X]$ ist. Eisenstein mit $p = 2$ zeigt, dass $X^4 + 2X^2 + 4X + 2$ irreduzibel in $\mathbb{Z}[X]$ ist. Nach dem Lemma von Gauss ist dann $X^4 + 2X^2 + 4X + 2$ irreduzibel in $\mathbb{Q}[X]$. f_2 ist also irreduzibel über $\mathbb{Q}$.

(iii) $f_3 = X^3 + 6X + 1$ in $\mathbb{Q}[X]$

Es gilt $f_3 = X^3 + X + 1$ mod 5. Man kann prüfen, dass dieses Polynom keine Nullstelle in $\mathbb{F}_5$ hat. Weil es Grad 3 hat, ist es dann irreduzibel über $\mathbb{F}_5$. Nach dem Reduktionskriterium ist f_3 irreduzibel in $\mathbb{Z}[X]$. Nach dem Lemma von Gauss ist dann f_3 irreduzibel in $\mathbb{Q}[X]$.

(iv) $f_4 = X^4 + 1$ in $\mathbb{R}[X]$

Es gilt $X^4 + 1 = (X - a)(X - \overline{a})(X + a)(X + \overline{a})$ mit $a = e^{\frac{i\pi}{4}}$. Bemerke: $(X - a)(X - \overline{a}) = X^2 - \sqrt{2}X + 1 \in \mathbb{R}[X]$ und $(X + a)(X + \overline{a}) = X^2 + \sqrt{2}X + 1 \in \mathbb{R}[X]$, also ist $f_4 = (X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1)$ reduzibel in $\mathbb{R}[X]$.

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 faktorieller Ring, K sein Quotientenkörper und $f, g \in K[X]$, so dass $fg \in R[X]$. Zeigen Sie: wenn a ein Koeffizient von f ist und b ein Koeffizient von g, dann gilt $ab \in R$.

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

Wir schreiben $f = a_0 + a_1X + \cdots + a_nX^n$ und $g = b_0 + b_1X + \cdots + b_mX^m$ mit $a_k, b_k \in K$ und $a_n, b_m \neq 0$. Falls $\deg(g) = 0$ ist, gilt $g = b_0$, also sind die Koeffizienten von fg die a_kb_0 für $0 \leq k \leq n$, und wegen $fg \in R[X]$ muss dann $a_kb_0 \in R$ gelten, also ist die Aussage wahr. Wir nehmen also an, dass $1 \leq \deg(f), \deg(g)$. Dann ist das Polynom fg reduzibel in $K[X]$. Weil R faktoriell ist, können wir das Lemma von Gauss anwenden: es existieren $x, y \in K$ mit $xf, yg \in R[X]$ und $xfyg = fg$, also $xy = 1$. Seien $k, l \in \{0, \ldots, n\}$. Es gilt $a_kb_l = xya_kb_l = xa_kyb_l$. Weil xa_k ein Koeffizient von $xf \in R[X]$ ist, gilt $xa_k \in R$, und weil yb_l ein Koeffizient von $yg \in R[X]$ ist, gilt $yb_l \in R$. Daraus folt $a_kb_l = xa_kyb_l \in R$.

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 die Begriffe **endlich erzeugte Körpererweiterung** und **endliche Körpererweiterung**.

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

Sei K ein Körper. Eine Körpererweiterung von K ist ein Körper L, der K enthält.

Die Erweiterung L/K heißt endlich erzeugt, falls es eine endliche Menge $S \subseteq L$ gibt, so dass $L = K(S)$, d.h L ist der kleinste Körper, der K und S enthält.

Die Erweiterung L/K heißt endlich, wenn ihr Grad endlich ist. Der Grad der Erweiterung L/K ist die Dimension von L als K-Vektorraum.

(b) (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. Wir nehmen an, dass $\deg(f)$ und $\deg(g)$ teilerfremd sind. Zeigen Sie, dass f irreduzibel über $K(\beta)$ ist.

Sei $n := \deg(f)$ und $m := \deg(g)$. Es gilt $[K(\alpha) : K] = n$ und $[K(\beta) : K] = m$. Weil $ggT(n, m) = 1$ ist, gilt $[K(\alpha, \beta) : K] = nm$ (Korollar 4 der Vorlesung 11). Nach dem Gradsatz gilt $[K(\alpha, \beta) : K] = [K(\alpha, \beta) : K(\beta)] \underbrace{[K(\beta) : K]}_{=m}$, also ist $[K(\alpha, \beta) : K(\beta)] = n = \deg(f)$. Daraus folgt, dass f das Minimalpolynom von α über $K(\beta)$ ist. Insbesondere ist f irreduzibel in $K(\beta)[X]$.

