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 $i \in \{1, \ldots, n\}$ 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 ± 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 kategorielle Beschreibung des halbdirekten Produkts? (So, wie man das direkte Produkt auch als terminales Objekt in der Kategorie der Möchtegern-Produkte beschreiben kann.)

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

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

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) nützlich.

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 anderem Thema soll den Unterschied verdeutlichen: Unter den Mengen

$$\emptyset, \quad \{a\}, \quad \{a,b\}, \quad \{a,b,c\}, \quad \{d\}, \quad \{d,e\}, \quad \{d,f\}$$

gibt es keine größte, aber drei maximale: Nämlich $\{a,b,c\}$, $\{d,e\}$ und $\{d,f\}$. Ferner gibt es eine kleinste (nämlich $\emptyset$). 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 einzige Menge, die maximal ist. Außerdem ist sie die größte. Für eine der Richtungen 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 Überlappungsfrage: Eine Untergruppe mit $2^2 \cdot 3^5$ Elementen kann nur im Identitätselement mit einer Untergruppe von $7^2 \cdot 11^3$ überlappen (wieso?). Eine Untergruppe mit $2^2 \cdot 3^5$ Elementen kann mit einer Untergruppe von $3^2 \cdot 11^3$ Elementen in höchstens 3^2 Elementen überlappen (wieso?).

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

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.

Für Teilaufgabe b) kann man das Verfahren aus der Vorlesung (mit Zeilen- und Spaltentransformationen) oder Teilaufgabe a) verwenden.

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

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

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

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

Übungsblatt 6

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

Jedes endlich erzeugte Ideal von $\mathbb{Z}$ ist sogar ein Hauptideal, kann also von einem einzigen Element erzeugt werden. Ein explizites Beispiel: Es gilt $(12, 15) = \{12a + 15b \mid a, b \in \mathbb{Z}\} = (3)$.

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 $\sqrt{(0)} = (2) \subseteq \mathbb{Z}/(4)$.

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 $S = (e) \subseteq R$ setzen. Mit den Operationen von R 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.

Teilaufgabe b) kann man so anpacken, indem man erstmal ausschreibt, was die Voraussetzungen sind: Lokal sind Inverse geben, die haben eine bestimmte Form. Die Inversen sind wirklich Inverse (erfüllen also eine entsprechende Gleichung die auf „= 1" endet), das nach kann man Definition in einer Gleichung über R umwandeln. Dann mit „o. B. d. A."s etwas Ordnung in den Index-Dschungel bringen und den „1_N"-Trick der Vorlesung verwenden. Alternativ kann man auch ein bestimmtes Lemma der Vorlesung zu Hilfe nehmen, dann tauscht man ein paar Rechnungen gegen ein paar allgemeine Überlegungen ein.

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 $\phi_{ij} : R_i \to R_j$ für jedes Paar (i, j) mit $i \preceq j$. Diese Ringhomomorphismen müssen für $i \preceq j \preceq k$ die Gleichung

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

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

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

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

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

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 ϕ'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 Schanke 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 $[\langle k, \phi_{ik}(x) + \phi_{jk}(x) \rangle]$ 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 Repräsanten 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)?

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

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 $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in R[X]$ schreibt, so ist vorausgesetzt, dass $\overline{f}(X) = X^n + [a_{n-1}]X^{n-1} + \cdots + [a_1]X + [a_0] \in (R/I)[X]$ 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 Gradformel (wieso?).

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

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?)

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

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

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.

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?)

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.