

# Hinweise zu den Übungsaufgaben in Algebra II

## Übungsblatt 3

**Aufgabe 1.** Teilaufgabe a) hat etwas mit Standgruppen zu tun. Für Teilaufgabe b) ist interessant, was Fixpunkte mit Bahnen zu tun haben. (Was sind Fixpunkte denn überhaupt, und was sind Bahnen?) Welche Gleichung der Vorlesung ist also vermutlich anwendbar?

**Aufgabe 4.** Ein beliebiges Element der disjunkt-gemachten Vereinigung  $Y_1 \amalg \cdots \amalg Y_n$  ist ein Paar  $(i, y)$ , wobei  $i \in \{1, \dots, n\}$  ein Index und  $y$  ein Element der entsprechenden Menge  $Y_i$  ist. Ein *Isomorphismus von  $G$ -Wirkungen* ist per Definition eine bijektive  $G$ -äquivariante Abbildung. Für Teilaufgabe b) ist es hilfreich,  $X$  in Bahnen zu zerlegen.

**Aufgabe 5.** Diese Aufgabe benötigt aber nur die Definition von Normalteilern und das Verständnis der mengentheoretischen Schreibweise: Die Menge  $N$  besteht aus all den Elementen von  $G$ , welche in allen  $N_i$  liegen. Über die Größe von  $I$  kann nichts vorausgesetzt werden. Wer mag, kann aber zuerst den Fall des Schnitts zweier Normalteiler behandeln; der allgemeine Fall verläuft ähnlich.

## Übungsblatt 4

**Aufgabe 1.** Ein *kleinster Normalteiler*, welcher  $H$  umfasst, ist per Definition ein Normalteiler  $N$  in  $G$ , welcher  $H$  umfasst und welcher folgende Eigenschaft hat: Für jeden beliebigen Normalteiler  $N'$  in  $G$ , welcher  $H$  umfasst, gilt  $N \subseteq N'$ .

**Aufgabe 2.** In beiden Teilaufgaben geht es nicht um Umkehrfunktionen, sondern um Urbildmengen.

**Aufgabe 3.** Die Gruppe  $\mathrm{GL}_n(\mathbb{R})$  ist die Menge der invertierbaren  $(n \times n)$ -Matrizen, mit der Matrixmultiplikation als Gruppenverknüpfung. Die Untergruppe  $\mathrm{O}_n(\mathbb{R})$  ist die Teilmenge der orthogonalen Matrizen. Eine Matrix  $A$  heißt genau dann *orthogonal*, wenn das Produkt  $A^t A$  die Einheitsmatrix ist. Orthogonale Matrizen haben als Determinante stets  $\pm 1$ . Die Untergruppe  $\mathrm{SO}_n(\mathbb{R})$  ist die Teilmenge solcher orthogonalen Matrizen, deren Determinante  $+1$  ist. Für die Determinante gilt die Rechenregel  $\det(AB) = \det(A) \cdot \det(B)$ .

Bei Teilaufgabe b) muss man sich zunächst überlegen, ob man  $\mathrm{SO}_n(\mathbb{R})$  auf  $C_2$  oder umgekehrt wirken lassen möchte (nur eine Variante funktioniert), und wie diese Wirkung explizit aussehen soll. Wie bei Teilaufgabe c) die Gruppe  $\mathrm{SO}_3(\mathbb{R})$  auf  $\mathbb{R}^3$  wirkt, ist im Skript angegeben (Beispiel 6.76).

Im Staatsexamen ist das halbdirekte Produkt immer wieder wichtig, um die öfter vorkommenden Aufgaben der Art *Geben Sie eine nicht-abelsche Gruppe der Ordnung 2012 an.* zu lösen.

*Für Teilnehmer des Pizzaseminars:* Findet ihr eine kategoriale Beschreibung des halbdirekten Produkts? (So, wie man das direkte Produkt auch als terminales Objekt in der Kategorie der Möchtegern-Produkte beschreiben kann.)

Die Diagonaleinträge mit  $+1$  besetzt sind, spielt bei Teilaufgabe b) eine Rolle. Wer mich anschreibt, bekommt weitere Tipps.  
Die Diagonaleinträge die oben links eine  $-1$  stehen und deren restliche Diagonaleinträge

**Aufgabe 4.** Eine endliche Gruppe heißt genau dann *p-Gruppe*, wenn die Anzahl ihrer Elemente eine *p-Potenz* ist.

Das Kriterium aus a) ist für b) nutzlich.  
Eine nichttriviale *p*-Gruppe besitzt stets ein Element der Ordnung *p* in ihrem Zentrum.

**Aufgabe 5.** Ein *größter endlicher auflösbarer Normalteiler* ist per Definition ein Normalteiler *N* in *G*, welcher selbst endlich und auflösbar ist und folgende Eigenschaft hat: Für jeden beliebigen endlichen auflösbaren Normalteiler *N'* in *G* gilt  $N' \subseteq N$ .

Für b) ist a) nutzlich.

## Übungsblatt 4

Auf dem gesamten Übungsblatt bezeichnet „*p*“ stets eine Primzahl.

**Aufgabe 1.** Konventionsgemäß ist die Zahl 1 eine *p-Potenz*. (Wieso ist das sinnvoll und für Teilaufgabe b) wichtig?)

**Aufgabe 2.** Eine *p-Untergruppe von G* ist per Definition eine Untergruppe von *G*, deren Ordnung eine *p-Potenz* ist. Eine Untergruppe *H* heißt per Definition genau dann *maximal unter allen p-Untergruppen von G*, wenn sie selbst eine *p-Untergruppe von G* ist und außerdem folgende Eigenschaft hat: Ist  $K \subseteq G$  eine beliebige *p-Untergruppe mit  $H \subseteq K$* , so gilt schon  $H = K$ .

Eine *maximale p-Untergruppe* ist also etwas anderes als eine *größte p-Untergruppe*!