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

(c) (4 Punkte) Bestimmen Sie den Grad der Erweiterung $\mathbb{Q}(\sqrt[5]{2}, \sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

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

Wir wissen aus einem Übungsblatt, dass $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ und dass das Minimalpolynom von $\sqrt{2} + \sqrt{3}$ über $\mathbb{Q}$ den Grad 4 hat. Nach Eisenstein mit $p = 2$ und Lemma von Gauss ist $X^5 - 2$ das Minimalpolynom von $\sqrt[5]{2}$ über $\mathbb{Q}$. Aus $ggT(4, 5) = 1$ und Teil (b) dieser Aufgabe folgt, dass $X^5 - 2$ das Minimalpolynom von $\sqrt[5]{2}$ über $\mathbb{Q}(\sqrt{2} + \sqrt{3})$ ist, also gilt $[\mathbb{Q}(\sqrt[5]{2}, \sqrt{2} + \sqrt{3}) : \mathbb{Q}(\sqrt{2} + \sqrt{3})] = \deg(X^5 - 2) = 5$.

Alternativer Beweis: nach dem Gradsatz gilt $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4$ ($[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ weil $\sqrt{3} \notin \sqrt{2}$). Nach Eisenstein mit $p = 2$ und Lemma von Gauss ist $X^5 - 2$ das Minimalpolynom von $\sqrt[5]{2}$ über $\mathbb{Q}$, also ist $[\mathbb{Q}(\sqrt[5]{2}) : \mathbb{Q}] = 5$. Weil $ggT(4, 5) = 1$ gilt, ist $[\mathbb{Q}(\sqrt[5]{2}, \sqrt{2}, \sqrt{3})/\mathbb{Q}] = 4.5$. Nach dem Gradsatz gilt außerdem $4.5 = [\mathbb{Q}(\sqrt[5]{2}, \sqrt{2}, \sqrt{3})/\mathbb{Q}] = [\mathbb{Q}(\sqrt[5]{2}, \sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2}, \sqrt{3})] \underbrace{[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]}_{=4}$, also muss $[\mathbb{Q}(\sqrt[5]{2}, \sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2}, \sqrt{3})] = 5$ gelten.

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) (3 Punkte) Geben Sie die **Bahngleichung** und die **zweite Klassengleichung 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 eine Menge X operiert. Für alle $x \in X$ ist die Bahn von x die Menge $\mathcal{O}(x) = \{g.x \mid g \in G\}$. Ein Vertretersystem der Bahnen ist eine Menge $\{x_1, \ldots, x_n\}$, so dass $G = \bigcup_{k=1}^{n} \mathcal{O}(x_k)$ und $\mathcal{O}(x_k) \cap \mathcal{O}(x_l) = \varnothing$ für $k \neq l$.

Bahngleichung: Es gilt $|X| = \sum_{k=1}^{n} [G : Stab_{x_k}]$. Dabei ist $x_1, \ldots, x_n$ ein Vertretersystem der Bahnen, und $Stab_{x_k} = \{g \in G \mid g.x_k = x_k\}$ für alle k.

Klassengleichung : Es gilt $|G| = |C| + \sum_{k=1}^{n} [G : C(x_k)]$. Dabei ist $C = \{g \in G \mid \forall h \in G, \quad gh = hg\}$ das Zentrum von G, $\{x_1, \ldots, x_n\}$ ein Vertretersystem der Konjugationsklassen in $G \backslash C$ und $C(x_k) := \{g \in G \mid gx_k = x_k g\}$ für alle k.

(b) (3 Punkte) Sei G eine Gruppe der Ordnung 55, die auf eine Menge X der Ordnung 39 operiert. Zeigen Sie, dass diese Aktion einen Fixpunkt hat, d.h es existiert ein $x \in X$ mit $g.x = x$.

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

Die Bahngleichung liefert: $|X| = \sum_{k=1}^{n} [G : Stab_{x_k}]$, wobei $x_1, \ldots, x_n$ ein Vertretersystem der Bahnen ist. Wir nehmen an, dass die Aktion keinen Fixpunkt hat. Dann gilt $[G : Stab_{x_k}] \neq 1$ für alle k. Nach Lagrange gilt $[G : Stab_{x_k}] \in \{5, 11, 55\}$ für alle k. Es gilt also: $39 = |X| = \sum_{k=1}^{n} [G : Stab_{x_k}] = 5n + 11m$ für bestimmte $n, m \in \mathbb{N}$. Man prüft leicht, dass diese Gleichung keine Lösung in $\mathbb{N}^2$ hat, also ist das ein Widerspruch.

(c) (4 Punkte) Sei G eine endliche Gruppe. Zeigen Sie, dass der Index des Zentrums von G keine Primzahl ist.

