Einführung in die Algebra — Anwesenheitszettel 1

Prof. Dr. Catharina Stroppel, Dr. Martin Palmer-Anghel (Assistent) // Wintersemester 17/18

Aufgabe 1. (Untergruppen)

(a) Gelten für Untergruppen $U_1, U_2 < G$ stets die folgenden Aussagen?
  (i) $U_1 \smallsetminus U_2 < G$
  (ii) $U_1 \cap U_2 < G$

(b) Versuchen Sie, eine prägnante, zu (ii) äquivalente Aussage zu finden.

(c) Gibt es echte Untergruppen $U_1, U_2 < G$ mit $G = U_1 \cup U_2$?

(d) Sei G eine unendliche Gruppe. Zeigen Sie, dass es mindestens eine echte, nicht-triviale Untergruppe $H < G$ gibt.

*(e) Es gilt sogar, dass es unendlich viele solche Untergruppen H gibt.

Aufgabe 2. (Erzeugendensysteme)

(a) Hat jede Gruppe ein Erzeugendensystem?

(b) Bestimmen Sie alle 1-elementigen Erzeugendensysteme von $(\mathbb{Z}, +)$.

(c) Bestimmen Sie alle n-elementigen Erzeugendensysteme von $(\mathbb{Z}, +)$, die nicht verkleinert werden können (d.h. so dass keine $(n-1)$-elementige Teilmenge ein Erzeugendensystem ist).

*(d) Beschreiben Sie ein Erzeugendensystem für die Gruppe $(\mathbb{Q}, +)$. Ist diese Gruppe endlich erzeugt?

Aufgabe 3. (Die Quadratgruppe und die Vorzeichen-Permutation-Gruppen)

(a) Die Quadratgruppe D_4 besteht aus alle Isometrien eines Quadrats. Was ist die *Ordnung* $|D_4|$ dieser Gruppe? Beschreiben Sie ein Erzeugendensystem für D_4.
Hinweis: Betrachten Sie zuerst die Untergruppe aller orientierungserhaltenden Isometrien des Quadrats.

(b) Bestimmen Sie das *Zentrum* $Z(D_4)$ von D_4. Wie viele Untergruppen hat D_4?

(c) Beschreiben Sie ein Erzeugendensystem für die Gruppe WB_n aller Vorzeichen-Permutationen der Menge $\{\pm 1, \ldots, \pm n\}$.

*(d) Das Quadrat hat zwei Diagonalen, die durch eine Isometrie entweder getauscht werden oder auf sich selbst abgebildet werden. Betrachten Sie genauer was mit diesen Diagonalen passiert, wenn eine Isometrie angewandt wird, definieren Sie dadurch einen Gruppenhomomorphismus $D_4 \longrightarrow WB_2$, und zeigen Sie, das dies ein Isomorphismus ist.

Aufgabe 4. (Gruppenhomomorphismen und Gruppenisomorphismen)

(a) Bestimmen Sie alle Gruppenhomomorphismen zwischen folgenden Gruppen (jeweils mit der offensichtlichen Gruppenoperation):

$$\{e\} \qquad \mathbb{Z} \qquad \mathbb{Z}/2\mathbb{Z} \qquad \mathbb{Z}/5\mathbb{Z} \qquad \mathbb{Q} \qquad \mathbb{R} \qquad \{z \in \mathbb{C} \mid |z| = 1\}$$

(b) Sei G eine Gruppe mit der Eigenschaft, dass $\langle g \rangle$ endlich ist für jedes Element $g \in G$. Wie viele Gruppenhomomorphismen $G \longrightarrow \mathbb{Z}$ gibt es?

(c) Kann es einen Gruppenisomorphismus zwischen der additiven Gruppe $(\mathbb{Q}, +)$ und der multiplikativen Gruppe $(\mathbb{Q}_{>0}, \cdot)$ geben?
Hinweis: betrachten Sie die Quadratwurzel von $2\ldots$

Wenn ein Teil einer Aufgabe mit dem Symbol $*$ etikettiert wird, zeigt dies, dass er etwas anspruchsvoller sein sollte.

Aufgabe 5. (Torsionsmengen und Torsionsgruppen)

Sei G eine beliebige Gruppe. Wir definieren eine *Teilmenge* von G:

$$\mathrm{Tor}(G) = \{g \in G \mid \langle g \rangle \text{ ist endlich}\} \subseteq G.$$

(a) Jetzt sei G abelsch. Zeigen Sie, dass $\mathrm{Tor}(G)$ eine *Untergruppe* von G ist.

*(b) Sei $S_{\mathbb{Z}}$ die Symmetriegruppe von $\mathbb{Z}$, und sei $D_\infty < S_{\mathbb{Z}}$ die Untergruppe von allen Bijektionen $f\colon \mathbb{Z} \longrightarrow \mathbb{Z}$ so dass $|f(n+1) - f(n)| = 1$ gilt für jede $n \in \mathbb{Z}$. Zeigen Sie, dass $\mathrm{Tor}(D_\infty)$ *keine* Untergruppe von D_∞ ist.

Aufgabe 6. Sei $G = \{g_1, g_2, \ldots, g_n\}$ eine endliche abelsche Gruppe so dass $g^2 \neq e$ gilt für jedes $e \neq g \in G$. Zeigen Sie die Gleichung $g_1 g_2 \cdots g_n = e$.

Einführung in die Algebra — Übungsblatt 1

Prof. Dr. Catharina Stroppel, Dr. Martin Palmer-Anghel (Assistent) // Wintersemester 17/18

[**Abgabe**: 19. Oktober 2017, **vor** der Vorlesung, 10:00 – 10:15]

Aufgabe 1. (4 Punkte)

(a) Es seien K ein Körper und $n > 1$. Zeigen Sie, dass die Gruppe $GL(n, K)$ nicht abelsch ist.
Hinweis: Betrachten Sie zuerst den Fall $n = 2$.
(b) Berechnen Sie das Zentrum $Z(GL(n, K))$ von $GL(n, K)$.

Aufgabe 2. (5 Punkte)

Zeigen Sie:

(a) Jede endlich erzeugte Untergruppe von $(\mathbb{Q}, +)$ ist zyklisch.
(b) Die Funktion $f\colon (\mathbb{Q}, +) \longrightarrow (\mathbb{C}^\star, \cdot)$ definiert durch $f(x) = e^{2\pi i x}$ ist ein Gruppenhomomorphismus. Was sind der Kern und das Bild von f?
(c) Für jedes $g \in \mathrm{im}(f) < \mathbb{C}^\star$ ist $\langle g \rangle$ endlich.

Aufgabe 3. (3 Punkte)

Zeigen Sie, dass $\mathrm{Aut}(S_3)$ isomorph zu S_3 ist.

Aufgabe 4. (4 Punkte)

Die *Diedergruppe* D_n besteht aus alle Isometrien eines regelmäßigen Polygons mit n Kanten.

(a) Aus wie vielen Elementen besteht D_n? Ist diese Gruppe abelsch?
(b) Definieren Sie einen Gruppenhomomorphismus $g\colon D_n \longrightarrow \mathbb{Z}/2\mathbb{Z}$.
Hinweis: Benutzen Sie das Konzept der Orientierung.
(c) Was ist der Kern von g? Definieren Sie einen weiteren Gruppenhomomorphismus $s\colon \mathbb{Z}/2\mathbb{Z} \longrightarrow D_n$ so dass $g \circ s = \mathrm{id}_{\mathbb{Z}/2\mathbb{Z}}$ gilt.

Bonusaufgabe 5. (4 Bonuspunkte)

Die *Oktaedergruppe* Okt besteht aus alle Isometrien eines regelmäßigen Oktaeders.

*(a) Definieren Sie Gruppenhomomorphismen $h\colon \mathrm{Okt} \longrightarrow \mathbb{Z}/2\mathbb{Z}$ und $t\colon \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathrm{Okt}$ so dass $h \circ t = \mathrm{id}_{\mathbb{Z}/2\mathbb{Z}}$ gilt. Bestimmen Sie das Bild und den Kern von h. Wir nennen den Kern Okt^+.
*(b) Bezeichnen wir nun die Flächen des Oktaeders mit den Buchstaben $\{a, b, c, d\}$ so, dass gegenüberliegende Flächen denselben Buchstaben bekommen. Konstruieren Sie einen surjektiven Gruppenhomomorphismus $k\colon \mathrm{Okt}^+ \twoheadrightarrow S_{\{a,b,c,d\}}$.
(c) Bestimmen Sie (durch ein geometrisches Argument) die Anzahl der Elemente der Gruppen Okt und Okt^+.
(d) Folgern Sie, dass k ein Isomorphismus ist.

NB: Wenn ein Teil einer Aufgabe mit dem Symbol $*$ versehen wird, zeigt dies, dass dieser Teil etwas anspruchsvoller sein sollte.

Einführung in die Algebra — Übungsblatt 2

Prof. Dr. Catharina Stroppel, Dr. Martin Palmer-Anghel (Assistent) // Wintersemester 17/18

[**Abgabe**: 26. Oktober 2017, **vor** der Vorlesung, 10:00 – 10:15]

Aufgabe 1. (5 Punkte)

Für die folgenden Paare (G, H) von Gruppen und Untergruppen, bestimmen Sie, ob H ein Normalteiler von G ist oder nicht. Falls H ein Normalteiler ist, geben Sie eine bekannte Gruppe G' an, so dass $G/H \cong G'$ ist (begründen Sie ihre Antwort).

(a) $\{e\} < G$ (für beliebiges G)
(b) $G = (\mathbb{Q}, +)$ und $H = \mathbb{Z} < \mathbb{Q}$
Hinweis: denken Sie an einer Aufgabe des vorherigen Übungsblatts.
(c) $G = (\mathbb{C}, +)$ und $H = \mathbb{R} < \mathbb{C}$
Hinweis: definieren Sie einen Gruppenhomomorphismus $\mathbb{C} \to \mathbb{R}$ *durch* $x + \mathrm{i}y \mapsto y$.
(d) $G = (\mathbb{C}^\star, \cdot)$ und $H = \mathbb{R}^\star < \mathbb{C}^\star$
Hinweis: definieren Sie einen Gruppenhomomorphismus $\mathbb{C}^\star \to S^1 = \{e^{\mathrm{i}t} \mid t \in [0, 2\pi)\}$ *durch* $re^{\mathrm{i}t} \mapsto e^{2\mathrm{i}t}$.
(e) $SO(2) < SO(3)$ (die Untergruppe aller Rotationen von $\mathbb{R}^3$, die die z-Achse fix lässt)
(f) $O(2) < GL(2, \mathbb{R})$
(g) $SO(n) < O(n)$
(h) $S_n < WB_n$, wobei WB_n die Gruppe aller Vorzeichen-Permutationen der Menge $\{\pm 1, \ldots, \pm n\}$ ist, und ein Element $g \in WB_n$ genau dann zu S_n gehört, wenn es kein Vorzeichen ändert.
(i) $GL(2, \mathbb{R}) < GL(2, \mathbb{C})$

Aufgabe 2. (3 Punkte)

(a) Sei G und H zwei Gruppen, und $G \times H$ das Produkt der Mengen G und H. Definieren Sie eine Struktur einer Gruppe auf $G \times H$ und zeigen Sie, dass dies wohldefiniert ist.
(b) Zur Erinnerung: D_6 ist die Gruppe aller Isometrien eines Regelmäßigen Hexagons. Konstruieren Sie eine Untergruppe $G < D_6$, so dass G isomorph zu S_3 ist. Ist D_6 isomorph zum Produkt $S_3 \times \mathbb{Z}/2\mathbb{Z}$?
(c) Sei G eine endliche Gruppe, $H < G$, so dass $|G| = 2.|H|$. Zeigen Sie, dass $H \lhd G$.