Ein Beispiel zu einem ganz anderen Thema soll den Unterschied verdeutlichen: Unter den Mengen  $\emptyset, \{a\}, \{a, b\}, \{a, b, c\}, \{d\}, \{d, e\}, \{d, f\}$  gibt es keine größte, aber drei maximale: Namlich  $\{a, b, c\}, \{d, e\}$  und  $\{d, f\}$ . Ferner gibt es kleine kleinste (namlich  $\emptyset$ ). Diese ist auch minimal. Ergänzt man noch die Menge  $\{a, b, c, d, e, f\}$ , so ändert sich die Situation: Diese neue Menge ist jetzt die Menge  $\{a, b, c, d, e, f\}$ , die maximal ist. Außerdem ist sie die größte. Für eine der Rückfragen der Behauptung *der Aufgabe hilft der erste Sylowsche Satz*.

**Aufgabe 3.** Captain Obvious bittet mich, folgenden Tipp zu verbreiten: Die Sylowschen Sätze könnten helfen.

An dieser Stelle hatte ich ein vollständiges Schema versprochen, jedoch muss das bis nach der Besprechung warten, da ein solches zu viel vorwegnehmen würde. Auf Anfrage gebe ich aber trotzdem gerne weitere Tipps.

Ein Beispiel zur Überlappungstheorie: Eine Untergruppe mit  $2^2 \cdot 3^2$  Elementen kann nur im Identitätslement mit einer Untergruppe von  $7^2 \cdot 11^3$  überlappen (wieso?). Eine Untergruppe mit  $2^2 \cdot 3^2$  Elementen kann mit einer Untergruppe von  $3^2 \cdot 11^3$  Elementen in höchstens  $3^2$  Elementen überlappen (wieso?).

gegeben müsste, als faktisch in der Gruppe vorhanden sind. Wenn Widerspruch herzuleiten: Die Elementübersicht muss zeigen, dass es mehr Elemente als Identitätslement gemeinsam (wie so?). Mit diesen Überlegungen kann man versuchen, das Identitätslement zu unterscheiden. Primzahlen haben aber stets nur überlappen. Sylowsche Untergruppen zu verschiedenen Primzahlen können zur selben Primzahl identisch werden. Außerdem können sich Sylowsche Untergruppen zu einer Primzahl mehrfach gesetzt haben aber all diese Untergruppen gemeinsam und darf daher nicht mehrfach gesetzt sein. Das Identitätslement scheide Untergruppe jeweils entsprechend viele weitere Elemente. Erneut gilt es für jede Sylow-Gruppe anzugeben: Stets gilt es das neutrale Element. Ferner gilt es die Hypothese zu bestätigen, dass alle  $n_p > 1$  sind, eine Übersicht über die Elemente der Anzahl der Sylowschen  $p$ -Untergruppen ist. In diesem Fall hilft es manchmal, für die Lieder bleiben bei anderen Gruppenordnungen meistens mehrere Möglichkeiten für die Anzahl  $n_7$  der Sylowschen 7-Untergruppen zu betrachten. Da nun die Hypothese genau eine Sylowsche 7-Untergruppe, und diese muss daher ein Normalteiler sein. An positiven Teilen gilt es nur 1, 2, 3, 4, 12. Daher muss  $n_7 = 1$  sein. Es gilt also eine Bijektion  $M \rightarrow M$ . Die Bijektion  $\text{conj}^g$  schickt eine Sylowsche 3-Untergruppe  $H$  auf  $gHg^{-1}$ .

**Aufgabe 4.** Die zweite Voraussetzung an die beiden Primzahlen ist, dass  $p$  kein Teiler von  $q - 1$  ist.

Hier ein Beispiel. Sei  $G$  eine Gruppe mit  $|G| = 84 = 2^2 \cdot 3 \cdot 7$  Elementen. Dann muss die Anzahl  $n_7$  der Sylowschen 7-Untergruppen ein Teiler von  $2^2 \cdot 3$  und modulo 7 Kongruent zu 1 sein. An positiven Teilen gilt es nur 1, 2, 3, 4, 12. Daher muss  $n_7 = 1$  sein. Es gilt

$$G \rightarrow \text{Aut}(M), \quad g \mapsto \text{conj}^g$$

Für Teilaufgabe a) hilft es vielleicht, die Abbildung

## Übungsblatt 5

**Aufgabe 1.** Ein  $i$ -Minor ist die Determinante einer (nicht notwendigerweise zusammenhängenden)  $(i \times i)$ -Untermatrix. Etwa sind die 2-Minoren der Matrix

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$$

die Zahlen  $1 \cdot 5 - 4 \cdot 2$ ,  $1 \cdot 6 - 4 \cdot 3$  und  $2 \cdot 6 - 5 \cdot 3$ . Je nach Konvention gehören die Negativen dieser Zahlen auch noch zu den 2-Minoren; für welche Konvention man sich entscheidet, spielt bei dieser Aufgabe aber keine Rolle, da es sowieso nur um den größten gemeinsamen Teiler der  $i$ -Minoren geht.

Unter den Transformationen der Vorlesung, die man benötigt, um eine Matrix in Smith-Normalform zu überführen, steht diejenige, die man benötigt, um eine Matrix in Smith-Normalform zu überführen, nämlich die  $i$ -Minoren, andererweise  $i$ -Minoren. Dieses Fakuum ist gut zu beweisen. Ein eleganter Beweis ist mit Techniken des äu ßeren Kalküls (siehe etwa die jetzige LA-I-Vorlesung möglich, andere Beweisansätze gibt es aber sicher auch).

**Aufgabe 2.** Bei beiden Teilaufgaben ist also eine Liste von abelschen Gruppen der jeweiligen Ordnung gesucht, sodass jede abelsche Gruppe dieser Ordnung isomorph zu einer der Gruppen auf der Liste ist und sodass keine zwei verschiedenen Gruppen der Liste zueinander isomorph sind. Ohne Unterstützung mit Vorlesungswissen ist die Aufgabe schwer.

