Übungblätter zur Algebra und Zahlentheorie bei Soergel im WS 2024/25

Allgemeine Hinweise:

- Bei der Bearbeitung der Üungen und später der Klausuraufgaben ist keine übertriebene Ausführlichkeit gefordert. Einfach zu schreiben, es sei klar, reicht nicht, aber eine schlüssige Kette von richtigen Argumenten in der nächsten Stufe der Ausführlichkeit reicht aus. Allerdings soll die Argumentationskette auch für Sie selbst schlüssig sein. Sie müssen sie im Tutorat erklären können und in der Lage sein, auf Nachfragen Schritte Ihrer Argumentation genauer auszuführen. In der Vorlesung bewiesene Aussagen müssen dabei aber keinesfalls nochmals bewiesen werden, da reicht ein Zitat.

- Es gibt jede Woche vier Aufgaben und für jede Aufgabe gibt es vier Punkte, obwohl der Schwierigkeitsgrad der Aufgaben durchaus sehr unterschiedlich sein wird. Ergänzende Übungen sind meist schwieriger, sind für die Klausur nicht relevant und geben bis zu vier Bonuspunkte.

- Die Übungen werden Dienstags ausgegeben und müssen die Woche danach am Dienstag vor der Vorlesung abgegeben werden. Sie seien ermutigt, die Aufgaben mit Ihren Kommilitonen zu besprechen und zu zweit abzugeben. Mehr als zwei Namen auf einem Zettel gilt aber nicht.

- Die Übungen werden auf den folgenden Seiten dieses Textes ins Netz gestellt, der jede Woche um das Übungsblatt der jeweiligen Woche ergänzt werden wird.

Anwesenheitsaufgaben zweite Vorlesungswoche Algebra und Zahlentheorie

Diese Übungen müssen nicht abgegeben werden, sondern sollen im Laufe der zweiten Vorlesungswoche in den Tutoraten bearbeitet werden. Zu diesem Zeitpunkt liegen ja noch keine korrigierten Hausaufgaben vor, die zu besprechen wären.

Übung 0.1. Seien M ein Monoid und e sein neutrales Element. Man zeige: Unser Monoid ist genau dann eine Gruppe, wenn es für jedes $a \in M$ ein $\bar{a} \in M$ gibt mit $\bar{a} \top a = e$, und dies Element $\bar{a}$ ist dann notwendig das Inverse von a in M.

Übung 0.2. Ein endliches Monoid $(M, \top)$, in dem für jedes Element $a \in M$ die Multiplikationsabbildung eine Injektion $(a\top) : M \hookrightarrow M$ ist, muß bereits eine Gruppe sein.

Übung 0.3 (**Koinduzierte Verknüpfung**). Sei $(X, \top)$ eine Menge mit Verknüpfung. Gegeben eine Surjektion $X \twoheadrightarrow Q$ gibt es höchstens eine Verknüpfung auf Q derart, daß unsere Surjektion ein Homomorphismus von Magmas ist. Wenn es solch eine Verknüpfung gibt, heißt unsere Surjektion **an die Verknüpfung angepaßt** und die fragliche Verknüpfung auf Q die **auf Q koinduzierte Verknüpfung**. Zum Beispiel ist die Surjektion $\mathbb{N} \twoheadrightarrow \{0, 1, \ldots, 9\}$, die jeder Zahl die letzte Ziffer ihrer Dezimaldarstellung zuordnet, angepaßt sowohl an die Addition als auch an die Multiplikation.

Übung 0.4 (**Eigenschaften einer koinduzierten Verknüpfung**). Die Eigenschaften der Assoziativität und Kommutativität übertragen sich auf die koinduzierte Verknüpfung. Das Bild des Einselements ist ein Einselement für die koinduzierte Verknüpfung, das Bild des Inversen ein Inverses. Jede koinduzierte Verknüpfung zu einer angepaßten Surjektion von einer Gruppe auf eine Menge macht besagte Menge zu einer Gruppe.

Übung 0.5. Ist M eine Menge mit assoziativer Verknüpfung und existiert ein $e \in M$ mit $e \top a = a \; \forall a \in M$ sowie für jedes $a \in M$ ein $\bar{a} \in M$ mit $\bar{a} \top a = e$, so ist M eine Gruppe. Hinweis: Man zeige, daß $\bar{a}\top$ bijektiv ist.

Übungen Algebra und Zahlentheorie

Abgabe bis Dienstag, den 22.10 um 10:15

Übung 1.1. Eine endliche nichtleere Teilmenge einer Gruppe, die mit je zwei Elementen auch die Verknüpfung der beiden enthält, ist notwendig bereits eine Untergruppe.