Aufgabe 3. (4 Punkte)

Für n eine positive natürliche Zahl sei $\varphi(n)$ die Anzahl der natürlichen Zahlen m im Intervall $1 \leqslant m \leqslant n$, die zu n *teilerfremd* sind. Dies definiert die *Eulerische φ-Funktion* $\varphi\colon \mathbb{N} \smallsetminus \{0\} \longrightarrow \mathbb{N}$.

(a) Sei G eine zyklische Gruppe der Ordnung n. Zeigen Sie, dass es genau $\varphi(n)$ verschiedene Elemente $g \in G$ gibt mit $\langle g \rangle = G$.
(b) Wann gibt es ein Element g so dass $|\langle g \rangle| = \frac{1}{7}|G|$ gilt?
(c) Zeigen Sie: Für p eine Primzahl und $\ell \geqslant 1$ gilt $\varphi(p^\ell) = p^{\ell-1}(p-1)$.
Hinweis: Betrachten Sie zuerst den Fall $\ell = 1$.
(d) Ferner, falls n und m teilerfremd sind, so gilt $\varphi(n)\varphi(m) = \varphi(nm)$.

Aufgabe 4. (4 Punkte)

(a) Sei S_{n+1} die Gruppe aller Permutationen der Menge $\{1, \ldots, n+1\}$ und sei $S_n < S_{n+1}$ die Untergruppe aller Permutationen, die das Element $n+1$ auf sich selbst abbilden. Zeigen Sie, dass die Regel

$$(g_1 S_n, g_2 S_n) \mapsto g_1 g_2 S_n \quad : \quad S_{n+1}/S_n \times S_{n+1}/S_n \longrightarrow S_{n+1}/S_n$$

nicht wohldefiniert ist. Folgern Sie, dass S_n kein Normalteiler von S_{n+1} ist. (Dies können Sie auch direkt beweisen.)

(b) Sei $\varphi\colon G \to H$ ein surjektiver Gruppenhomomorphismus mit Kern K. Zeigen Sie, dass die Abbildung von Mengen

$$\{U \mid U < G \text{ Untergruppe mit } K \subseteq U\} \longrightarrow \{W \mid W < H \text{ Untergruppe}\}$$

durch $U \mapsto \varphi(U)$ wohldefiniert und bijektiv ist. Kann man "Untergruppe" durch "Normalteiler" ersetzen?

(c) Bestimmen Sie alle Untergruppen U von $G = \mathbb{Z}/12\mathbb{Z}$. Welche sind Normalteiler? Wie sieht jeweils G/U aus?

Bonusaufgabe 5. (4 Bonuspunkte)

(a) Der Kommutator $[G, G]$ einer Gruppe G ist die Untergruppe aller Elemente der Form

$$g_1 h_1 g_1^{-1} h_1^{-1} g_2 h_2 g_2^{-1} h_2^{-1} \cdot \cdots \cdot g_n h_n g_n^{-1} h_n^{-1}$$

für $g_1, \ldots, g_n, h_1, \ldots, h_n \in G$ und $n \geqslant 1$. Zeigen Sie, dass dies ein Normalteiler von G ist.

(b) Eine perfekte Gruppe G ist eine, für die $G = [G, G]$ gilt. Sei $P < G$ eine perfekte Untergruppe von G. Zeigen Sie, dass P in $[G, G]$ enthält ist.

*(c) Zeigen Sie, dass es für jede gegebene Gruppe G eine *größte* perfekte Untergruppe gibt, dass heißt, eine perfekte Untergruppe $\mathrm{Perf}(G) < G$, so dass jede perfekte Untergruppe $P < G$ in $\mathrm{Perf}(G)$ enthält ist.
Hinweis: seien P_1 und P_2 perfekte Untergruppen von G. Dann müssen Sie zeigen, dass es eine weitere perfekte Untergruppe P_3 von G gibt, die sowohl P_1 als auch P_2 enthält.

*(d) Zeigen Sie, dass $\mathrm{Perf}(G)$ ein Normalteiler von G ist.

(e) Folgern Sie, dass $G/\mathrm{Perf}(G)$ immer eine wohldefinierte Gruppe ist.

(f) Zeigen Sie:
   (i) Die Quotientengruppe $G/\mathrm{Perf}(G)$ is trivial, genau dann, wenn G perfekt ist.
   *(ii) Die Quotientengruppe $G/\mathrm{Perf}(G)$ is abelsch, genau dann, wenn $[G, G]$ perfekt ist.

NB: Wenn ein Teil einer Aufgabe mit dem Symbol $*$ versehen wird, zeigt dies, dass dieser Teil etwas anspruchsvoller sein sollte.

Einführung in die Algebra — Übungsblatt 3

Prof. Dr. Catharina Stroppel, Dr. Martin Palmer-Anghel (Assistent) // Wintersemester 17/18

[**Abgabe**: 2. November 2017, **vor** der Vorlesung, 10:00 – 10:15]

Aufgabe 1. (7 Punkte)

Für eine Primzahl p und $n \in \mathbb{N}$ sei $\nu_p(n)$ die größte ganze Zahl $k \geqslant 0$ so dass $p^k \mid n$.

(a) Beweisen Sie die Legendre-Formel, d.h. $\nu_p(n!) = \sum_{i=1}^{\infty} \lfloor n/p^i \rfloor$.
Hier ist $\lfloor\ \rfloor$ die Abrundungsfunktion: für $x \in \mathbb{R}$ ist $\lfloor x \rfloor = \max\{k \in \mathbb{Z} \mid k \leqslant x\}$.
Erklären Sie zuerst, warum diese Summe für eine gegebene n tatsächlich endlich ist.

(b) Benutzen Sie diese Formel um Folgendes zu beweisen: wenn $p \nmid m$, dann ist

$$\nu_p\left(\binom{p^r m}{p^k}\right) = r - k.$$

Der Rest dieser Aufgabe ist ein Beweis vom dritten Teil des Satzes von Sylow. Sei G eine endliche Gruppe, $|G| = p^r m$ wobei p eine Primzahl ist, und $p \nmid m$. Sei H eine p-Untergruppe von G und $S \in \mathrm{Syl}_p(G)$.

(c) Wenn $H < N_G(S)$, beweisen Sie, dass HS/S eine wohldefinierte p-Gruppe ist.
Hinweis: benutzen Sie einen der Isomorphiesätze.

(d) Folgern Sie, dass dies tatsächlich die triviale Gruppe ist, und deshalb ist $H < S$.

(e) Die p-Sylowuntergruppe S operiert auf $\mathrm{Syl}_p(G)$ durch Konjugation. Zeigen Sie, dass es genau einen Fixpunkt gibt.
Hinweis: zeigen Sie, dass $S' \in \mathrm{Syl}_p(G)$ genau dann ein Fixpunkt ist, wenn $S' < N_G(S)$.

(f) Folgern Sie, dass $|\mathrm{Syl}_p(G)| \equiv 1 \pmod{p}$.

(g) Zeigen Sie auch, dass $|\mathrm{Syl}_p(G)| = [G : N_G(S)]$, und deshalb ist $|\mathrm{Syl}_p(G)|$ ein Teiler von m.
Hinweis: betrachten Sie die Operation der ganzen Gruppe G auf $\mathrm{Syl}_p(G)$ durch Konjugation.

Aufgabe 2. (5 Punkte)

(a) Sei G eine Gruppe, die auf einer Menge X operiert. Für $x \in X$ und $g \in G$ zeigen Sie, dass G_x und G_{gx} in derselben Konjugationsklasse liegen.

Betrachten Sie die folgenden Paare (G, X) mit der gegebenen Operation von G auf X. Begründen Sie jeweils kurz, dass die behauptete Operation tatsächlich eine Operation ist. Beschreiben Sie die Bahnen und alle Stabilisatoren G_x bis auf Konjugation und insbesondere die Fixpunkte X^G.

(b) $G = S_3$ und X ist der Simplex $\{(x, y, z) \in \mathbb{R}^3 \mid x, y, z \geqslant 0 \text{ und } x + y + z = 1\}$ mit der Operation durch Permutation der Koordinaten,

(c) $G = SL(n, \mathbb{R})$ und $X = \mathbb{R}^n$, durch Multiplikation von Matrix mit Vektor,

(d) $G = GL(n, \mathbb{R})$ und $X = \{A \subseteq \mathbb{R}^n \mid |A| = 2\}$, durch Multiplikation von Matrix mit Vektor für jedes Element in A,

*(e) $G = GL(n, \mathbb{R})$ und $X = \{A \subseteq \mathbb{R}^n \mid |A| = k\}$ für eine ganze Zahl $k \geqslant 3$, mit der Operation wie in (d) beschrieben,

(f) $G = S_n$ und $X = \mathcal{P}(\{1, \ldots, n\}) = \{A \subseteq \{1, \ldots, n\} \text{ Teilmenge}\}$, durch Permutation der Elemente in $\{1, \ldots, n\}$,

*(g) $G = S_n$ und $X = \{f \colon \{1, \ldots, n\} \to \{1, \ldots, n\} \text{ Funktion}\}$, mit der Operation definiert durch $g \cdot f(i) = f(g^{-1}(i))$ für $g \in G$, $f \in X$ und $1 \leqslant i \leqslant n$.

Aufgabe 3. (5 Punkte)

(a) Sei G eine endliche p-Gruppe. Konstruieren Sie eine endliche Normalreihe, deren Faktoren isomorph zu $\mathbb{Z}/p\mathbb{Z}$ sind. Damit folgt, dass G auflösbar ist.
Hinweis: finden Sie ein Element $g \in Z(G)$, das nicht trivial ist. Dann ist $\mathrm{ord}(g) = pm$ *für irgendeine m, also setzten Sie $G_1 = \langle g^m \rangle$.*

(b) Sei G eine Gruppe der Ordnung $|G| = p^2$ für p eine Primzahl. Zeigen Sie, dass G entweder zu $\mathbb{Z}/p^2\mathbb{Z}$ oder zu $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ isomorph ist.

(c) Geben Sie eine Normalreihe wie im Teil (a) für jede Gruppe der Ordnung 4 explizit an.