**Aufgabe 3.** Die Notation in der Angabe ist etwas seltsam, hat aber einen guten Grund. Wie dem Text zu entnehmen ist, gilt

$$A[p^\infty] := \{x \in A \mid \text{ord}(x) \text{ ist eine } p\text{-Potenz}\} \subseteq A.$$

Bei der Besprechung von Blatt 5 haben wir gesehen, wie man diese Menge auch geringfügig einfacher beschreiben kann. Für Teilaufgabe b) ist ein geeigneter Isomorphismus

$$A[p_1^\infty] \times \cdots \times A[p_r^\infty] \longrightarrow A$$

zu finden (anzugeben). Auch muss nachgerechnet werden, dass die gefundene Abbildung tatsächlich ein Gruppenhomomorphismus ist und bijektiv ist.

**Aufgabe 4.** Der Ring  $\mathbb{Z}_{(p)}$  ist nicht zu verwechseln mit dem Restklassenring  $\mathbb{Z}/(p)$ . Bitte rechnet nicht alle Ringaxiome nach, sondern nur die Unterringaxiome: Die neutralen Elemente bezüglich Addition und Multiplikation müssen enthalten sein, die Summe und das Produkt zweier Elemente muss wieder enthalten sein und Negative von Elementen müssen wieder enthalten sein.

**Aufgabe 5.** Es gilt  $\mathbb{Z}[\zeta] = \{a_0 + a_1\zeta + \cdots + a_{n-1}\zeta^{n-1} \mid a_0, \dots, a_{n-1} \in \mathbb{Z}\}$ , dieser Umstand muss nicht nachgewiesen werden.

Zu Teilaufgabe b): Die Techniken des üblichen Beweises, dass  $\mathbb{Q} = \mathbb{Z}$ , lassen sich auf diesen Fall übertragen. Ein genauerer Hinweis wird noch folgen.

## Übungsblatt 6

**Aufgabe 1.** Teilaufgabe a) lautet ausformuliert wie folgt: Sei  $\varphi : R \rightarrow S$  ein Homomorphismus von Ringen. Sei  $\mathfrak{b} \subseteq S$  ein Ideal in  $S$ . Zeige, dass  $\varphi^{-1}(\mathfrak{b}) = \{x \in R \mid \varphi(x) \in \mathfrak{b}\} \subseteq R$  ein Ideal in  $R$  ist. Die Behauptung in Teilaufgabe b) (welche falsch ist) wäre, dass für ein Ideal  $\mathfrak{a} \subseteq R$  die Menge  $\varphi(\mathfrak{a}) = \{\varphi(x) \mid x \in \mathfrak{a}\} \subseteq S$  ein Ideal von  $S$  ist.

Für Teilaufgabe b) genügt ein Gegenbeispiel.

**Aufgabe 2.** Falls ihr euch wundert, welches Ideal von  $\mathbb{Z}$  nicht endlich erzeugt ist: In klassischer Logik gibt es kein solches. (Bonusaufgabe: Beweise das.)

Bitte überseht bei Teilaufgabe c) kein Ideal. Es sind insgesamt zwei Elemente erzeugt werden. Ein explizites Beispiel: Es gilt  $(12, 15) = \{12a + 15b \mid a, b \in \mathbb{Z}\} = \{6(2a + 5b) \mid a, b \in \mathbb{Z}\}$ .

**Aufgabe 3.** Die Lösung zu Teilaufgabe c) lässt sich einfacher aufschreiben, wenn man folgende Charakterisierung verwendet (welche nicht bewiesen werden muss): Ein Ring  $R$  ist genau dann der Nullring, wenn  $1 = 0 \in R$ .

Ein Beispiel für Teilaufgabe b): Für  $n = 4$  gilt  $\bigvee \{\underline{0}\} = \underline{0} \in \mathbb{Z}/(4)$ .

**Aufgabe 4.** Die Eindeutigkeit des Ringhomomorphismus muss nicht bewiesen werden. Achtet aber darauf, den Homomorphismus explizit genug anzugeben.

**Aufgabe 5.** Bonusfrage: Wie kann man sich  $S \times T$  geometrisch vorstellen, wenn man geometrische Vorstellungen von  $S$  und  $T$  kennt?

Für die Richtung a)  $\leftarrow$  b) kann man  $S = (e) \subseteq H$  setzen. Mit den Operationen von  $H$  wird das zu einem Ring, allerdings mit einem anderen Einselement.

## Übungsblatt 8

**Aufgabe 1.** „ $f = g$  in  $R[s_i^{-1}]$ “ bedeutet, dass die Brüche  $f/1$  und  $g/1$  als Elemente von  $R[s_i^{-1}]$  gleich sind. Was das wiederum bedeutet, steht bei der Definition der Lokalisierung im Skript. Bei Teilaufgabe b) ist mit „dem Bild von  $f$  in  $R[s_i^{-1}]$ “ das Element  $f/1 \in R[s_i^{-1}]$  gemeint.

tauscht man ein paar Bezeichnungen gegen ein paar allgemeine Übereinstimmungen ein.  
Alternativ kann man auch ein bestimmtes Lemma der Vorlesung zu Hilfe nehmen, dann ordne ich den Dex-Dschungelbrigden und den „L<sub>N</sub>-Trick“ der Vorlesung vorwenden. Dann kann man Definition in eicher Gleichung über  $R$  umwandeln. Dann mit „o. B. d. A.“ s etwas witzlich lösbar (erfüllen also eine entsprechende Gleichung die auf „=“ endet), das nach zugehen sind: Lokal sind Limes gegeben, die haben eine bestimme Form. Die Limesen sind Teilaufgabe b) kann man so aufpacken, indem man erstmal ausschreibt, was die Vorlesung