Übung 1.2. Wieviele Untergruppen hat die additive Gruppe eines zweidimensionalen Vektorraums über dem Körper mit zwei Elementen? Wieviele Untergruppen hat die additive Gruppe eines n-dimensionalen Vektorraums über dem Körper mit zwei Elementen?

Übung 1.3. Man berechne den größten gemeinsamen Teiler von 3456 und 436 und eine Darstellung desselben als ganzzahlige Linearkombination unserer beiden Zahlen.

Übung 1.4. Gegeben zwei von Null verschiedene natürliche Zahlen a, b nennt man die kleinste von Null verschiedene natürliche Zahl, die sowohl ein Vielfaches von a als auch ein Vielfaches von b ist, das **kleinste gemeinsame Vielfache** von a und b und notiert sie $\mathrm{kgV}(a, b)$. Man zeige in dieser Notation die Formel $\mathrm{kgV}(a, b)\,\mathrm{ggT}(a, b) = ab$.

Übungen Algebra und Zahlentheorie

Abgabe bis Dienstag, den 29.10 um 10:15

Übung 2.1. Haben zwei endliche Untergruppen einer Gruppe teilerfremde Kardinalitäten, so besteht ihr Schnitt nur aus dem neutralen Element.

Übung 2.2. Man zeige, daß in der symmetrischen Gruppe $\mathcal{S}_4$ die Doppeltranspositionen zusammen mit dem neutralen Element einen Normalteiler $D \subset \mathcal{S}_4$ bilden, und konstruiere einen Isomorphismus $\mathcal{S}_4/D \xrightarrow{\sim} \mathcal{S}_3$.

Übung 2.3. Gegeben ein surjektiver Gruppenhomomorphismus $\varphi : G \twoheadrightarrow \bar{G}$ und ein Normalteiler $\bar{N} \subset \bar{G}$ mit Urbild $\varphi^{-1}(\bar{N}) = N \subset G$ induziert φ einen Gruppenisomorphismus

$$\varphi : G/N \xrightarrow{\sim} \bar{G}/\bar{N}$$

Übung 2.4. Sei $G \supset H$ eine Gruppe mit einer Untergruppe. Ist G/H endich, so zeige man, daß H einen Normalteiler N von G umfaßt mit G/N endlich.

Übungen Algebra und Zahlentheorie

Abgabe bis Dienstag, den 5.11 um 10:15

Übung 3.1. Man führe die Induktion zum Beweis des Chinesischen Restsatzes aus und zeige: Ist $m = q_1 \dots q_s$ ein Produkt von paarweise teilerfremden ganzen Zahlen, so liefert die offensichtliche Abbildung einen Isomorphismus

$$\mathbb{Z}/m\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/q_1\mathbb{Z} \times \ldots \times \mathbb{Z}/q_s\mathbb{Z}$$

Übung 3.2. Gegeben Primzahlen $p_1, \dots, p_r$ und eine Zahl e mit

$$e \equiv 1 \pmod{(p_i - 1)} \; \forall i$$

zeige man für alle $a \in \mathbb{Z}$ die Kongruenz $a^e \equiv a \pmod{(p_1 \dots p_r)}$.

Übung 3.3. Gibt es ein Vielfaches von 17, dessen letzte Ziffern 39 lauten? Wie rechnen Sie sowas aus?

Übung 3.4. Wieviele Möglichkeiten gibt es, für eine Schatzsuche eine Klasse mit 21 Schülern in drei Mannschaften zu je sieben Schülern aufzuteilen? Wie hilft die Bahnformel?

Übungen Algebra und Zahlentheorie

Abgabe bis Dienstag, den 12.11 um 10:15

Übung 4.1. Man gebe eine Kompositionsreihe der symmetrischen Gruppe $\mathcal{S}_4$ an.

Übung 4.2. Man zeige: Jede Untergruppe einer nilpotenten Gruppe ist nilpotent.

Übung 4.3. Man zeige: Für jede Primzahl p gibt es bis auf Isomorphismus genau zwei Gruppen der Ordnung $2p$, eine zyklische Gruppe und eine Diedergruppe. Hinweis: Man erinnere die Argumentation im Fall $p = 3$ und interessiere sich für die Anzahl der 2-Sylows.

Übung 4.4. Wieviele p-Sylows hat die Gruppe $\mathrm{GL}(2; \mathbb{F}_p)$?