(d) Sei $B_n(\mathbb{Z})$ die Gruppe aller invertierbaren* oberen $(n \times n)$-Dreiecksmatrizen mit Einträgen in $\mathbb{Z}$. Berechnen Sie die Kommutatoruntergruppe $[B_n(\mathbb{Z}), B_n(\mathbb{Z})]$, und zudem auch die abgeleitete Reihe von $B_n(\mathbb{Z})$. Folgern Sie, dass $B_n(\mathbb{Z})$ auflösbar ist.
*Zur Verdeutlichung: das obige Wort "invertierbar" bedeutet, dass es eine inverse Matrix gibt, deren Einträge auch in $\mathbb{Z}$ sind.

Aufgabe 4. (3 Punkte)

Zeigen Sie:

(a) Sei R ein Ring und $I \triangleleft R$ ein Ideal. Dann ist R/I auf natürliche Weise wieder ein Ring.

(b) Formulieren und beweisen Sie ein Analogon des Homomorphiesatzes für Ringe.

NB: Wenn ein Teil einer Aufgabe mit dem Symbol $*$ versehen wird, zeigt dies, dass dieser Teil etwas anspruchsvoller sein sollte.

Einführung in die Algebra — Übungsblatt 4

Prof. Dr. Catharina Stroppel, Dr. Martin Palmer-Anghel (Assistent) // Wintersemester 17/18

[**Abgabe**: 9. November 2017, **vor** der Vorlesung, 10:00 – 10:15]

Aufgabe 1. (6 Punkte)

(a) Seien A und B zwei Gruppen und sei $\phi\colon A \to \mathrm{Aut}(B)$ ein Gruppenhomomorphismus. Zeigen Sie, dass die folgende Regel eine wohldefinierte Gruppenstruktur auf der Menge $B \times A$ ist:

$$(b_1, a_1) \cdot (b_2, a_2) \;=\; (b_1\phi(a_1)(b_2), a_1a_2).$$

Wir nennen die auf diese Weise definierte Gruppe $B \rtimes_\phi A$.

(b) Seien $s\colon H \to G$ und $q\colon G \to H$ zwei Gruppenhomomorphismen, so dass die Gleichung $q \circ s = \mathrm{id}_H$ gilt. Definieren Sie einen Gruppenhomomorphismus $\phi\colon H \to \mathrm{Aut}(\ker(q))$ durch $\phi(h)(g) = s(h).g.s(h)^{-1}$. Zeigen Sie, dass ϕ wohldefiniert ist und dass $G \cong \ker(q) \rtimes_\phi H$.

(c) Von Blatt 1, Aufgaben 4 und 5 folgern wir jetzt, dass

$$D_n \;\cong\; \mathbb{Z}/n\mathbb{Z} \rtimes_\psi \mathbb{Z}/2\mathbb{Z} \qquad \text{und} \qquad \mathrm{Okt} \;\cong\; S_4 \rtimes_\upsilon \mathbb{Z}/2\mathbb{Z}$$

für geeignete $\psi\colon \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ und $\upsilon\colon \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(S_4)$. Beschreiben Sie ψ und υ.

*(d) Zeigen Sie, dass es tatsächlich mehrere Homomorphismen υ gibt, so dass der obige Isomorphismus für Okt gilt. Deshalb kann man *nicht* aus $\phi_1 \neq \phi_2\colon A \to \mathrm{Aut}(B)$ folgern, dass $B \rtimes_{\phi_1} A$ und $B \rtimes_{\phi_2} A$ nicht isomorph sind. Wie viele Möglichkeiten gibt es für ψ?

Aufgabe 2. (4 Punkte)

(a) Beschreiben Sie explizit für zwei beliebige Ideale I, J in $R = \mathbb{Z}$ die Summe $I + J$, den Schnitt $I \cap J$ und das Produkt $I \cdot J$.

(b) Geben Sie ein Beispiel für ein Linksideal (bzw. Rechtsideal) in einem Ring an, das kein Ideal ist.

(c) Seien R und S zwei Ringe. Dann ist $R \times S$ auf natürliche Weise wieder ein Ring.

(d) Gelten für Ringe analoge Aussagen zu den Isomorphiesätzen für Gruppen? Begründen Sie ihre Antwort ausführlich.

Aufgabe 3. (5 Punkte)

Sei R ein Ring, nicht notwendig kommutativ. Ein Element $a \in R$ heißt *Links-Nullteiler* wenn es ein weiteres Element $0_R \neq b \in R$ gibt, so dass $a \cdot b = 0_R$. Es heißt *Rechts-Nullteiler* wenn es $0_R \neq b \in R$ gibt, so dass $b \cdot a = 0_R$. Es heißt *Einheit* wenn es $b \in R$ gibt, so dass $a \cdot b = b \cdot a = 1_R$.

(a) Zeigen Sie, dass $R^\star \subseteq R$ durch Multiplikation eine Gruppe ist.

*(b) Geben Sie ein Beispiel für einen Links-Nullteiler in einem Ring an, der kein Rechts-Nullteiler ist.

Für die folgende Ringe R, beschreiben Sie jeweils die Einheitengruppe $R^\star$ und alle Rechts- bzw. Links-Nullteiler.

(c) $R = \mathbb{Z}/n\mathbb{Z}$, (*Hinweis: Aufgabe 3 von Blatt 2 könnte nützlich sein.*)

(d) $R = K$ ein Körper,

(e) $R = M_n(\mathbb{R})$ der Ring aller $(n \times n)$-Matrizen mit Einträgen in $\mathbb{R}$,

(f) $R = \mathbb{R}[x]$ der Polynomring in einer Variable mit Koeffizienten in $\mathbb{R}$,

(g) $R = K \times L$ das Produkt (siehe Aufgabe 2(c)) von zwei Körpern K und L.

Aufgabe 4. (5 Punkte)

(a) Sei $\{p_1, p_2, p_3, \ldots\}$ die Menge aller Primzahlen und sei A die Menge aller Folgen $(n_1, n_2, n_3, \ldots)$ mit $n_i \in \mathbb{Z}/p_i\mathbb{Z}$. Definieren Sie eine Struktur eines Rings auf A.

(b) Sei $B < A$ die Untergruppe aller Reihen $(n_1, n_2, n_3, \ldots)$ so dass $n_i \neq 0$ für nur endlich viele Indizes i. Prüfen Sie zunächst, dass dies wirklich eine Untergruppe ist.

(c) Zeigen Sie, dass $\mathrm{ord}(b)$ endlich ist für jedes $b \in B$. Man nennt B dann *Torsionsgruppe*.

(d) Sei G eine beliebige Torsionsgruppe. Dann definieren wir $\exp(G) = \mathrm{kgV}\{\mathrm{ord}(g) \mid g \in G\}$ wenn dies endlich ist und ∞ sonst.
Sei R ein Ring so dass $(R, +)$ eine Torsionsgruppe ist. Zeigen Sie: $\exp(R, +) = \mathrm{ord}(1_R)$.

(e) Zeigen Sie, dass $\exp(B) = \infty$.

(f) Folgern Sie, dass es *keine* Ringstruktur auf B gibt, mit dieser abelschen Gruppe als additive Gruppe.

(g) Warum kann man nicht einfach die Ringstruktur von A auf B einschränken?

NB: Wenn ein Teil einer Aufgabe mit dem Symbol $*$ versehen wird, zeigt dies, dass dieser Teil etwas anspruchsvoller sein sollte.

Einführung in die Algebra — Übungsblatt 5

Prof. Dr. Catharina Stroppel, Dr. Martin Palmer-Anghel (Assistent) // Wintersemester 17/18

[**Abgabe**: 16. November 2017, **vor** der Vorlesung, 10:00 – 10:15]

Aufgabe 1. (5 Punkte)

Zeigen Sie:

(a) Sei R ein Integritätsbereich. Zeigen Sie, dass $R[t]$ auch ein Integritätsbereich ist.
(b) Sei im folgenden K ein Körper. Zeigen Sie, dass dann $K[t]$ ein Hauptidealring ist.
(c) Zeigen Sie, dass $K[t_1, \ldots, t_n]$ für $n \geqslant 2$ jedoch kein Hauptidealring ist.
(d) Zeigen Sie, dass der Polynomring $\mathbb{Z}[t]$ ebenfalls kein Hauptidealring ist.

Aufgabe 2. (5 Punkte)

Sei $\mathbb{Z}[\mathrm{i}] \subseteq \mathbb{C}$ die Menge der Gaußschen Zahlen: $\mathbb{Z}[\mathrm{i}] = \{x + y\mathrm{i} \mid x, y \in \mathbb{Z}\}$.

(a) Zeigen Sie, dass $\mathbb{Z}[\mathrm{i}]$ ein Unterring von $\mathbb{C}$ ist, und ferner, dass es ein Integritätsbereich ist.
(b) Die Betragsfunktion $|\ |: \mathbb{C} \to \mathbb{R}$ ist definiert durch $|x + y\mathrm{i}| = \sqrt{x^2 + y^2}$. Zeigen Sie: $|zw| = |z|\,|w|$ für $z, w \in \mathbb{C}$, und $|z| = 0$ dann und nur dann, wenn $z = 0$.
(c) Zeigen Sie ferner: für jede $z \in \mathbb{C}$ gibt es $b \in \mathbb{Z}[\mathrm{i}]$, so dass $|z - b| \leqslant \frac{1}{\sqrt{2}}$.
(d) Sei I ein Ideal in $\mathbb{Z}[\mathrm{i}]$, $I \neq \{0\}$. Zeigen Sie, dass die Teilmenge

$$\{|a| \mid a \in I, a \neq 0\} \subseteq \mathbb{R}$$

ein kleinstes Element r hat.
(e) Sei jetzt $a \in I$, $a \neq 0$. Zeigen Sie, dass es für jedes $g \in I$ mit $|g| = r$ ein Element $b \in \mathbb{Z}[\mathrm{i}]$ gibt, so dass $|a - bg| < r$.
(f) Folgern Sie, dass $a = bg$.
(g) Folgern Sie schließlich, dass $\mathbb{Z}[\mathrm{i}]$ ein Hauptidealring ist.

Aufgabe 3. (4 Punkte)

Für die folgenden Ringe R, beschreiben Sie alle maximalen Ideale:

(a) $R = K$ ein Körper,
(b) $R = \mathbb{Z}/n\mathbb{Z}$,
(c) $R = K[t]$ für einen algebraisch abgeschlossenen Körper K,
*(d) $R = \mathbb{R}[t]$.

Aufgabe 4. (6 Punkte)

Sei R ein kommutativer Ring und $S \subseteq R$ eine Teilmenge, so dass $1_R \in S$ und $a, b \in S \Rightarrow a \cdot b \in S$.

(a) Zeigen Sie, dass die Relation $\sim$ auf $R \times S$,

$$(a, b) \sim (a', b') \qquad \text{wenn} \qquad \exists s \in S \quad \text{mit} \quad s \cdot (a \cdot b' - a' \cdot b) = 0_R,$$

eine Äquivalenzrelation ist.