**Aufgabe 2.** Wenn euch die Definition des gerichteten Limes im Skript zu ungenau ist, hier eine ausführlichere Definition: Sei ein gerichtetes System  $(R_i)_{i \in I}$  von Ringen gegeben. Dieses umfasst also eine bestimmte gerichtete Menge  $I$ , für jeden Index  $i \in I$  jeweils einen Ring  $R_i$  und in der Notation unterdrückte Ringhomomorphismen  $\phi_{ij} : R_i \rightarrow R_j$  für jedes Paar  $(i, j)$  mit  $i \preceq j$ . Diese Ringhomomorphismen müssen für  $i \preceq j \preceq k$  die Gleichung

$$\phi_{jk} \circ \phi_{ij} = \phi_{ik} : R_i \rightarrow R_k$$

erfüllen. Als Menge ist dann der gerichtete Limes  $R := \varinjlim_{i \in I} R_i$  durch

$$R := \left( \coprod_{i \in I} R_i \right) / \sim$$

gegeben. Ein beliebiges Element von  $R$  hat also die Form

$$[\langle i, x \rangle],$$

wobei  $i$  ein Index aus  $I$  und  $x$  ein Element aus dem entsprechenden Ring  $R_i$  ist. Die Äquivalenzrelation ist durch die Forderung

$$\langle i, x \rangle \sim \langle j, y \rangle \iff \exists k \in I, i \preceq k, j \preceq k: \phi_{ik}(x) = \phi_{jk}(y)$$

festgelegt. Ein Element von  $R$  wird also repräsentiert durch ein Element aus einem der  $R_i$ , wobei zwei solche Elemente genau dann als äquivalent zählen, wenn ihr Bild in einem Ring  $R_k$  mit  $i, j \preceq k$  übereinstimmt. Die  $\phi$ 's stammen aus dem Datum des gerichteten Systems, von dem man den Limes nimmt.

Die Addition ist wie folgt definiert: Seien  $[\langle i, x \rangle], [\langle j, y \rangle]$  Elemente von  $R$ . Da  $I$  gerichtet ist, gibt es eine gemeinsame obere Schranke für  $i$  und  $j$ , also ein Element  $k \in I$  mit  $i \preceq k$  und  $j \preceq k$ . Die Summe der beiden Elemente ist dann als  $[\langle k, \phi_{ik}(x) + \phi_{jk}(y) \rangle]$  definiert. Man kann nachrechnen, dass dieses Ergebnis nicht von den getroffenen Wahlen (insgesamt drei Stück: den Wahlen der beiden Repräsentanten und die Wahl von  $k$ ) abhängt. (Ihr müsst das aber nicht machen, die Beweislast liegt dafür bei der Vorlesung.) Man addiert

also, indem man die Repräsentanten in einen gemeinsamen Ring überführt und dort addiert. Die Multiplikation funktioniert völlig analog.

In Teilaufgabe a) meint „ $x \in R_i$  in  $R_j$  invertierbar“, dass  $\phi_{ij}(x) \in R_j$  invertierbar ist.

*Bonusaufgabe:* Wieso ist wichtig, dass man von einer gerichteten Menge fordert, dass sie bewohnt ist (also ein Element enthält)?

Erzeugten Unterringe des vorgegebenen Rings zu betrachten.  
Für Teilaufgabe b) kann es sinnvoll sein, die Gesamtheit aller (als  $\mathbb{Z}$ -Algebra) endlich

**Aufgabe 3.** Im Skript ist ein Schema-F-Verfahren beschrieben, mit dem man Teilaufgabe c) lösen kann. Vergesst nicht, die Irreduzibilität der gefundenen Faktoren nachzuweisen. Die Kriterien aus Aufgabe 4 könnten dafür und für Teilaufgabe b) hilfreich sein.

**Aufgabe 4.** In Teilaufgabe b) lautet die Voraussetzung an  $f(X)$  wie folgt: Wenn man  $f(X) = X^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0 \in R[X]$  schreibt, so ist vorausgesetzt, dass  $\bar{f}(X) = X^n + [a_{n-1}]X^{n-1} + \dots + [a_1]X + [a_0] \in (R/I)[X]$  irreduzibel ist.

Wer sich fragt, wann die seltsame Bedingung an  $I$  erfüllt ist: Der Faktorring  $R/I$  ist genau dann ein Integritätsbereich, wenn  $I$  ein Primideal ist. Was das ist, lernen wir nächste Woche.

Für Polynome über Integritätsbereichen gilt die übliche Gaußsche Eliminationsmethode (wieso?).

**Aufgabe 5.** In Spiegelschrift folgende manche Lemmas, die hilfreich sein könnten.

Sei ein Bruch aus  $R[f]^{-1}$  gegeben. Dann kann man den Zähler im  $R$  in irreduzible Elemente zerlegen. Diese werden in  $R[f]^{-1}$  jedoch im Allgemeinen nicht irreduzibel sein: Manche werden invertierbar werden also nicht zur gesuchten Zerlegung des Bruches in irreduzible über  $R[f]^{-1}$ .

Lemma: Sei ein Element  $x \in R$  irreduzibel und kein Teiler von  $f$ . Dann ist  $x$  auch in  $R[f]^{-1}$  irreduzibel. (Wieso?)

Lemma: Ein Element  $x \in R$  ist genau dann in  $R[f]^{-1}$  invertierbar, wenn  $x$  ein Teiler einer gewissen Potenz  $f^n$ ,  $n \geq 0$ , ist. (Wieso?)

**Aufgabe 6.** Wer möchte, kann mit dieser Aufgabe mehr als 100 % der Übungspunkte erreichen oder diese interessante Aufgabe zugunsten anderer Aufgaben bearbeiten. [Es bleibt aber dabei, dass für die 1,0 nicht 100 % der Übungspunkte benötigt werden.] Es darf verwendet werden, dass sich das Ideal der  $i$ -Minoren unter Basiswechsel (d. h. unter Multiplikation mit invertierbaren Matrizen von links und von rechts) nicht ändert. Für Teilaufgabe d) folgt ein genauerer Hinweis auf Anfrage per Mail.

Matrizen  $A, B$  gleicher Dimension heißen genau dann *zueinander ähnlich*, wenn es invertierbare Matrizen  $R, S$  passender Größe mit  $B = RAS$  gibt.