Übungen Algebra und Zahlentheorie

Abgabe bis Dienstag, den 19.11 um 10:15

Übung 5.1. Gegeben eine endliche Menge X und eine Abbildung $f : X \to X$ zeige man, daß es natürliche Zahlen m, n gibt mit $n \geq 1$ und $f^m = f^{m+n}$.

Übung 5.2. Man zeige, daß das Bild eines Ideals unter einem surjektiven Ringhomomorphismus stets wieder ein Ideal ist.

Übung 5.3. Man zeige, daß es für jeden Ring R genau einen Ringhomomorphismus $\mathbb{Z} \to R$ gibt.

Übung 5.4. Man finde das multiplikative Inverse der Nebenklasse von 22 im Körper $\mathbb{F}_{31}$. Hinweis: Euklidischer Algorithmus.

Übungen Algebra und Zahlentheorie

Abgabe bis Dienstag, den 26.11 um 10:15

Übung 6.1. Man zeige: Eine natürliche Zahl, die kongruent zu sieben ist modulo acht, kann nicht eine Summe von drei Quadraten sein. Nebenbei bemerkt ist auch jede natürliche Zahl, die nicht kongruent zu sieben ist modulo acht, eine Summe von drei Quadraten. Das aber ist keine Übungsaufgabe mehr, sondern braucht solide Grundlagen in Zahlentheorie.

Übung 6.2. Man finde ein Nichtquadrat a im Körper $\mathbb{F}_5$ und zeige, daß der Restklassenring $\mathbb{F}_5[X]/\langle X^2 - a\rangle$ ein Körper mit 25 Elementen ist.

Übung 6.3. Man zeige, daß $\mathbb{Z}[X]$ kein Hauptidealring ist.

Übung 6.4. Sei k ein Körper. Man zeige: (1) Alle Polynome vom Grad 1 sind irreduzibel in $k[X]$. (2) Ist $P \in k[X]$ irreduzibel und $\operatorname{grad} P > 1$, so hat P keine Nullstelle in k. (3) Ist $P \in k[X] \setminus k$ vom Grad $\operatorname{grad} P \leq 3$ und hat P keine Nullstelle in k, so ist P irreduzibel in $k[X]$. (4) Ist k algebraisch abgeschlossen, so sind die irreduziblen Polynome in $k[X]$ genau die Polynome vom Grad 1. Man gebe auch (5) ein Polynom positiven Grades in $\mathbb{R}[X]$ an, das keine Nullstelle hat, aber dennoch nicht irreduzibel ist.

Übungen Algebra und Zahlentheorie

Abgabe bis Dienstag, den 3.12 um 10:15

Übung 7.1. Man schreibe $9 + 13\mathrm{i}$ als Produkt von Gaußprimzahlen.

Übung 7.2. Man bestimme sämtliche Zerlegungen von 1000 in eine Summe von zwei Quadratzahlen.

Übung 7.3. Seien R ein faktorieller Ring und $q \in \mathrm{Quot}(R)$ ein Element seines Quotientenkörpers und $n \geq 1$ mit $q^n \in R$. Man zeige $q \in R$.

Übung 7.4. Man bestimme die Partialbruchzerlegung von $1/(x^4 + 2)$ in $\mathbb{C}(X)$.

Übungen Algebra und Zahlentheorie

Abgabe bis Dienstag, den 10.12 um 10:15

Übung 8.1. Seien k ein Körper und $0 < n(1) < n(2) < \ldots < n(r) < n$ natürliche Zahlen, $r \geq 0$. Man zeige, daß das Polynom

$$T^n + a_r T^{n(r)} + \ldots + a_1 T^{n(1)} + a_0$$

irreduzibel ist in $K[T]$, für $K = \operatorname{Quot} k[' a_0, \ldots, a_r]$ der Funktionenkörper. Hinweis: Jede Zerlegung käme von einer Zerlegung im Polynomring $k[' a_0, \ldots, a_r, T]$ her und müßte unter dem Einsetzen $a_1 = \ldots = a_r = 0$ zu einer Zerlegung von $T^n + a_0$ in $k[' a_0, T]$ führen.

Übung 8.2. Man zeige, daß $X^7 - 9$ ein irreduzibles Polynom in $\mathbb{Z}[X]$ ist. Hinweis: Man betrachte die Einbettung $\mathbb{Z}[X] \hookrightarrow \mathbb{Z}[Y]$ mit $X \mapsto Y^2$.

Übung 8.3. Man zerlege $(X^n - Y^n)$ in $\mathbb{C}[X, Y]$ in ein Produkt irreduzibler Faktoren.