Wir bezeichnen mit $S^{-1}R$ die Menge der Äquivalenzklassen für diese Äquivalenzrelation, und schreiben $[a, b]$ für die Äquivalenzklasse von (a, b).

(b) Zeigen Sie, dass $S^{-1}R$ zu einem kommutativen Ring $(S^{-1}R, +, \cdot)$ wird, mit den Operationen $[a, b]+[c, d] = [ad+bc, bd]$ und $[a, b]\cdot[c, d] = [ac, bd]$. (Zeigen Sie zuerst, dass diese Operationen überhaupt wohldefiniert sind.)

(c) Wenn R ein Integritätsbereich ist können wir $S = R \setminus \{0_R\}$ nehmen (warum?). In diesem Fall schreiben wir $\mathrm{Quot}(R) \coloneqq S^{-1}R$. Zeigen Sie, dass $\mathrm{Quot}(R)$ ein Körper ist.

(d) Zeigen Sie, dass die Ringe $\mathrm{Quot}(\mathbb{Z})$ und $\mathbb{Q}$ isomorph (als Ringe) sind.

*(e) Sei $S = \{p^k \mid k \geqslant 0\}$, für eine Primzahl p. Zeigen Sie, dass die Teilmenge

$$\{r \in \mathbb{Q} \mid r = ap^{-k} \text{ für } a, k \in \mathbb{Z} \text{ mit } k \geqslant 0\} \subseteq \mathbb{Q}$$

ein Unterring ist, und dass er isomorph als Ring zu $S^{-1}\mathbb{Z}$ ist.

⟨ Die Fachschaft Mathematik feiert am 23.11. ihre Matheparty in der N8schicht. Der VVK findet am Mo. 20.11., Di. 21.11. und Mi. 22.11. in der Mensa Poppelsdorf statt. Alle weitere Infos auch auf fsmath.uni-bonn.de. ⟩

NB: Wenn ein Teil einer Aufgabe mit dem Symbol $*$ versehen wird, zeigt dies, dass dieser Teil etwas anspruchsvoller sein sollte.

Einführung in die Algebra — Übungsblatt 6

Prof. Dr. Catharina Stroppel, Dr. Martin Palmer-Anghel (Assistent) // Wintersemester 17/18

[**Abgabe**: 23. November 2017, **vor** der Vorlesung, 10:00 – 10:15]

Aufgabe 1. (3 Punkte)

Geben Sie einen Beweis für das Lemma 7.16 der Vorlesung:
Lemma 7.16. Seien S ein kommutativer Ring, $R \subseteq S$ ein Unterring und $a_1, \dots, a_n \in S$. Dann:

(1) $a_1, \dots, a_n$ sind algebraisch abhängig genau dann, wenn es $p(t_1, \dots, t_n) \in R[t_1, \dots, t_n] \smallsetminus \{0\}$ gibt, so dass $p(a_1, \dots, a_n) = 0$.
(2) Diese Aussage ist äquivalent zur folgenden:
$a_1, \dots, a_n$ sind algebraisch *un*abhängig $\Leftrightarrow$ Ist für ein Polynom $p(t_1, \dots, t_n) \in R[t_1, \dots, t_n]$ das Element $p(a_1, \dots, a_n) \in S$ null, dann muss $p(t_1, \dots, t_n) = 0$ sein.

Aufgabe 2. (6 Punkte)

Sei $R = \mathbb{Z}[\mathrm{i}\sqrt{5}] = \{a + b\mathrm{i}\sqrt{5} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$.

(a) Zeigen Sie, dass R der von $\mathrm{i}\sqrt{5}$ erzeugte Unterring über $\mathbb{Z}$ in $\mathbb{C}$ ist.
(b) Mithilfe der Betragsfunktion $|\ |\colon \mathbb{C} \to \mathbb{R}$ (*cf.* Blatt 5 Aufgabe 2) zeigen Sie, dass $R^\times = \{\pm 1\}$.
(c) Zeigen Sie, dass die Elemente $2, 3, 1 + \mathrm{i}\sqrt{5}, 1 - \mathrm{i}\sqrt{5} \in R$ irreduzibel sind.
(d) Folgern Sie, dass R kein faktorieller Ring ist.
(e) Deshalb ist R auch kein Hauptidealring. Geben Sie mit Begründung ein Ideal in R an, das kein Hauptideal ist.
Hinweis: benutzen Sie dafür wieder die Betragsfunktion.

Aufgabe 3. (6 Punkte)

(a) Seien $n_1, n_2, \dots, n_k \in \mathbb{N}$ paarweise teilerfremd — das heißt, es gibt keine Primzahl p mit $p \mid n_i$ und $p \mid n_j$ für zwei verschiedene i, j — und sei $N = n_1 n_2 \cdots n_k$. Zeigen Sie, dass

$$\mathbb{Z}/N\mathbb{Z} \ \cong\ \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z} \tag{1}$$

als Ringe.
(b) Zeigen Sie, dass (1) *nicht* wahr ist, sogar nicht einmal als Gruppen, wenn $n_1, n_2, \dots, n_k \in \mathbb{N}$ *nicht* paarweise teilerfremd sind.
Hinweis: was ist die größte Ordnung eines Elements der rechten Seite?
(c) Finden Sie alle $x \in \mathbb{Z}$, so dass $x \equiv 4 \pmod 7$ und $x \equiv 7 \pmod{12}$.
Hinweis: finden Sie zuerst eine Lösung, dann benutzen Sie den Isomorphismus (1), um alle anderen zu finden. Um die erste Lösung zu finden, könnten Sie z.B. zuerst ganze Zahlen a, b finden, so dass $7a + 12b = 1$.
(d) Finden Sie alle $x \in \mathbb{Z}$, so dass $x \equiv 4 \pmod 6$, $x \equiv 33 \pmod{35}$ und $x \equiv 10 \pmod{11}$.
(e) Finden Sie alle $x \in \mathbb{Z}$, so dass $x \equiv p - 2 \pmod p$ für alle Primzahlen $p < 100$.

Aufgabe 4. (5 Punkte)

Sei $(X, \leqslant)$ eine partiell geordnete Menge. Man sagt, dass eine aufsteigende Kette $x_0 \leqslant x_1 \leqslant \cdots$ in X *stationär* wird, wenn ein $n_0 \in \mathbb{N}$ existiert mit $x_m = x_{n_0}$ für alle $m \geqslant n_0$.

Sei jetzt R ein Integritätsbereich und $\mathrm{HI}(R)$ die partiell geordnete Menge aller Hauptideale von R.

Zeigen Sie:

(a) Wenn R ein faktorieller Ring ist, dann gilt:
  (i) Jedes irreduzible Element von R ist prim.
  (ii) Jede aufsteigende Kette in $\mathrm{HI}(R)$ wird stationär.

(b) Wenn (i) und (ii) für R gelten, dann ist R ein faktorieller Ring.

Zur Information. Nach der Vorlesung gilt

$$\{\text{euklidische Ringe}\} \subseteq \{\text{Hauptidealringe}\} \subseteq \{\text{faktorielle Ringe}\}.$$

Allerdings sind die beiden Inklusionen jeweils echt. Für die zweite Inklusion werden wir in der Vorlesung sehen, dass $\mathbb{Z}[t]$ und $\mathbb{C}[t_1, t_2]$ faktorielle Ringe sind, aber nach Aufgabe 1 von Übungsblatt 5 wissen wir, dass sie keine Hauptidealringe sind. Für die erste Inklusion gilt das Folgende.

Sei $d \in \mathbb{Z}$ eine quadratfreie ganze Zahl und definiere $\mathcal{O}_d = \mathbb{Z}[\sqrt{d}]$ wenn $d \equiv 2$ oder $3 \pmod 4$ und $\mathcal{O}_d = \mathbb{Z}\big[\frac{1}{2}(1 + \sqrt{d})\big]$ wenn $d \equiv 1 \pmod 4$, wobei für $z \in \mathbb{C}$ bedeutet $\mathbb{Z}[z]$ den von z erzeugten Unterring über $\mathbb{Z}$ in $\mathbb{C}$, anders gesagt: $\mathbb{Z}[z] = \{a + bz \mid a, b \in \mathbb{Z}\}$. Wenn d positiv ist, bezeichnet $\sqrt{d}$ die positive Wurzel, wie üblich, und wenn d negativ ist, definieren wir $\sqrt{d} = \mathrm{i}\sqrt{-d}$. Zum Beispiel ist $\mathcal{O}_{-1} = \mathbb{Z}[\mathrm{i}]$ der Ring der Gaußschen Zahlen. Wir haben in Aufgabe 2 oben gesehen, dass $\mathcal{O}_{-5}$ kein faktorieller Ring ist. Andererseits haben wir in Aufgabe 2 auf Übungsblatt 5 gezeigt, dass $\mathcal{O}_{-1}$ ein Hauptidealring, und deshalb insbesondere ein faktorieller Ring, ist. Es gibt tatsächlich nur endlich viele negative d, so dass $\mathcal{O}_d$ ein faktorieller Ring ist, nämlich:

$$d \in \{-163, -67, -43, -19, -11, -7, -3, -2, -1\}.$$

Für positive d kennt man die entsprechende Liste noch nicht, und nicht einmal ob die Liste endlich ist. Für alle Ringe der Form $\mathcal{O}_d$ gilt die Äquivalenz: Hauptidealring $\Leftrightarrow$ faktorieller Ring (was im allgemeinen bestimmt nicht gilt, wie oben schon bemerkt), also die Frage, wann $\mathcal{O}_d$ ein Hauptidealring ist, hat dieselbe (unvollständige) Lösung. Es gibt aber eine komplette Lösung zur Frage, wann $\mathcal{O}_d$ ein *euklidischer* Ring ist. Dies gilt nämlich genau dann, wenn:

$$d \in \{-11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}.$$

Also insbesondere ist $\mathcal{O}_{-19} = \mathbb{Z}\big[\frac{1}{2}(1 + \mathrm{i}\sqrt{19})\big]$ ein Hauptidealring, der kein euklidischer Ring ist. Dazu vergleiche man die Abschnitte 14.7–9 und die zugehörigen "Notes" in:
G. H. Hardy, E. M. Wright, *An Introduction to the Theory of Numbers*, fifth ed., 1979 (OUP).

NB: Wenn ein Teil einer Aufgabe mit dem Symbol $*$ versehen wird, zeigt dies, dass dieser Teil etwas anspruchsvoller sein sollte.

Einführung in die Algebra — Übungsblatt 7

Prof. Dr. Catharina Stroppel, Dr. Martin Palmer-Anghel (Assistent) // Wintersemester 17/18

[**Abgabe**: 30. November 2017, **vor** der Vorlesung, 10:00 – 10:15]

Aufgabe 1. (6 Punkte = 1 + 1 + 1 + 1 + 2)

Entscheiden Sie, ob die folgenden Polynome, jeweils über den gegebenen Ringen, irreduzibel sind oder nicht.