Ist der zugrundeliegende Ring sogar ein Körper, so führt die Rangdefinition der Übungsaufgabe auf die bekannte Rangdefinition aus der linearen Algebra.

Eine  $(n \times m)$ -Matrix besitzt keinerlei  $i$ -Minoren für  $i > n$  und für  $i > m$ . Das Ideal, das von solchen  $i$ -Minoren erzeugt wird, ist daher das Nullideal.

Nur zur Information: Ein Beispiel für einen lokalen Ring ist  $\mathbb{Z}_{(p)}$ , wobei  $p$  eine Primzahl ist. Ferner ist jeder Körper ein lokaler Ring. Der Ring  $\mathbb{Z}$  selbst ist dagegen kein lokaler Ring. Der Ring  $K[X, Y]_{(X-a, Y-b)} := S^{-1}K[X, Y]$  mit  $S := K[X, Y] \setminus (X - a, Y - b) = \{f(X, Y) \in K[X, Y] \mid f(a, b) \neq 0\}$  ist ein geometrisch motiviertes Beispiel für einen lokalen

Ring: Seine Elemente sind *Keime* „guter Funktionen“ auf  $K^2$  – das sind Funktionen, die nur auf einer kleinen offenen Umgebung um  $(a, b)$  definiert sein müssen.

Zu Teilaufgabe b): Der Fall  $r = 0$  lässt sich kurz erledigen, wieso? Im Fall  $r = 1$  ist mindestens ein Matrixintrag invertierbar (wieso?). Diesen kann man dann mit elementaren Zeilen- und Spaltenumformungen nach oben links bringen (wieso?). Wie geht es dann weiter? Vielleicht ist folgende Allgemeine Beobachtung nützlich: Wenn das dann erzeugte Ideal das Einideal ist, so ist für alle  $j < i$  auch das von den  $j$ -Algorithmen erzeugte Ideal das Einideal ist, so ist für alle  $j < i$  auch das von den  $j$ -Algorithmen erzeugte Ideal das Einideal ist. Würde nicht, dass ihr verwerden könnt.

Bei Teilaufgabe a) lässt sich ein Beispiel über  $R = \mathbb{Z}$  finden.

## Übungsblatt 9

**Aufgabe 2.** Die erste Teilaufgabe ist so gedacht, dass man *keine* vollständigen Faktorisierungen in irreduzible Elemente bestimmt, sondern sich mit teilweisen Faktorisierungen begnügt. Für die zweite Teilaufgabe steckt im Beweis der Vorlesung, dass der Polynomring über einem ggT-Ring wieder ein ggT-Ring ist (Proposition 7.97), ein explizites Verfahren, was man hier einsetzen kann.

**Aufgabe 3.** In Teilaufgabe a) meint „ $d/c$ “ das eindeutig bestimmte Element  $v \in R$  mit  $vc = d$ . (Wieso existiert ein solches?) Allgemein heißt ein Element  $u$  genau dann *größter gemeinsamer Teiler* zweier Elemente  $x$  und  $y$ , wenn

- $u$  ein Teiler von  $x$  und von  $y$  ist und
- für jeden gemeinsamen Teiler  $\tilde{u}$  von  $x$  und  $y$  gilt, dass  $\tilde{u}$  ein Teiler von  $u$  ist.

Betrachte für Teilaufgabe b) den größten gemeinsamen Teiler von  $ac$  und  $bc$ .

**Aufgabe 4.** Die Gleichheit  $\mathcal{O}_{\mathbb{Q}(\omega)} = \mathbb{Z}[\omega]$  muss nicht nachgerechnet werden. Der so erhaltene Ring heißt auch *Ring der Eisenstein-Zahlen*.

**Aufgabe 5.** Im DigiCampus findet ihr nützliche Rechenregeln für Ideale und Ringisomorphismen.

Nur zur Information: Mit klassischer Logik lässt sich auch die Umkehrung der Aussage in Teilaufgabe a) zeigen: Ein Element, dass in allen Primidealen eines Rings enthalten ist, ist tatsächlich schon nilpotent. Wer mag, kann sich daran versuchen; in unserer Vorlesung haben wir aber nicht die nötige Technologie, um den Beweis einfach aussehen zu lassen.

## Übungsblatt 10

**Aufgabe 1.** Für Teilaufgabe a) könnte man die Beweise der Vorlesung durchgehen (die nämlich garantieren, dass das Ideal lokal ein Hauptideal ist). Das dauert aber in der Praxis recht lange. Schneller kommt man zum Ziel, wenn man versucht, durch systematisches Probieren eine geeignete Zerlegung der Eins zu finden. Beachtet, dass in einem Ring der Form  $R[f^{-1}]$  nicht nur  $f$  selbst, sondern auch alle Teiler von  $f$  invertierbar sind. Für Teilaufgabe b) gibt es in der Vorlesung ein Schema-F-Verfahren (Seite 327). Das sieht auf

den ersten Blick länglich und umständlich aus, wird bei dieser Aufgabe aber schon nach dem ersten Schritt terminieren.

Zwischenrechnungen bei Teilaufgabe b), zur Kontrolle: Sei  $a = (14, x+7)$  und  $b = (35, x-14)$ . Dann kann man mit Hilfe der Rechenregeln für Ideale (siehe DigiCampus) sehen, dass für die Summe dieser beiden Ideale gilt:  $\mathfrak{d} = a+b = (x)$ . Danach sieht die Quotienten  $\mathfrak{d} : a = \mathfrak{d} : b = b$  zu bestimmen. Wenn man den Tipp im vorhergehenden Absatz befolgt, kann man diese Beziehung durchführen; man erhält  $\mathfrak{d} = (2, x - x^3)$ . Wenn wir andere Zwischenrechnitte zur Idealrechenfachung tätigen, sieht einer Ergebnis vielleicht anders aus, das wäre also kein Grund zur Beunruhigung. Noch eine allgemeine Bemerkung: Es gilt  $a : b = a : (a + b)$ , für beliebige Ideale  $a, b$ .