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

Wir nehmen an, dass $[G : C] = p$ ein Primzahl ist. Es gibt dann insbesondere $x \in G \backslash C$. Es gilt $C \lhd C(x) \subseteq G$. Da $C(x)/C$ eine Untergruppe von G/C ist, muss nach Lagrange $|C(x)/C| \mid p$ gelten. Weil p prim ist muss dann $C(x) = C$ oder $C(x) = G$ gelten. Weil $x \in C(x) \backslash C$ gilt, ist $C \neq C(x)$, also muss $C(x) = G$ gelten. Das bedeutet aber, dass x mit allen Elementen von G kommutiert, also $x \in C$: Widerspruch.

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) (3 Punkte) Geben Sie den **zweiten 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.

Sei G eine endliche Gruppe und p ein Primzahl mit $p \mid |G|$. Es gilt:

(1) Die p-Sylow-Untergruppen von G sind zueinander konjugiert.

(2) Die Anzahl der p-Sylow-Untergruppen von G ist $\equiv 1 \bmod p$ und ist ein Teiler von $[G : H]$ für alle p-Sylow-Untergruppen H.

(3) Jede Untergruppe von G, deren Ordnung p^k für ein $k \in \mathbb{N}$ ist, ist in einer p-Sylow-Untergruppe enthalten.

(b) (4 Punkte) Sei G eine einfache Gruppe der Ordnung 120. Wie viele Elemente der Ordnung 5 gibt es in G?

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

Es gilt $|G| = 120 = 2^3.3.5$. Wir bemerken: ein $x \in G$ hat genau dann die Ordnung 5, wenn es in einem 5-Sylow-UG enthalten ist und $x \neq 1$. Sei s_5 die Anzahl der 5-Sylow-Untergruppen. Nach dem zweiten Sylow-Satz gilt $s_5 \mid 24$ und $s_5 \equiv 1 \bmod 5$. Die Möglichkeiten sind 1 und 6. Wenn $s_5 = 1$ wäre, wäre die einzige 5-Sylow-Untergruppe von G eine normale Untergruppe, was nach Voraussetzung unmöglich ist, also gilt $s_5 = 6$. Seien $H_1, \ldots, H_6$ die 5-Sylow-Untergruppen von G. Nach Lagrange gilt $H_k \cap H_l = \{1\}$ wenn $k \neq l$. Die Anzahl der Elemente der Ordnung 5 in G ist $|\bigcup_{k=1}^{6} H_k \backslash \{1\}| = 6.4 = 24$.

(c) (3 Punkte) Sei G eine Gruppe der Ordnung 68. Zeigen Sie, dass G auflösbar ist.

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

Es gilt $|G| = 68 = 2^2.17$. Sei s_{17} die Anzahl aller 17-Sylow-Untergruppen. Nach dem zweiten Sylow-Satz gilt $s_{17} \mid 4$ und $s_{17} \equiv 1 \bmod 17$. Es muss also $s_{17} = 1$ gelten. Sei H_{17} die einzige 17-Sylow-Untergruppe von G. Weil $|H_{17}| = 17$ eine Primzahl ist, ist H_{17} abelsch, und weil $s_{17} = 1$ gilt, ist H_{17} eine normale Untergruppe von G. Die Gruppe G/H_{17} hat die Ordnung 4, also ist sie abelsch. Wir haben also eine Normalreihe $\{1\} \lhd H_{17} \lhd G$ gefunden, deren Quotienten abelsch sind, und G ist damit auflösbar.

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 $f := (X^2 - 5)(X^2 - 6) \in \mathbb{Q}[X]$ und K der Zerfällungskörper von f. Geben Sie alle Zwischenkörper der Erweiterung $K/\mathbb{Q}$ an.

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

Man kann schon bemerken, dass $K = \mathbb{Q}(\sqrt{5}, \sqrt{6})$ und dass $\mathbb{Q}, \mathbb{Q}(\sqrt{5}), \mathbb{Q}(\sqrt{6}), \mathbb{Q}(\sqrt{30})$ und K Zwischenkörper der Erweiterung $K/\mathbb{Q}$ sind. Um zu prüfen, dass es keinen weiteren Zwischenkörper gibt, wendet man den Hauptsatz der Galoistheorie an.