(a) $t^4 + 6t^3 - 12$ in $\mathbb{Z}[t]$,
(b) $t^7 + 3t^4 + 6t^2 - 12$ in $\mathbb{Q}[t]$,
(c) $t^7 + 3t^4 + 6t^2 - 12$ in $\mathbb{R}[t]$,
(d) $t^4 + 4$ in $\mathbb{Z}[t]$.

(e) Erinnern Sie sich, dass $A = \mathbb{Z}[\sqrt{-5}]$ ein Unterring von $\mathbb{C}$ ist, und ist deshalb ein Integritätsbereich (weil $\mathbb{C}$ ein ist). Deshalb existiert der Quotientenkörper $\mathrm{Quot}(A)$. Zeigen Sie, dass das Polynom $3t^2 + 4t + 3$ in $A[t]$ irreduzibel ist (dafür müssen Sie zeigen, dass es keine Lösung in A für die Gleichung $3t^2 + 4t + 3 = 0$ geben kann), aber in $\mathrm{Quot}(A)[t]$ reduzibel ist. Warum ist diese Aussage kein Widerspruch zum Satz von Gauß?

Aufgabe 2. (4 Punkte = 1 + 3)

Seien A ein Ring und S eine multiplikativ abgeschlossene Teilmenge von A. Zeigen Sie:

(a) Wenn A ein Integritätsbereich ist, dann ist $S^{-1}A$ auch ein Integritätsbereich.
(b) Wenn A ein Hauptidealring ist und $0 \notin S$, dann ist $S^{-1}A$ auch ein Hauptidealring.

Aufgabe 3. (10 Punkte = 1 + 2 + 1 + 2 + 2 + 2)

Für eine positive ganze Zahl n, sei $W_n \subseteq \mathbb{C}$ die Menge aller complexen Zahlen z, so dass $z^n = 1$.

(a) Beschreiben Sie explizit alle Elemente von W_2, W_3 und W_4 als $a + ib$ mit $a, b \in \mathbb{R}$. (Dabei sollte die Beschreibung wirklich explizit sein und keine allgemeine Formel.)
(b) Zeigen Sie, dass W_n durch Multiplikation eine Gruppe isomorph zu $\mathbb{Z}/n\mathbb{Z}$ ist, und dass die Vereinigung $\bigcup_{n\in\mathbb{N}} W_n$ durch Multiplikation eine Gruppe isomorph zu $\mathbb{Q}/\mathbb{Z}$ ist.
(c) Berechnen Sie die Kreisteilungspolynomen $\Phi_1(t), \Phi_2(t), \ldots, \Phi_8(t)$.
(d) Sei $n \in \mathbb{N}$ und p eine Primzahl, so dass $p \mid n$. Zeigen Sie, dass $\Phi_{np}(t) = \Phi_n(t^p)$. Berechnen Sie damit $\Phi_{p^k}(t)$ für jede Primzahl p und $k \in \mathbb{N}$.
(e) Seien $f, g \in \mathbb{Z}[t]$ zwei Polynome, wobei f normiert ist. Zeigen Sie, dass es $q, r \in \mathbb{Z}[t]$ gibt, mit $g = qf + r$ und entweder $r = 0$ oder $\mathrm{Grad}(r) < \mathrm{Grad}(f)$.
(f) Zeigen Sie, dass $\Phi_d(t) \in \mathbb{Z}[t]$ und normiert ist für alle $d \in \mathbb{N}$.
Verwenden Sie Induktion nach d. Schreiben Sie $t^d - 1 = f\Phi_d(t)$, mit $f \in \mathbb{Z}[t]$ und normiert nach Induktionsvoraussetzung, und teilen Sie dann $t^d - 1$ durch f unter Verwendung vom Teil (e).

Einführung in die Algebra — Übungsblatt 8

Prof. Dr. Catharina Stroppel, Dr. Martin Palmer-Anghel (Assistent) // Wintersemester 17/18

[**Abgabe**: 7. Dezember 2017, **vor** der Vorlesung, 10:00 – 10:15]

Aufgabe 1. (5 Punkte = $2 + 3 \cdot 1$)

Für ein Integritätsbereich K sei $K(t) = \mathrm{Quot}(K[t])$.

(a) Mithilfe der universellen Eigenschaft der Lokalisierung, konstruieren Sie eine injektive Abbildung $\mathbb{R}(t) \to \mathbb{C}(t)$. Zeigen Sie, dass ihr Bild $K \subset \mathbb{C}(t)$ der kleinste Unterkörper von $\mathbb{C}(t)$ ist, der $\mathbb{R} \subset \mathbb{C}(t)$ und $t \in \mathbb{C}(t)$ enthält.

Zeigen Sie, dass die folgende Polynome über den gegebenen Ringen irreduzibel sind. Benutzen Sie dafür entweder das Kriterium von Eisenstein oder das Reduktionskriterium (siehe unten) für ein Primideal $(p) \subset \mathbb{Z}$.

(b) $t^3 + at^2 + (7-a)t + 1$ in $\mathbb{Z}[t]$, wobei $a \in \mathbb{Z}$,
(c) $t^3 + 3bt^2 + 8t + 1$ in $\mathbb{Z}[t]$, wobei $b \in \mathbb{Z}$,
(d) $t^5 + 4t^3 - t + \mathrm{i}t + 3 + 3\mathrm{i}$ in $\mathbb{Z}[\mathrm{i}][t]$.

Aufgabe 2. (5 Punkte = $2 + 1 + 2$)

(a) Seien $L /\!\!/ K$ und $M /\!\!/ L$ zwei Körpererweiterungen, so dass $[M /\!\!/ K] = [L /\!\!/ K] < \infty$. Zeigen Sie, dass $M \cong L$.
(b) Sei $L /\!\!/ K$ eine Körpererweiterung mit $[L /\!\!/ K] = p$ eine Primzahl und sei $a \in L \smallsetminus K$. Zeigen Sie, dass $K(a) = L$.
(c) Seien K ein Körper und A ein Integritätsbereich mit $K \subset A$, so dass jedes Element $a \in A$ algebraisch abhängig über K ist. Zeigen Sie, dass A ein Körper ist.

Aufgabe 3. (7 Punkte = $5 \cdot 1 + 2$)

Sei $L /\!\!/ K$ eine Körpererweiterung. Bestimmen Sie in den folgenden Beispielen das Minimalpolynom des Elements $a \in L$ über K.

(a) $a = \mathrm{i} \in L = \mathbb{C}$ und $K = \mathbb{Q}$,
(b) $a = \frac{1}{2}(1 + \sqrt{5}) \in L = \mathbb{R}$ und $K = \mathbb{Q}$,
(c) $a = e^{\pi \mathrm{i}/3} \in L = \mathbb{C}$ und $K = \mathbb{Q}$,
(d) $a = e^{2\pi \mathrm{i}/p^2} \in L = \mathbb{C}$ und $K = \mathbb{Q}$, wobei p eine Primzahl ist,
(e) $a = \sqrt{11} \in L = \mathbb{C}$ und $K = \mathbb{R}$.
(f) Bestimmen Sie alle Zwischenkörper $\mathbb{Q} \subset K \subset \mathbb{Q}(\sqrt[5]{17})$.

Hinweis: für die Teile (c) *und* (d) *wäre Aufgabe 3 von Übungsblatt 7 nützlich.*

Aufgabe 4. (3 Punkte = $2 + 1$)

Seien K ein Körper und $P \subset K$ der Primkörper von K. Sei ϕ ein Automorphismus von K, das heißt, eine Bijektion $\phi\colon K \to K$ mit $\phi(0) = 0$, $\phi(1) = 1$, $\phi(a+b) = \phi(a) + \phi(b)$ und $\phi(ab) = \phi(a)\phi(b)$ für je zwei Elemente $a, b \in K$. Zeigen Sie:

(a) Für jedes Element $a \in P$ ist $\phi(a) = a$. (Betrachten Sie zuerst das Beispiel $P = \mathbb{Q} \subset \mathbb{C} = K$.)
(b) Deshalb ist ϕ ein P-Automorphismus, d.h. ein Automorphismus des P-Vektorraums K.

Das Reduktionskriterium für ein Primideal $(p) \subset \mathbb{Z}$**.** Sei p eine Primzahl. Dann ist (p) ein Primideal im faktoriellen Ring $\mathbb{Z}$. Wir schreiben $\mathrm{can}\colon \mathbb{Z} \to \mathbb{Z}/(p)$ für den kanonischen Ringhomomorphismus. Sei $f = a_0 + a_1 t + \cdots + a_n t^n \in \mathbb{Z}[t]$ ein Polynom mit $\mathrm{can}(a_n) \neq 0$, d.h. $p \nmid a_n$. Wenn $\mathrm{can}(a_0) + \mathrm{can}(a_1)t + \cdots + \mathrm{can}(a_n)t^n \in \mathbb{Z}/(p)[t]$ irreduzibel ist, dann ist f über $\mathbb{Q}$ irreduzibel. (Und wenn f außerdem primitiv ist, ist f auch über $\mathbb{Z}$ irreduzibel.)

Einführung in die Algebra — Übungsblatt 9

Prof. Dr. Catharina Stroppel, Dr. Martin Palmer-Anghel (Assistent) // Wintersemester 17/18

[**Abgabe**: 14. Dezember 2017, **vor** der Vorlesung, 10:00 – 10:15]

Aufgabe 1. (5 Punkte = $5 \cdot 1$)

Wahr oder falsch? Begründen Sie Ihre Antwort. Sei $M /\!\!/ L$ und $L /\!\!/ K$ Körpererweiterungen.

(a) Wenn $M /\!\!/ K$ algebraisch ist, dann sind auch $M /\!\!/ L$ und $L /\!\!/ K$ algebraisch.
(b) Wenn $M /\!\!/ L$ und $L /\!\!/ K$ beide endlich sind, dann ist auch $M /\!\!/ K$ endlich.
(c) Sei $L /\!\!/ \mathbb{R}$ eine algebraische Körpererweiterung mit L algebraisch abgeschlossen. Dann gilt $[\![L : \mathbb{R}]\!] = 2$.
(d) Es gibt keine Zwischenkörper $\mathbb{Q} \subset K \subset \mathbb{Q}(e^{2\pi \mathrm{i}/5})$ außer $\mathbb{Q}$ und $\mathbb{Q}(e^{2\pi \mathrm{i}/5})$.
Hinweis: die reelle Zahl $e^{2\pi \mathrm{i}/5} + e^{-2\pi \mathrm{i}/5}$ ist eine Wurzel des Polynoms $t^2 + t - 1$.
(e) Es gibt keine Zwischenkörper $\mathbb{Q} \subset K \subset \mathbb{Q}(\sqrt[p]{q})$ außer $\mathbb{Q}$ und $\mathbb{Q}(\sqrt[p]{q})$, wobei p, q Primzahlen sind.