Manche Idealdivisionen lassen sich einfach durchführen: In jedem Brüg gilt die Regel  $(x \cdot a_1, \dots, x \cdot a_n) : (x) = (a_1, \dots, a_n)$ , falls  $x$  ein reguläres Element ist (wieso?). Wenn man das Verfahren der Vorfaktoren anwendet, kann man also versuchen, die als Divisoren auftretenden Ideale so zusammenzuschreiben, dass ihre Erzeuger jeweils Vielfache des Dividenden sind. Dabei ist die Rechenregel  $\mathfrak{d} = x \cdot (3 + x - x^3)$  nützlich (wieso gilt dies Divisionssätze sind). Dabei ist die Rechenregel  $\mathfrak{d} = x \cdot (3 + x - x^3)$  nützlich (wieso gilt aufgetrennen Ideale so zusammenzuschreiben, dass ihre Erzeuger jeweils Vielfache des Dividenden Divisoren auftretenden Ideale zu Hauptidealen zu vereinfachen und die als Divisoren auftretenden Ideale so zusammenzuschreiben, dass ihre Erzeuger jeweils Vielfache des Dividenden Ideale ist (wieso?).

**Aufgabe 2.** In einer ersten Version des Übungsblatts fehlte die wichtige Voraussetzung, dass auch schon bei Teilaufgabe a) der Ring als prüfersch und das irreduzible Ideal als endlich erzeugt angenommen werden kann. Entschuldigung dafür!

Für  $u := 1 + \sqrt{-13}$  gilt  $u \cdot u = 1 + 13 = 14$ . Je nachdem, wie man in Teilaufgabe a) herangeht, kann diese Beziehung helfen oder nicht helfen. Eindeutig ist die Beziehung  $u \cdot u = 1 + \sqrt{-13}$  für  $u = 1 + \sqrt{-13}$ . Hierfür und für den Rest der Teilaufgabe ist das Stichwort irreduzible muss sein:  $\mathfrak{p} = \mathfrak{q}$ . Hierfür und für den Rest der Teilaufgabe ist das Stichwort irreduzible und enthält  $\mathfrak{p}$  ein reguläres Element (das bedeutet, dass  $\mathfrak{p}$  nicht das Nullideal ist). Dann ist  $\mathfrak{p} \in \mathfrak{q}$  (siehe): Seien  $\mathfrak{p}, \mathfrak{q}$  endlich erzeugte Primideale in einem prüferschen Bereich. Geleite  $\mathfrak{p} \subset \mathfrak{q}$  aus. Für Teilaufgabe b) ist folgendes Lemma nützlich (was für volle Punktzahl bewiesen werden kann):

$$\mathfrak{a} : (x + y) = \mathfrak{a} : (xy) = \mathfrak{a} : (x) = \mathfrak{a} : (y).$$

Für Teilaufgabe a): Welche wichtige Rechenoperation mit Idealen funktioniert im Allgemeinen nur in prüferschen Bereichen gut? Vergesst bitte nicht, beide Primidealaxiome (sehr sinnvolle) Konventionen im Hinterkopf behalten: Das leere Produkt von Idealen ist Um zu zeigen, dass ein irreduzibles Ideal nicht das Einideal sein kann, muss man folgende nachzuweisen. Um zu zeigen, dass ein irreduzibles Ideal nicht das Einideal sein kann, hilft es, einen der folgenden Idealquotienten zu betrachten:

**Aufgabe 3.** Exemplarisch wollen wir genauer verstehen, was der Test in Teilaufgabe a) bewerkstelligen kann: Diesem Test kann man ein beliebiges nicht verschwindendes endlich erzeugte Ideal geben. Sollte das Ideal irreduzibel sein, meldet das der Test. Sollte das Ideal nicht irreduzibel sein, gibt es zwei Möglichkeiten: Es könnte das Einideal sein, oder es könnte nicht das Einideal sein. Der Test meldet dann, welcher dieser beiden Fälle eingetreten ist. Im zweiten Fall gibt er außerdem zwei Faktoren (wiederum endlich erzeugte Ideale) an, die miteinander multipliziert das getestete Ideal ergeben. Diese Faktoren sind *echt*, also jeweils nicht das Einideal.

Diese Aufgabe ist recht interessant. Eine der Hauptschwierigkeiten liegt darin, zu zeigen, dass das von euch erfundene Verfahren *terminiert*, also nach endlich vielen Schritten

endet. Bitte zögert nicht, mir ggf. Fragen zu schicken. Insbesondere kann ich euch zeigen, wie man eines der in Spiegelschrift vorgeschlagenen Hilfsverfahren konstruiert.

Ein endlich erzeugtes Ideal heißt genau dann *nicht verschwindend*, wenn es nicht das Nullideal ist. In Integritätsbereichen ist das gleichbedeutend damit, dass es ein reguläres Element enthält (wieso?).

Wozu helfen diese Hilfsverfahren?  
 Ist, oder sonst ein endlich erzeugtes maximales Ideal findet, was das gegebene umfasst.  
 Einem gegebenen nicht verschwindenden endlich erzeugten Ideal feststellt, ob es maximal ist, oder sonst ein endlich erzeugtes irreduzibles Ideal findet, was das gegebene umfasst. Für Teilaufgabe b) kann es analog hilfreich sein, erst ein Verfahren zu entwickeln, was von gegebenen nicht verschwindenden endlich erzeugten Idealen feststellt, ob es das Einseidel ist.  
 Für Teilaufgabe a) kann es hilfreich sein, zuerst ein Verfahren zu entwickeln, was von einem

#### Aufgabe 4. Induktion über $m$ .

Im Induktionssschritt  $m \rightarrow m+1$  kann man eine aufsteigende Folge  $i_0, i_1, i_2, \dots$  von Indizes finden, sodass für alle  $n \geq 0$  und  $j \in \{1, \dots, m\}$  gilt:  $a_{j, i_n} = a_{j, i_{n+1}}$ . Wie funktioniert das genau? Was hilft einem das?