Sei $G := Gal(K/\mathbb{Q})$. Wir suchen zunächst den Grad der Erweiterung $K/\mathbb{Q}$. Wegen $\sqrt{5} \notin \mathbb{Q}$ hat $X^2 - 5$ keine Nullstelle in $\mathbb{Q}$, und weil es den Grad 2 hat ist es dann irreduzibel in $\mathbb{Q}[X]$, also ist es das Minimalpolynom von $\sqrt{5}$ über $\mathbb{Q}$, also $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = \deg(X^2 - 5) = 2$. Ähnlich ist $X^2 - 6$ irreduzibel über $\mathbb{Q}(\sqrt{5})$ wegen $\sqrt{6} \notin \mathbb{Q}(\sqrt{5})$, also gilt $[K : \mathbb{Q}(\sqrt{5})] = 2$ (Wir nehmen an, dass $\sqrt{6} \in \mathbb{Q}(\sqrt{5})$; dann gibt es $a, b \in \mathbb{Q}$ mit $\sqrt{6} = a + b\sqrt{5}$, also $6 = a^2 + 5b^5 + 2ab\sqrt{5}$. Weil $1, \sqrt{5}$ eine $\mathbb{Q}$-Basis ist, folgt daraus, dass $ab = 0 = a^2 + 5b^2 - 6$ und daraus folgt, dass $\sqrt{6} \in \mathbb{Q}$: Widerspruch). Nach dem Gradsatz gilt $[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt{5})][\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 4$.

Weil $\mathbb{Q}$ perfekt ist, ist f separabel, also ist K eine galoissche Erweiterung von $\mathbb{Q}$, also gilt $|G| = [K : \mathbb{Q}] = 4$. Daraus folgt, dass $G \cong C_4$ oder $G \cong C_2 \times C_2$ gelten muss. Nach dem Hauptsatz werden die Zwischenkörper als die Fixkörper von Untergruppen von G gegeben. Man bemerke, dass C_4 nur drei Untergruppen hat. Wir haben aber schon 5 Zwischenkörper gefunden, also kann $G \cong C_4$ nicht gelten (sonst hätten wir einen Widerspruch zum Hauptsatz). Es gilt also $G \cong C_2 \times C_2$. Man bemerke jetzt, dass diese Gruppe genau 5 Untergruppen hat. Die fünf oben gennanten Zwischenkörper von $K/\mathbb{Q}$ sind also die einzigen Zwischenkörper von $K/\mathbb{Q}$.

Alternativ kann man auch zum Berechnen der Zwischenkörper zuerst die Galoisgruppe explizit beschreiben. Weil $X^2 - 6$ das Minimalpolynom von $\sqrt{6}$ über $\mathbb{Q}(\sqrt{5})$ ist, gibt es $\sigma \in Gal(K/\mathbb{Q}(\sqrt{5}))$ mit $\sigma(\sqrt{6}) = -\sqrt{6}$. Ähnlich gibt es $\tau \in Gal(K/\mathbb{Q}(\sqrt{6}))$ mit $\tau(\sqrt{5}) = -\sqrt{5}$. Das ergibt schon 4 Automorphismen:

$$\begin{array}{cccc} id & \sigma & \tau & \sigma\tau \\ \sqrt{5} & \sqrt{5} & \sqrt{5} & -\sqrt{5} & -\sqrt{5} \\ \sqrt{6} & \sqrt{6} & -\sqrt{6} & \sqrt{6} & -\sqrt{6} \end{array}$$

Da $|G| = 4$ gilt, ist dann $G = \{id, \sigma, \tau, \tau\sigma\}$. Man sieht, dass $G \cong C_2 \times C_2$.

Nach dem Hauptsatz werden die Zwischenkörper als die Fixkörper von Untergruppen von G gegeben. Die Untergruppen von G sind $H_0 = \{id\}, H_1 = \{id, \sigma\}, H_2 = \{id, \tau\}, H_3 = \{id, \sigma\tau\}, H_4 = G$. Es gilt $Inv(H_0) = K$, $Inv(H_1) = \mathbb{Q}(\sqrt{5}), Inv(H_2) = \mathbb{Q}(\sqrt{6}), Inv(H_3) = \mathbb{Q}(\sqrt{30})$ und $Inv(H_4) = \mathbb{Q}$. Das sind alle Zwischenkörper der Erweiterung $K/\mathbb{Q}$.

(c) (3 Punkte) Sei L/K eine Galoiserweiterung vom Grad 2^n, $n \in \mathbb{N}$. Zeigen Sie, dass es eine Galoiserweiterung von K vom Grad 2 gibt, die in L enthalten ist.

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

Sei $G := Gal(L/K)$. Nach dem ersten Sylow-Satz gibt es $H \leq G$ mit $|H| = 2^{n-1}$. Es gilt also $[G : H] = 2$, also ist H normal in G. Sei $F := Inv(H) \subseteq L$. Nach dem Hauptsatz der Galoistheorie ist die Erweiterung F/K normal und vom Grad $[G : H] = 2$. Weil L/K separabel ist, muss F/K auch separabel sein, also ist F/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