Aufgabe 2. (6 Punkte = $2 + 2 + 1 + 1$)

Für eine Menge I betrachten wir die Menge $\mathbb{N}^{(I)}$ aller Familien $(a_i)_{i \in I}$ mit $a_i \in \mathbb{N}$ für alle $i \in I$ und mit $a_i = 0$ für alle $i \in I$ außer einer endlichen Teilmenge. Es gibt auf $\mathbb{N}^{(I)}$ eine Addition, die komponentenweise definiert ist, mit neutralem Element die Familie $0 = (a_i)_{i \in I}$ mit $a_i = 0$ für alle $i \in I$. Für einen kommutativen Ring R definieren wir jetzt $R[(t_i)_{i \in I}]$ gleich der Menge aller Abbildungen $f \colon \mathbb{N}^{(I)} \to R$ mit $f(a) = 0_R$ für alle $a \in \mathbb{N}^{(I)}$ außer einer endlichen Teilmenge. Die Addition ist komponentenweise definiert, $(f+g)(a) = f(a)+g(a)$, und die Multiplikation ist durch $(f \cdot g)(a) = \sum f(b)g(c)$ definiert, wobei wir über alle Paare $(b, c) \in \mathbb{N}^{(I)} \times \mathbb{N}^{(I)}$ mit $a = b + c$ summieren.

Für $j \in I$ definieren wir das Element $t_j \in R[(t_i)_{i \in I}]$ als f, wobei $f(a) = 1_R$ wenn $a = (a_i)_{i \in I}$ mit $a_j = 1$ und $a_i = 0$ für $i \neq j$ und $f(a) = 0_R$ sonst. Es gibt einen injektiven Ringhomomorphismus $R \to R[(t_i)_{i \in I}]$, definiert durch $r \mapsto f_r$, wobei $f_r(a) = 0_R$ für alle $a \in \mathbb{N}^{(I)}$ mit $a \neq 0$ und $f_r(0) = r$. Deshalb können wir R als Unterring von $R[(t_i)_{i \in I}]$ betrachten.

(a) Prüfen Sie nach, dass dies ein kommutativer Ring bildet.
(b) Zeigen Sie die universelle Eigenschaft: Sei S ein kommutativer Ring, $\phi \colon R \to S$ ein Ringhomomorphismus und $s = (s_i)_{i \in I}$ eine Familie mit $s_i \in S$ für alle $i \in I$. Dann gibt es genau einen Ringhomomorphismus $\mathrm{ev} \colon R[(t_i)_{i \in I}] \to S$ mit $\mathrm{ev}|_R = \phi$ und $\mathrm{ev}(t_j) = s_j$ für jedes $j \in I$.
(c) Sei I endlich mit $|I| = n$. Zeigen Sie, dass $R[(t_i)_{i \in I}]$ als Ring zu $R[t_1, \ldots, t_n]$ isomorph ist.
(d) Sei jetzt $L /\!\!/ K$ eine Körpererweiterung, J eine Menge, $f_1, \ldots, f_n \in J$ paarweise verschiedene Elemente und $a_1, \ldots, a_n \in L$ Elemente. Dann gibt es genau einen Ringhomomorphismus $\mathrm{ev} \colon K[(X_f)_{f \in J}] \to L[(X_f)_{f \in J}]$ mit $\mathrm{ev}(\lambda) = \lambda$ für $\lambda \in K$, $\mathrm{ev}(X_{f_i}) = a_i$ für $i \in \{1, \ldots, n\}$ und $\mathrm{ev}(X_f) = X_f$ für $f \in J \smallsetminus \{f_1, \ldots, f_n\}$.

Aufgabe 3. (9 Punkte = $2 + 2 + 2 + 3$)

Sei $M /\!\!/ K$ eine Körpererweiterung und L_1, L_2 zwei Zwischenkörper, d.h. $M /\!\!/ L_i$ und $L_i /\!\!/ K$ für $i = 1, 2$. Das Kompositum $L_1 \cdot L_2$ ist der kleinste Unterkörper von M, der die Teilmenge $L_1 \cup L_2$ enthält. Zeigen Sie:

(a) $L_1 \cdot L_2 = L_1(L_2) = L_2(L_1)$.
(b) Wenn $L_1 /\!\!/ K$ und $L_2 /\!\!/ K$ beide algebraisch sind, dann ist auch $L_1 \cdot L_2 /\!\!/ K$ algebraisch.
(c) Wenn $L_1 /\!\!/ K$ und $L_2 /\!\!/ K$ beide endlich sind, dann ist

$$[\![L_1 \cdot L_2 : K]\!] \leqslant [\![L_1 : K]\!] \cdot [\![L_2 : K]\!].$$

Wenn $[\![L_1 : K]\!]$ und $[\![L_2 : K]\!]$ teilerfremd sind, dann gilt oben die Gleichheit.
(d) Benutzen Sie dies, um zu zeigen, dass $[\![\mathbb{Q}(a, b) : \mathbb{Q}]\!] = n$, wobei:
(i) $a = e^{2\pi \mathrm{i}/5}$, $b = \sqrt[3]{2}$ und $n = 12$,
(ii) $a = e^{\pi \mathrm{i}/3}$, $b = \sqrt[4]{2}$ und $n = 8$.

Einführung in die Algebra — Übungsblatt 10

Prof. Dr. Catharina Stroppel, Dr. Martin Palmer-Anghel (Assistent) // Wintersemester 17/18

[**Abgabe**: 21. Dezember 2017, **vor** der Vorlesung, 10:00 – 10:15]

Aufgabe 1. (6 Punkte = $6 \cdot 1$)

Wahr oder falsch? Begründen Sie Ihre Antwort.

(a) Seien K_1 und K_2 Körper. Dann ist $K_1 \times K_2$ mit der komponentenweise Addition und Multiplikation wieder ein Körper.
(b) Ein Ringhomomorphismus $f\colon R \to K$ ist immer surjektiv wenn K ein Körper ist.
(c) Seien $L/\!\!/K$ und $K/\!\!/\mathbb{Q}$ endliche Körpererweiterungen, wobei L algebraisch abgeschlossen ist, und $\phi\colon K \to K$ ein Ringisomorphismus. Dann gibt es einen Ringisomorphismus $\psi\colon L \to L$ mit $\psi|_K = \phi$.
(d) Wenn $K/\!\!/\mathbb{Q}$ eine endliche Körpererweiterung ist, ist jeder Ringhomomorphismus $K \to K$ ein Isomorphismus.
(e) Es existiert ein Körper K mit $K \subseteq K_1 \subsetneq K_2$, so dass K_1 und K_2 algebraische Abschlüsse von K sind.
(f) Es gibt eine einzige abelsche Gruppe der Ordnung 462 und genau zwei der Ordnung 780.

Aufgabe 2. (6 Punkte = $2 + 3 + 1$)

Sei $L/\!\!/K$ und $L'/\!\!/K'$ algebraische Körpererweiterungen, $a \in L$ und $f\colon K \to K'$ ein Ringhomomorphismus. Wir schreiben $f_*\colon K[t] \to K'[t]$ für den induzierten Ringhomomorphismus der Polynomringe (durch Anwenden von f auf die Koeffizienten wie in der Vorlesung) und $p(t) = m_a(t) \in K[t]$ für das Minimalpolynom des Elements a über K.

(a) Gegeben $a' \in L'$ mit $f_*(p(t))(a') = 0$, konstruieren Sie einen Ringhomomorphismus $\varphi\colon K(a) \to L'$ mit $\varphi(a) = a'$ und $\varphi|_K = f$.
(b) Zeigen Sie, dass $\varphi \mapsto \varphi(a)$ eine Bijektion bildet zwischen der Menge aller Ringhomomorphismen $\varphi\colon K(a) \to L'$ mit $\varphi|_K = f$ und der Menge aller Nullstellen von $f_*(p(t))$ in L'.
(c) Zeigen Sie: Jeder Ringhomomorphismus $\varphi\colon K(a) \to L'$ mit $\varphi|_K = f$ induziert einen Isomorphismus von Körpern zwischen $K(a)$ und $f(K)(\varphi(a))$.

Aufgabe 3. (8 Punkte = $2 + 2 + 1 + 2 + 1$)

Sei ϕ ein Automorphismus des Körpers $\mathbb{R}$. Wir wissen von der Aufgabe 4(a) auf Übungsblatt 8, dass die Einschränkung von ϕ auf $\mathbb{Q}$ die Identität ist, also $\phi \in \mathrm{Aut}(\mathbb{R}/\!\!/\mathbb{Q})$.

(a) Zeigen Sie: Wenn $x < y$ für $x, y \in \mathbb{R}$, dann ist $\phi(x) < \phi(y)$.
Hinweis: eine reelle Zahl x ist genau dann positiv, wenn es $y \in \mathbb{R}$ gibt, mit $y \neq 0$ und $x = y^2$.
(b) Folgern Sie, dass ϕ die Identität sein muss.

Sei jetzt $a = \sqrt[n]{p} \in \mathbb{R}$, wobei n eine positive ganze Zahl und p eine Primzahl ist, und sei ϕ ein Automorphismus des Körpers $\mathbb{Q}(a) \subseteq \mathbb{R}$, also $\phi \in \mathrm{Aut}(\mathbb{Q}(a)/\!\!/\mathbb{Q})$.

(c) Zeigen Sie, dass $\phi(a)^n = p$.
(d) Folgern Sie, dass der Körper $\mathbb{Q}(a)$ genau einen Automorphismus bzw. zwei Automorphismen besitzt, das heißt, $\mathrm{Aut}(\mathbb{Q}(a)/\!\!/\mathbb{Q})$ zur trivialen Gruppe bzw. zu $\mathbb{Z}/2\mathbb{Z}$ isomorph ist, wenn n ungerade bzw. gerade ist.
(e) Zeigen Sie, dass $\mathrm{Aut}(\mathbb{Q}(\mathrm{i})/\!\!/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ (Isomorphismus von Gruppen) und beschreiben Sie explizit das nicht-triviale Element.

Einführung in die Algebra — Übungsblatt 11

Prof. Dr. Catharina Stroppel, Dr. Martin Palmer-Anghel (Assistent) // Wintersemester 17/18

[**Abgabe**: 11. Januar 2018, **vor** der Vorlesung, 10:00 – 10:15]

Sie können sich aus den sieben Aufgaben vier aussuchen (Aufgabe 5 ist aber eine Voraussetzung für Aufgabe 6) und diese bearbeiten. Sie bekommen dann eine Punktzahl von zwanzig, wie üblich. Wenn Sie mehr als vier Aufgaben bearbeiten, und Sie a_i Punkte für Aufgabe i bekommen haben, ist Ihre Punktzahl $\max\{a_{\sigma(1)} + a_{\sigma(2)} + a_{\sigma(3)} + a_{\sigma(4)} \mid \sigma \in \mathfrak{S}_7\}$.

Aufgabe 1. (5 Punkte $= 5 \cdot 1$)

Wahr oder falsch? Begründen Sie Ihre Antwort.