**Aufgabe 5.** Umfangreiche Erklärungen mit einem Musterbeispiel finden sich in einem separaten Dokument im Dicampus. Wenn man nach diesem Dokument vorgeht, muss man zum Schluss eine große Tabelle anlegen; das macht per Hand keinen Spaß. Besser ist es, wenn man sich entweder durch viel Denken Rechenarbeit abnimmt (mühsam!) oder sich eines Computers bedient (empfohlen!). Man muss das Verfahren nicht bis zum Ende durchziehen, um viele Punkte zu erzielen.

Wer sich für den zahlentheoretischen Hintergrund interessiert, findet eine allgemeine Diskussion von reinen kubischen Erweiterungen in einer Notiz von Ian Kiming: [http://www.math.ku.dk/~keming/lecture\\_notes/2003-2004-algebraic\\_number\\_theory\\_koch/pure\\_cubic\\_fields.pdf](http://www.math.ku.dk/~keming/lecture_notes/2003-2004-algebraic_number_theory_koch/pure_cubic_fields.pdf)

$$X^3 - \frac{a}{36}X^2 + \frac{-4bc + a^2}{16c^3 + 12abc - 4b^3 - a^3}X + \frac{3888}{1259712}.$$

Zur Kontrolle: Man erhält Minimalpolynoms (und das tatsächliche Minimalpolynom benötigt man hier gar nicht). Abbildung  $z \mapsto zx$  auf. Deren charakteristisches Polynom ist dann das Minimalpolynom bestimmen. Das kann man mit dem Verfahren aus Algebra I, Blatt 3, Aufgabe 2 machen: Man stellt bezüglich der  $\mathbb{Q}$ -Basis  $(1, a, a^2)$  von  $\mathbb{Q}(a)$  die Darstellungsmatrix zur linearen

$$x = \frac{108}{1}(a + ba + ca^2)$$

Vieleicht muss man das Minimalpolynom einer Zahl der Form Diskriminante der dann erhaltenen Basis ist  $-108$ . Die  $\mathbb{Q}$ -Basis muss man das letzte Basiselement geeignet ersezten. Zur Kontrolle: Die dichtige Basis muss man das letzte Basiselement geeignet ersezten. Zur Kontrolle: Die  $\mathbb{Q}(a)$ -Basis  $(1, a, a^2)$  von  $\mathbb{Q}(a)$ , wobei  $a = \sqrt[3]{4}$ , ist noch keine Ganzheitsbasis. Für eine

## Übungsblatt 11

**Aufgabe 1.** Diese Aufgabe ist eine typische Staatsexamensaufgabe. Die „S“-Markierung hätte aber das Layout gestört.

**Aufgabe 2.** Gibt es Polynome, die keine Nullstellen besitzen, und trotzdem reduzibel ist?

**Aufgabe 3.** Hinweise in Spiegelschrift.

- Weise stattdessen die Irreduzibilität in  $K[X][Y]$  nach. Was ist damit gemeint? (Dieses Element von  $K(y)[X]$  nachgewiesen werden.)
- Argumentiere, dass es genügt, die Irreduzibilität des angeblichen Minimalpolynoms als Element von  $K[y][X]$  nachzuweisen. (Eigentlich muss ja die Irreduzibilität als Koeffizienten vor den  $X$ -Eins ist. Für diesen Schritt gibt es Bonuspunkte.)
- Zeige, dass das im ersten Schritt gefundene Polynom als Polynom über  $K[y]$  (im teilkörper von  $K[Y]$  gleich  $K(Y)$ ). Aber das ist nicht die Aussage, die da steht.)
- Der Quotientenkörper von  $K[y]$  ist  $K(y)$ . (Direkt nach Definition ist der Quotientenring ist ein Unterring von  $K(X)$  und enthält alle in  $y$  polynomießen Ausdrücke, es gibt keine Polynomgleichung vom Grad 1 oder höher, die  $y$  als Lösung und Unbestimmte  $X$  ist überhaupt nicht dasselbe wie  $y$ .)
- Wegen dieser Transzendenz ist der Ring  $K[y]$  kanonisch isomorph zu  $K[Y]$ . (Der zweite Ring ist der Rest der Polynomgleichungen in  $y$ , der Rest der Ausdrücke mit  $y$  zu tun. Es ist etwas Konzentration erforderlich, um bei den vielen Variablenamen nicht durchmischen zu kommen. Im Rest der Aufgabe geht es darum, die Irreduzibilität dieses Polynoms nachzuweisen.)
- Unter den gegebenen Voraussetzungen ist  $y \in K(X)$  transzendent über  $K$ , d.h. es gibt keine Polynomgleichung vom Grad 1 oder höher, die  $y$  als Lösung und Koeffizienten aus  $K$  hat.
- Wegen dieser Transzendenz ist der Körper  $K(y)$  kanonisch isomorph zu  $K[Y]$ . (Der erste Ring ist der Rest der Polynomgleichungen in  $y$ , der Rest der Ausdrücke geht es darum, die Irreduzibilität dieses Polynoms nachzuweisen.)
- Der zweite Ring ist der Rest der Polynomgleichungen in  $y$ , der Rest der Ausdrücke geht es darum, die Irreduzibilität dieses Polynoms nachzuweisen.)
- Zeige, dass das im ersten Schritt gefundene Polynom als Polynom über  $K$  irreduzibel ist. Für diesen Schritt gibt es Bonuspunkte.

**Aufgabe 5.** Detaillierte Erklärungen findet ihr in einem separaten Blatt zur Kronecker-Konstruktion im Digicampus.

## Blatt 12

**Aufgabe 3.** Ein Polynom  $f$  ist genau dann separabel, wenn Eins ein größter gemeinsamer Teiler von  $f$  und seiner formalen Ableitung  $f'$  ist.

In Algebra I wurde bewiesen, dass jedes irreduzible Polynom über  $\mathbb{Q}$  schon separabel ist. Den damaligen Beweis kann man in Teilaufgabe a) imitieren.