Übung 8.4. Was ist die Summe der $\lambda_1^3 + \lambda_2^3 + \lambda_3^3 + \lambda_4^3$ dritten Potenzen der vier komplexen Nullstellen $\lambda_1, \ldots, \lambda_4$ des Polynoms $X^4 + 3X^3 - 5X^2 + X + 1$?

Übungen Algebra und Zahlentheorie

Abgabe bis Dienstag, den 17.12 um 10:15

Übung 9.1. Gegeben $a, b \in \mathbb{Q}^\times$ zeige man, daß gilt $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{b})$ genau dann, wenn a/b in $\mathbb{Q}$ ein Quadrat ist. Zum Beispiel folgt $\sqrt{5} \notin \mathbb{Q}(\sqrt{2})$.

Übung 9.2. Seien K ein Körper und $P \in K[X] \backslash K$ ein nichtkonstantes Polynom. So ist der Ringhomomorphismus $K[Y] \to K[X]$ mit $Y \mapsto P$ injektiv und die davon induzierte Körpererweiterung $K(Y) \hookrightarrow K(X)$ hat als Grad den Grad von P.

Übung 9.3. Alle Elemente von $\mathbb{Q}(\sqrt[3]{2})$ lassen sich eindeutig schreiben in der Form $a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2$ mit $a, b, c \in \mathbb{Q}$. Man schreibe das Inverse von $7 + \sqrt[3]{2}$ in dieser Form.

Übung 9.4. Ist $\sqrt{2} + \sqrt{3}$ algebraisch über $\mathbb{Q}$? Wenn ja, was ist sein Minimalpolynom über $\mathbb{Q}$? Liegt $\sqrt{2}$ in $\mathbb{Q}(\sqrt{2} + \sqrt{3})$?

Übungen Algebra und Zahlentheorie

Abgabe bis Dienstag, den 7.1 um 10:15

Übung 10.1. Geben Sie einen Körperisomorphismus $\mathbb{F}_7(\sqrt{3}) \xrightarrow{\sim} \mathbb{F}_7(\sqrt{5})$ an als $\mathbb{F}_7$-lineare Abbildung in Bezug auf die Basen $1, \sqrt{3}$ links und $1, \sqrt{5}$ rechts.

Übung 10.2. Man zeige, daß es gegeben eine Primzahl $p > 2$ und $r \geq 1$ stets einen endlichen Körper der Charakteristik p gibt, dessen multiplikative Gruppe ein Element der Ordnung 2^r hat.

Übung 10.3. Gegeben eine endliche Körpererweiterung $K \subset L$ zeige man, daß jedes Polynom aus dem Polynomring $L[X]$ Teiler eines Polynoms aus dem Polynomring $K[X]$ ist.

Übung 10.4. Man zeige: Gegeben eine Primzahl p und zwei p-te Einheitswurzeln $\zeta, \xi \in \mathbb{C}$ der Ordnung p gilt $\mathbb{Q}(\zeta) = \mathbb{Q}(\xi)$ und es gibt genau einen Körperhomomorphismus $\mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta)$ mit $\zeta \mapsto \xi$. Hinweis: Irreduzibilität des p-ten Kreisteilungspolynoms.

Übungen Algebra und Zahlentheorie

Abgabe bis Dienstag, den 14.1 um 10:15

Übung 11.1. Man zeige: Ein Polynom mit Koeffizienten in einem Körper K der Charakteristik Null ist separabel genau dann, wenn es von keinem Quadrat eines K-irreduziblen Polynoms geteilt wird.

Übung 11.2. Finden Sie alle komplexen mehrfachen Nullstellen des Polynoms $X^4 - 4X^3 + 5X^2 - 4X + 4$.

Übung 11.3. Man zeige: Seien $M \supset L \supset K$ Körper. Ist M/L separabel und L/K separabel, so ist M/K separabel. Hinweis: Man ziehe sich zunächst auf den Fall endlicher Erweiterungen zurück und verwende dann den Satz über die Charakterisierungen separabler Körpererweiterungen.

Übung 11.4. Eine algebraische Körpererweiterung derart, daß nur die Elemente des kleinen Körpers über diesem separabel sind, heißt **rein inseparabel**. Man zeige, daß eine algebraische Erweiterung L/K eines Körpers K der Charakteristik $p > 0$ rein inseparabel ist genau dann, wenn für jedes Element von L die p^r-te Potenz für hinreichend großes r in K liegt.