(a) Seien $\mathbb{Q}(\sqrt[4]{2}) = L /\!\!/ K = \mathbb{Q}(\sqrt{2})$ und $f\colon K \to K$ ein Ringisomorphismus. Dann gibt es einen Ringisomorphismus $\hat{f}\colon L \to L$, so dass $\hat{f}|_K = f$.
(b) Das Polynom $t^4 - 4t^3 + 8t^2 - 8t + 4 \in \mathbb{R}[t]$ ist irreduzibel.
(c) Für eine endliche Teilmenge S eines Körpers K gibt es ein Polynom $f(t) \in K[t]$ mit keinen Nullstellen in S.
(d) Der algebraische Abschluss $\bar{\mathbb{F}}_n$ von $\mathbb{F}_n$, wobei $n = p^r$ für eine Primzahl p, ist unendlich.
(e) Ein endlicher Integritätsbereich ist ein Körper.

Aufgabe 2. (5 Punkte $= 2 + 2 + 1$)

Seien $K /\!\!/ \mathbb{Q}$ eine algebraische Körpererweiterung und $f\colon K \to K$ ein Ringhomomorphismus.

(a) Seien $a \in K$ und $S_a \subseteq K$ die Menge aller Nullstellen in K des Minimalpolynoms $m_a(t) \in \mathbb{Q}[t]$. Zeigen Sie, dass $f(S_a) \subseteq S_a$.
(b) Folgern Sie, dass wir tatsächlich $f(S_a) = S_a$ haben.
(c) Folgern Sie schließlich, dass f ein Ringisomorphismus ist.

Aufgabe 3. (5 Punkte $= 1 + 1 + 1 + 2$)

Seien R ein kommutativer Ring, und $f(t) = a_n t^n + \cdots + a_1 t + a_0 \in R[t]$ ein Polynom. Die formale Ableitung von $f(t)$ ist $f'(t) = n \cdot a_n t^{n-1} + (n-1) \cdot a_{n-1} t^{n-2} + \cdots + 2 \cdot a_2 t + a_1$.

Seien jetzt $r, s \in R$ und $f(t), g(t) \in R[t]$. Zeigen Sie:

(a) $(r \cdot f + s \cdot g)'(t) = r \cdot f'(t) + s \cdot g'(t)$,
(b) $(f \cdot g)'(t) = f'(t) \cdot g(t) + f(t) \cdot g'(t)$.
(c) Sei $f(t) = t^9 + a_8 t^8 + \cdots + a_0 \in \mathbb{F}_9[t]$ ein irreduzibles Polynom und sei K ein Zerfällungskörper von $f(t)$ über $\mathbb{F}_9$. Zeigen Sie, dass (mindestens) eine von den folgenden Aussagen wahr ist: (1) $f(t)$ hat genau 9 Nullstellen in K; (2) $f'(t)$ hat genau 9 Nullstellen in $\mathbb{F}_9$.
(d) Finden Sie doppelte Nullstellen für die folgenden Polynomen in $\mathbb{F}_9[t]$.
  (i) $t^6 + t^5 - t^4 - t^3 - t^2 + t$
  (ii) $t^{12} + t^6 + t^4 + 2t^3 + t$

Aufgabe 4. (5 Punkte $= 2 + 2 + 1$)

Seien K ein endlicher Körper und $a, b \in K^* = K \smallsetminus \{0\}$.

(a) Wie viele Elemente $z \in K^*$ gibt es, so dass $z = ax^2$ für $x \in K$?
(b) Zeigen Sie, dass es $x, y \in K$ mit $1 + ax^2 + by^2 = 0$ gibt.
(c) Wenn $|K|$ gerade ist, gilt sogar, dass es $x \in K$ mit $1 + ax^2 = 0$ gibt.

Aufgabe 5. (5 Punkte = 3 + 2)

(a) Seien G eine abelsche Gruppe der Ordnung p^n und $g \in G$ ein Element der maximalen Ordnung, d.h. für jedes Element $h \in G$ gilt $|h| \leqslant |g|$. Vorausgesetzt, dass G nicht gleich $\langle g \rangle$ ist, finden Sie eine Untergruppe $H < G$ der Ordnung p mit $H \cap \langle g \rangle = \{0\}$.

(b) Sei G eine abelsche Gruppe der Ordnung p^n. Zeigen Sie, dass G zu einem direkten Produkt von mehreren zyklischen Gruppen isomorph ist.
Hinweis: benutzen Sie Induktion nach n und die kanonische Abbildung $\mathrm{can}\colon G \to G/H$.

Aufgabe 6. (5 Punkte = 1 + 2 + 2)

(a) Mithilfe der Aufgabe 5 und einer Aussage aus der Vorlesung, folgern Sie:
Satz. Jede endliche abelsche Gruppe ist zu einem direkten Produkt von zyklischen Gruppen isomorph.

(b) Seien $p_1, p_2, \ldots, p_n$ beliebige Primzahlen und $N = p_1 p_2 \cdots p_n$. Zeigen Sie, dass es bis auf Isomorphie höchstens n^n endliche abelsche Gruppen der Ordnung N gibt.

(c) Sei G eine Gruppe der Ordnung 48 mit genau 12 Elemente der Ordnung 4. Bestimmen Sie G bis auf Isomorphie.

Aufgabe 7. (5 Punkte = 2 + 2 + 1)

Seien p eine Primzahl und $K_1 = \mathbb{F}_p$. Für $n \geqslant 1$ wählen wir jetzt rekursiv eine Körpererweiterung $K_{n+1} /\!\!/ K_n$ mit $p^{(n+1)!}$ Elementen, also $K_n \cong \mathbb{F}_{p^{n!}}$ für jedes n. Wir setzen $\mathbb{F}_{p^\infty} = \bigcup_{n=1}^{\infty} K_n$.

(a) Definieren Sie eine Addition und eine Multiplikation auf $\mathbb{F}_{p^\infty}$, die mit den Operationen auf jeden Unterkörper K_n übereinstimmen, und zeigen Sie, dass $\mathbb{F}_{p^\infty}$ auf diese Weise zu einem Körper wird.

(b) Zeigen Sie, dass $\mathbb{F}_{p^\infty}$ algebraisch abgeschlossen ist.

(c) Zeigen Sie, dass die Körpererweiterung $\mathbb{F}_{p^\infty} /\!\!/ \mathbb{F}_p$ algebraisch ist.

Einführung in die Algebra — Übungsblatt 12

Prof. Dr. Catharina Stroppel, Dr. Martin Palmer-Anghel (Assistent) // Wintersemester 17/18

[**Abgabe**: 18. Januar 2018, **vor** der Vorlesung, 10:00 – 10:15]

Aufgabe 1. (4 Punkte = 2 + 2)

(a) Zeigen Sie, dass $\mathbb{Q}(\sqrt{p})/\!\!/\mathbb{Q}$ eine normale Körpererweiterung ist, wobei p eine Primzahl ist.
(b) Zeigen Sie, dass $\mathbb{Q}(\sqrt[n]{p})/\!\!/\mathbb{Q}$ *keine* normale Körpererweiterung ist, wenn $n \geqslant 3$ (und p wieder eine Primzahl).

Aufgabe 2. (7 Punkte = 5 + 1 + 1)

Seien $\bar{K}$ ein algebraischer Abschluss von K und $K \subseteq L \subseteq \bar{K}$ ein Zwischenkörper. Zeigen Sie, dass die folgenden Eigenschaften äquivalent sind:

(i) $L/\!\!/K$ ist eine normale Körpererweiterung.
(ii) L ist ein Zerfällungskörper einer Teilmenge $S \subseteq K[t] \smallsetminus K$ über K.
(iii) Jeder K-Körperhomomorphismus $L \to \bar{K}$ hat Bild gleich L.

Seien jetzt $M/\!\!/L$ und $L/\!\!/K$ zwei Körpererweiterungen, so dass $M/\!\!/K$ normal ist.

(a) Zeigen Sie, dass $M/\!\!/L$ auch normal ist.
(b) Geben Sie ein Beispiel für diese Situation an, in dem $L/\!\!/K$ *nicht* normal ist.

Aufgabe 3. (5 Punkte = 3 + 2)

(a) Seien L ein endlicher Körper und $L/\!\!/K$ eine Körpererweiterung. Zeigen Sie, dass sie normal und separabel ist.
(b) Seien K ein Körper der Charakteristik $p > 0$, $a \in K$ und $f(t) = t^p - t - a \in K[t]$. Seien $L/\!\!/K$ eine Körpererweiterung und $b \in L$ eine Nullstelle von $f(t)$. Zeigen Sie, dass $f(t)$ über L in Linearfaktoren zerfällt, und beschreiben Sie diesen Zerfall explizit, indem Sie alle Nullstellen von $f(t)$ in L angeben.

Aufgabe 4. (4 Punkte)

Seien $M/\!\!/K$ eine algebraische Körpererweiterung und $K \subseteq L \subseteq M$ ein Zwischenkörper. Seien auch $\bar{K}$ und $\bar{L}$ algebraische Abschlüsse von K bzw. L mit $\bar{K} \subseteq \bar{L}$. Konstruieren Sie eine Bijektion

$$\mathrm{Hom}_K(L, \bar{K}) \times \mathrm{Hom}_L(M, \bar{L}) \longrightarrow \mathrm{Hom}_K(M, \bar{K})$$

und folgern Sie, dass der Separabilitätsgrad multiplikativ ist:

$$[\![M : L]\!]_{\mathrm{sep}} \cdot [\![L : K]\!]_{\mathrm{sep}} \;=\; [\![M : K]\!]_{\mathrm{sep}}.$$

Einführung in die Algebra — Übungsblatt 13

Prof. Dr. Catharina Stroppel, Dr. Martin Palmer-Anghel (Assistent) // Wintersemester 17/18

[**Abgabe**: 25. Januar 2018, **vor** der Vorlesung, 10:00 – 10:15]

Aufgabe 1. (6 Punkte = 1 + 2 + 2 + 1)

Seien $f(t) = t^3 - 3t - 1 \in \mathbb{Q}[t]$ und $L/\!\!/\mathbb{Q}$ ein Zerfällungskörper von $f(t)$ über $\mathbb{Q}$. Zeigen Sie:

(a) $f(t)$ ist irreduzibel über $\mathbb{Q}$ und hat keine mehrfache Nullstellen in L.
(b) Es gibt einen injektiven Gruppenhomomorphismus $\varphi\colon \mathrm{Gal}(L/\!\!/\mathbb{Q}) \to S_3$, dessen Bild entweder A_3 oder S_3 ist.
(c) Wenn a eine Nullstelle von $f(t)$ in L ist, dann sind $a^2 - a - 2$ und $2 - a^2$ die beiden anderen. Folgern Sie, dass φ nicht surjektiv ist, und deshalb, dass $\mathrm{Gal}(L/\!\!/\mathbb{Q})$ isomorph zu A_3 ist.
(d) Wie viele Zwischenkörper $\mathbb{Q} \subseteq K \subseteq L$ gibt es?