**Aufgabe 4.** In Teilaufgabe a) müsst ihr nicht nachrechnen, dass  $L$  überhaupt ein Ring ist – diese Verpflichtung lag bei der Vorlesung. Bitte vergesst aber nicht den zweiten Teil der

Körperbedingung – ein Ring heißt genau dann Körper, wenn jedes Element *entweder* Null oder invertierbar ist; das *entweder* ist wichtig! (Wieso?) In Teilaufgabe b) ist für jedes  $i \in I$  ein Ringhomomorphismus  $K_i \rightarrow L$  zu finden. Der sollte kanonisch sein, ihr solltet also nicht willkürliche Wahlen treffen, um ihn anzugeben. Dass eure Abbildung wirklich ein Homo ist, müsst ihr nicht nachweisen; sollte aber ein Wohldefiniertheitsnachweis erforderlich sein, wäre der wichtig.

**Aufgabe 5.** Ein Körper  $K$  heißt genau dann *vollkommen*, wenn jedes normierte Polynom über  $K$  ein Produkt separabler Polynome ist. Mehr muss man über Vollkommenheit nicht wissen, um diese Aufgabe zu bearbeiten. Bei Teilaufgabe b) ist kein explizites Gegenbeispiel nötig. Es genügt eine Argumentation, wieso die eine Richtung eures Beweises aus a) noch funktioniert und die andere nicht.

## Blatt 13

**Aufgabe 1.** Bei Teilaufgabe a) ist zu einem beliebigen Element aus  $E$  eine  $p$ -te Wurzel anzugeben (zusammen mit einem Beweis, dass es sich dabei wirklich um eine  $p$ -te Wurzel handelt).

Bei Teilaufgabe b) ist zu zeigen:  $E$  ist ein Körper und die angegebene Abbildung ist ein Ringhomomorphismus. Wieso genügt das?

**Aufgabe 2.** Bei Teilaufgabe a) ist zu zeigen:

- Der Primkörper von  $K$  ist überhaupt ein Unterkörper von  $K$ .
- Ist  $U$  irgendein Unterkörper von  $K$ , so ist  $U$  ein Oberkörper des Primkörpers.

„Kleinste“ bezieht sich also nicht auf die Anzahl der Elemente, sondern auf die Inklusionsbeziehung.

## Blatt 14

**Aufgabe 1.** Wenn ihr wollt, dürft ihr bei den Teilaufgaben b) und c) voraussetzen, dass  $L$  endlich über  $K$  ist. Dann gibt es weitere Beweismöglichkeiten (die aber etwa gleich schwer sind wie ohne die Zusatzvoraussetzung).

**Aufgabe 2.** Mit  $N_{L/K}(x)$  ist die *Norm* des Elements  $x \in L$  über  $K$  gemeint. Sie ist definiert als die Determinante der  $K$ -linearen Abbildung

$$L \longrightarrow L, z \mapsto zx.$$

beide gleich  $f(X)$  sind.

$$\begin{pmatrix} 0 & 0 & \cdots & 1 & -c_{n-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 1 & \cdots & 0 & -c_2 \\ 1 & 0 & \cdots & 0 & -c_1 \\ 0 & 0 & \cdots & 0 & -c_0 \end{pmatrix} \in K^{n \times n}, \quad B(f) =$$

eines normierten Polynoms  $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ , das ist die Matrix  
Nämlich, dass Nullmalpolynom und charakteristisches Polynom der sog. Begleitmatrix:  
die etwas mit  $x$  zu tun hat) und sich an ein Faktum der Linearen Algebra zu erinnern:  
zurück. Für diesen Fall ist natürlich, eine geeignete Basis von  $L$  über  $K$  zu wählen (eine,  
Führe den Fall eines beliebigen Elements  $x$  auf den Fall einer separablen Elementen  $x$

### Aufgabe 3. Hinweise in Spiegelschrift.

der Algebra I über Körpererweiterungen behält auch über allgemeinen Körpern Gültigkeit.  
primiven Elementen verwenden? Wie kann man stattdessen vorgehen? Das Hinweisblatt  
nicht weiter? (Wieso kann man also die Verfahren zur Bestimmung eines  
Wieso hilft hier der Beweis des Satzes über das primitive Element überhaupt

**Aufgabe 4.** Manche Beweise des Kapitels über Transzendenzbasen haben vielleicht an ähnliche Beweise aus der Linearen Algebra erinnert. Das ist kein Zufall: Hinter beiden Situationen steckt ein tieferes Konzept, das der sog. *Spannoperation*. In dieser Aufgabe wollen wir zwei Beispiele für Spannoperationen kennenlernen. Auf dem nächsten Blatt werden wir dann sehen, dass man sich mit dem Konzept der Spannoperation manche Beweise der Vorlesung und manche Beweise der Linearen Algebra hätte sparen können.

Eine *Spannoperation* auf einer Menge  $S$  ist eine Vorschrift, die jeder endlichen Teilmenge  $I \subseteq S$  eine gewisse Teilmenge  $\langle I \rangle \subseteq S$  (nicht unbedingt endlich) zuordnet. Dabei müssen folgende vier Axiome erfüllt sein (für alle endlichen Teilmengen  $I, J \subseteq S$  und Elemente  $x, y \in S$ ):

1.  $I \subseteq J \implies \langle I \rangle \subseteq \langle J \rangle$ .
2.  $I \subseteq \langle I \rangle$ .
3.  $I \subseteq \langle J \rangle \implies \langle I \rangle \subseteq \langle J \rangle$ .
4.  $x \in \langle I \cup \{y\} \rangle \implies x \in \langle I \rangle$  oder  $y \in \langle I \cup \{x\} \rangle$ .

Spannoperationen sind nicht nur in der Algebra, sondern auch in der Kombinatorik wichtig. Verallgemeinerungen von Spannoperationen sind sog. *Monaden*, welche überall in der Mathematik vorkommen.