Übungen Algebra und Zahlentheorie

Abgabe bis Dienstag, den 21.1 um 10:15

Übung 12.1. Gegeben $n \geq 1$ zeige man, daß $\mathbb{C}(X^n) \subset \mathbb{C}(X)$ eine Galoiserweiterung vom Grad n ist mit zyklischer Galoisgruppe.

Übung 12.2. Man bestimme die Galoisgruppe des Zerfällungskörpers des Polynoms $X^4 - 5$ über $\mathbb{Q}$ und über $\mathbb{Q}[\mathrm{i}]$.

Übung 12.3. Man zeige: Gegeben eine endliche Galoiserweiterung L/K ist die **Spurabbildung** $\mathrm{S}_L^K : L \to K$ gegeben durch

$$x \mapsto \sum_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x)$$

eine K-lineare von Null verschiedene Abbildung und die **Spurform** $L \times L \to K$ gegeben durch $(x, y) \mapsto \mathrm{S}_L^K(xy)$ ist eine nichtausgeartete Bilinearform auf dem K-Vektorraum L. Hinweis: Lineare Unabhängigkeit von Charakteren.

Übung 12.4. Seien k ein Körper der Charakteristik $p > 0$ und $\lambda \in k^\times$ und $t = t_\lambda : k(X) \xrightarrow{\sim} k(X)$ der Körperautomorphismus über k mit $X \mapsto X + \lambda$. Man zeige, daß der Körper der Invarianten genau das Bild derjenigen Einbettung $k(Y) \hookrightarrow k(X)$ ist, die durch $Y \mapsto X^p - \lambda^{p-1}X$ gegeben wird.

Übungen Algebra und Zahlentheorie

Abgabe bis Dienstag, den 28.1 um 10:15

Bis Freitag 24.1 Anmeldung zur Klausur,
bis Sonntag 26.1 Evaluation.

Übung 13.1. Man zeige: Gegeben eine Körpererweiterung L/K und zwei verschiedene normierte irreduzible Polynome in $K[X]$ kann kein Element der Galoisgruppe eine Nullstelle des einen Polynoms in eine Nullstelle des anderen Polynoms überführen.

Übung 13.2. Wieviele zu 140000 teilerfremde Zahlen a mit $1 \leq a \leq 140000$ gibt es?

Übung 13.3. Man zeige, daß die Einheitswurzeln des n-ten Kreisteilungskörpers für gerades n genau die n-ten Einheitswurzeln sind und für ungerades n genau die $2n$-ten Einheitswurzeln.

Übung 13.4. Gegeben $n > 2$ zeige man, daß im Kreisteilungskörper $\mathbb{Q}(\sqrt[n]{1}) = \mathbb{Q}(\zeta)$ für ζ eine primitive n-te Einheitswurzel gilt $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})] = 2$ und $[\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}] = \varphi(n)/2$. Man folgere $\Phi_n(X) = X^{\varphi(n)}\Phi_n(X^{-1})$.

Klausur Algebra und Zahlentheorie

am Dienstag, den 25.2.2025

Übung 14.1. Wieviele zu 27000 teilerfremde Zahlen a mit $1 \leq a \leq 27000$ gibt es?

Übung 14.2. Was ist die Summe $\lambda_1^2+\lambda_2^2+\lambda_3^2+\lambda_4^2$ der Quadrate der vier komplexen Nullstellen $\lambda_1, \ldots, \lambda_4$ des Polynoms $2X^4 - 6X^3 + X + 15$?

Übung 14.3. Man schreibe $4 + 18\mathrm{i}$ als Produkt von Gaußprimzahlen.

Übung 14.4. Man bestimme das Minimalpolynom von $\sqrt{5} + 2\sqrt{3}$ über $\mathbb{Q}$. Man bestimme alle Zwischenkörper der von diesem Element erzeugten Körpererweiterung von $\mathbb{Q}$.

Übung 14.5. Man finde das multiplikative Inverse der Nebenklasse von 21 im Körper $\mathbb{F}_{97}$.

Übung 14.6. Man zeige, daß das Bild eines Ideals unter einem surjektiven Ringhomomorphismus stets wieder ein Ideal ist.

Übung 14.7. Man bestimme die Galoisgruppe des Zerfällungskörpers des Polynoms $X^6 - 9$ über $\mathbb{Q}$ und über $\mathbb{Q}[\mathrm{i}]$.

Übung 14.8. Welche Möglichkeiten gibt es für die Anzahl der 2-Sylows einer Gruppe mit 24 Elementen? Geben Sie jeweils ein Beispiel an.