Aufgabe 2. (7 Punkte = 4 + 3)

In den folgenden Beispielen, zeigen Sie, dass $L/\!\!/\mathbb{Q}$ eine Galoiserweiterung ist und bestimmen Sie die Galoisgruppe $\mathrm{Gal}(L/\!\!/\mathbb{Q})$ und alle Zwischenkörper $\mathbb{Q} \subseteq K \subseteq L$.

(a) $L = \mathbb{Q}(\sqrt{2} + \sqrt{3})$,
(b) $L = \mathbb{Q}(e^{2\pi \mathrm{i}/5})$.

Hinweis zu (a): vergleichen Sie L mit dem Körper $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.
Hinweis zu (b): schauen Sie sich den Hinweis zu Aufgabe 1(d) auf Blatt 9 an.

Aufgabe 3. (3 Punkte)

Seien $L/\!\!/K$ eine endliche Körpererweiterung und $M/\!\!/K$ eine beliebige Körpererweiterung. Zeigen Sie, dass

$$|\mathrm{Hom}_K(L, M)| \leqslant [\![L : K]\!],$$

wobei $\mathrm{Hom}_K(L, M) = \{\varphi\colon L \to M \mid \varphi \text{ ist ein } K\text{-Homomorphismus von Körpern}\}$. Hinweis: betrachten Sie zunächst den Fall $L = K(a)$.

Aufgabe 4. (4 Punkte = 4 · 1)

Wahr oder falsch? Begründen Sie Ihre Antwort.

(a) Sei $M/\!\!/K$ eine separable Körpererweiterung und sei $K \subseteq L \subseteq M$ ein Zwischenkörper. Dann sind beide Erweiterungen $M/\!\!/L$ und $L/\!\!/K$ auch separabel.
(b) Die Körpererweiterung $\mathbb{Q}(\pi, \mathrm{i})/\!\!/\mathbb{Q}(\pi)$ ist Galois.
(c) Wenn $L/\!\!/K$ eine endliche Galoiserweiterung ist, dann gibt es genau $[\![L : K]\!]$ Zwischenkörper.
(d) Sei $L/\!\!/K$ eine endliche Galoiserweiterung mit keinen Zwischenkörpern außer K und L. Dann muss $[\![L : K]\!]$ eine Primzahl sein.

Einführung in die Algebra — Übungsblatt 14

Prof. Dr. Catharina Stroppel, Dr. Martin Palmer-Anghel (Assistent) // Wintersemester 17/18

[**Keine Abgabe** – nur zum Spaß und zur Vorbereitung auf die Klausur]

Klausur:

- **Mittwoch, den 14.02.2018 von 9:00 (s.t.!) bis 11:00.**
- Einsicht: Freitag, den 16.02.2018, Nachmittag (Zeit wird noch bekannt gegeben)
- Weitere Informationen zur Klausur auf der Webseite:
  www.math.uni-bonn.de/people/palmer/A1.html

Aufgabe 1. (4 Punkte = 2 + 2)

Seien $a = \sqrt[3]{2}$ und $b = e^{2\pi \mathrm{i}/3}$.
Von der Vorlesung wissen wir, dass $\mathbb{Q}(a,b)$ ein Zerfällungskörper von $t^3 - 2$ über $\mathbb{Q}$ ist, und außerdem, dass $G = \mathrm{Gal}(\mathbb{Q}(a,b)/\!\!/\mathbb{Q}) \cong S_3$ durch die Wirkung von G auf der Menge $\{a, ab, ab^2\}$.

(a) Zeigen Sie, dass a, ab und ab^2 paarweise algebraisch unabhängig sind.
(b) Beschreiben Sie explizit die Galoiskorrepondenz für die Galoiserweiterung $\mathbb{Q}(a,b)/\!\!/\mathbb{Q}$.

Aufgabe 2. (11 Punkte = 2 + 1 + 1 + 2 + 5)

Seien $f(t) = t^4 - 2 \in \mathbb{Q}[t]$ und $L/\!\!/\mathbb{Q}$ ein Zerfällungskörper von $f(t)$ über $\mathbb{Q}$.

(a) Zeigen Sie, dass $L = \mathbb{Q}(\alpha, \mathrm{i})$, wobei $\alpha = \sqrt[4]{2}$, und $[\![L : \mathbb{Q}]\!] = 8$.
(b) Konstruieren Sie einen injektiven Gruppenhomomorphismus $\phi\colon G = \mathrm{Gal}(L/\!\!/\mathbb{Q}) \hookrightarrow S_4$.
(c) Zeigen Sie, dass die Untergruppen $\phi(G)$ und D_4 von S_4 zueinander konjugiert sind. Deshalb gibt es einen Isomorphismus $G \cong D_4$.
(d) Zeigen Sie jetzt, dass es Elemente $\varphi, \psi \in G$ mit $\varphi(\alpha) = \mathrm{i}\alpha$, $\varphi(\mathrm{i}) = \mathrm{i}$, $\psi(\alpha) = \alpha$ und $\psi(\mathrm{i}) = -\mathrm{i}$ gibt und beschreiben Sie damit *explizit* einen Isomorphismus $G \cong D_4$.
(e) Beschreiben Sie explizit die Galoiskorrespondenz für die Galoiserweiterung $L/\!\!/\mathbb{Q}$.

Aufgabe 3. (15 Punkte = 3 + 1 + 3 + 2 + 3 + 1 + 2)

(a) Bestimmen Sie die irreduziblen Faktoren des Polynoms $t^4 + 1 \in \mathbb{F}_p[t]$ für $p = 2, 3, 5$.

In dieser Aufgabe werden wir unter anderem zeigen, dass t^4+1 reduzibel über $\mathbb{F}_p$ für alle Primzahlen p ist.

Sei n eine positive ganze Zahl und sei $\Phi_n(t) \in \mathbb{Z}[t]$ das n-te Kreisteilungspolynom, dessen Grad gleich $\varphi(n)$ ist. Sei auch K ein Körper und $r\colon \mathbb{Z} \to K$ der eindeutige Ringhomomorphismus. Wir schreiben $\Phi_n(t) = \sum_i a_i t^i$ und definieren $\hat{\Phi}_n(t) = \sum_i r(a_i) t^i \in K[t]$. Sei L ein Zerfällungskörper von $\hat{\Phi}_n(t)$ über K.

Wir nehmen an, dass $n \neq 0 \in K$, d.h., entweder $\mathrm{char}(K) = 0$ oder $\mathrm{char}(K) = p > 0$ und $p \nmid n$.

Zeigen Sie:

(b) $\hat{\Phi}_n(t)$ hat keine mehrfache Nullstellen in L.
(c) Wenn α eine Nullstelle von $\hat{\Phi}_n(t)$ in L ist, dann ist $\alpha^n = 1$ und $\alpha^m \neq 1$ für alle $0 < m < n$. *Hinweis: angenommen für einen Widerspruch, dass $\alpha^m = 1$ für $m \mid n$ und $m \neq n$. Zeigen Sie, dass α dann eine mehrfache Nullstelle von $t^n - 1$ sein muss, was nicht existieren kann.*
(d) Sei M ein Zerfällungskörper von $t^n - 1$ über L (was deshalb auch ein Zerfällungskörper von $t^n - 1$ über K ist). Zeigen Sie, dass $M = L = K(\alpha)$. Folgern Sie, dass jeder irreduzible Faktor von $\hat{\Phi}_n(t) \in K[t]$ den Grad $[\![L : K]\!]$ hat.

Seien jetzt $K = \mathbb{F}_p$ und $d = [\![L : \mathbb{F}_p]\!]$. Sei e die Ordnung des Elements $[p]$ in der Gruppe $(\mathbb{Z}/n\mathbb{Z})^\times$.

(e) Zeigen Sie, dass $d = e$.
Hinweis: $L^\times$ ist eine zyklische Gruppe.

(f) Deshalb hat $\hat{\Phi}_n(t)$ genau $\varphi(n)/e$ irreduzible Faktoren über $\mathbb{F}_p$. Insbesondere ist dieses Polynom irreduzibel über $\mathbb{F}_p$ genau dann, wenn $[p]$ ein Erzeuger der Gruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ ist.

(g) Zeigen Sie, dass $\hat{\Phi}_8(t) = t^4 + 1$ und $\hat{\Phi}_{12}(t) = t^4 - t^2 + 1$ reduzibel über $\mathbb{F}_p$ für alle Primzahlen p sind.

Aufgabe 4. (14 Punkte = $14 \cdot 1$) — *Wiederholung* —

Wahr oder falsch? Begründen Sie Ihre Antwort.

(a) Die Gruppe $(\mathbb{Q}, +)$ ist endlich erzeugt.

(b) Wenn G und H zwei Gruppen sind, gibt es auf der Menge $G \times H$ genau eine Struktur einer Gruppe, so dass $g \mapsto (g, 1_H) \colon G \to G \times H$ und $h \mapsto (1_G, h) \colon H \to G \times H$ Gruppenhomomorphismen sind.

(c) Seien m, n positive natürliche Zahlen. Dann ist das Element $\overline{m} = m + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ genau dann ein Erzeuger der Gruppe, wenn m und n teilerfremd sind.

(d) Sei G eine Gruppe mit $|G| = 54$. Es gibt genau zwei Gruppenhomomorphismen $G \to \mathbb{Z}/2\mathbb{Z}$.

(e) Es gibt eine offensichtliche Operation von S_n auf der Menge aller Teilmengen von $\{1, \dots, n\}$. Wenn $n \geqslant 2$ hat diese Operation genau einen Fixpunkt.

(f) $\mathbb{C}[t_1, \dots, t_n]$ ist ein Hauptidealring für jede Zahl $n \geqslant 1$.

(g) Die Einheitengruppe $\mathbb{Z}[\mathrm{i}\sqrt{5}]^\times$ hat die Ordnung 2.

(h) Das Polynom $t^5 - 10t^2 + 20 \in \mathbb{Z}[t]$ ist irreduzibel.

(i) Die Untergruppe $\{z \in \mathbb{C} \mid z^n = 1 \text{ für eine ganze Zahl } n\} < \mathbb{C}^\times$ ist isomorph zur Quotientengruppe $\mathbb{Q}/\mathbb{Z}$.

(j) $[\![\mathbb{Q}(\sqrt[3]{2}, e^{\pi \mathrm{i}/4}) : \mathbb{Q}]\!] = 12$.

(k) Sei $L /\!\!/ K$ eine endliche Körpererweiterung. Dann kann jeder Körperautomorphismus von K auf L erweitert werden.

(l) Jede endliche Körpererweiterung ist separabel.

(m) Sei $L /\!\!/ \mathbb{Q}$ eine algebraische Körpererweiterung. Dann gibt es eine weitere Körpererweiterung $M /\!\!/ L$, so dass $M /\!\!/ \mathbb{Q}$ und $M /\!\!/ L$ Galois sind.

(n) Sei K ein endlicher Körper mit $|K| = 2^r$. Dann hat jedes Element $x \in K$ eine Quadratwurzel, d.h., es gibt $y \in K$, so dass $x = y^2$.