Lösungen für die Klausur zur Vorlesung

Einführung in Algebra und Zahlentheorie

Aufgabe 1 (5 Punkte)
Sei $\mathbb{Z}[\sqrt{2}]$ der kleinste Teilring von $\mathbb{R}$, der $\mathbb{Z}$ und $\sqrt{2}$ enthält. Zeigen Sie:

a) $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$.

b) $a+b\sqrt{2}$ ist genau dann in $\mathbb{Z}[\sqrt{2}]^\times$, wenn $a^2-2b^2 \in \{\pm 1\}$. Bestimmen Sie das Inverse von $7 + 5\sqrt{2}$.
(*Hinweis:* Zeigen Sie, dass die Abbildung $N : (\mathbb{Z}[\sqrt{2}], \cdot) \to (\mathbb{Z}, \cdot)$, $a+b\sqrt{2} \mapsto a^2-2b^2$ ein Monoid-Homomorphismus ist.)

c) Zeigen Sie, dass es unendlich viele Einheiten in $\mathbb{Z}[\sqrt{2}]$ gibt.

Lösung.

a) Es ist klar, dass $\{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ in $\mathbb{Z}[\sqrt{2}]$ enthalten sein muss. Umgekehrt ist diese Menge ein Teilring von $\mathbb{R}$, denn 1 liegt darin, sie ist unter Addition und Subtraktion abgeschlossen (klar) und auch unter Multiplikation, denn

$$(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}.$$

b) Es ist $a^2 - 2b^2 = (a+b\sqrt{2})(a-b\sqrt{2})$, und daher $a+b\sqrt{2}$ im Fall $N(a+b\sqrt{2}) = \pm 1$ invertierbar mit Inversem $\pm(a - b\sqrt{2})$.

Für 2 Elemente $x = a + b\sqrt{2}$ und $y = c + d\sqrt{2}$ ist

$$\begin{aligned} N(xy) &= N((ac + 2bd) + (ad + bc)\sqrt{2}) = (ac + 2bd)^2 - 2(ad + bc)^2 \\ &= a^2c^2 + 4abcd + 4b^2d^2 - 2a^2d^2 - 4abcd - 2b^2c^2 \\ &= (a^2 - 2b^2)(c^2 - 2d^2) = N(x)N(y). \end{aligned}$$

Ist nun x invertierbar mit Inversem y, so gilt

$$1 = N(1) = N(xy) = N(x)N(y),$$

also ist die ganze Zahl $N(x)$ invertierbar und daher ± 1.

Es ist klar, dass die Inverse von $7 + 5\sqrt{2}$ daher $-7 + 5\sqrt{2}$ ist.

c) In $\mathbb{Z}[\sqrt{2}]$ liegt wegen b) die Einheit $u = 7 + 5\sqrt{2}$. Diese reelle Zahl ist nicht ± 1, da $\sqrt{2}$ irrational ist. Daher ist die Ordnung von u nicht endlich. Also enthält $\mathbb{Z}[\sqrt{2}]^\times$ die unendliche Untergruppe $\langle u \rangle$.

Aufgabe 2 (5 Punkte)
Sei $a > 2$ eine natürliche Zahl, so dass $p = a^2 + 1$ prim ist.

a) Zeigen Sie, dass a gerade ist und bei Teilen durch 5 Rest 0, 1 oder 4 lässt.

b) Finden Sie eine analoge Bedingung an die Restklasse von a modulo 13, die erfüllt sein muss.
Gibt es eine solche Bedingung auch modulo 11?

c) Geben Sie drei mögliche Werte für a an.

Lösung.

a) Wäre a ungerade, so wäre $a^2 + 1$ gerade und – da $a > 2$ – selbst nicht 2, also keine Primzahl.

Wäre a modulo 5 zu 2 oder 3 kongruent, so wäre a^2 kongruent zu -1 modulo 5 und damit $a^2 + 1$ durch 5 teilbar. Da jedoch $a > 2$ gilt, ist $a^2 + 1 > 5$ und daher als Primzahl nicht durch 5 teilbar.

b) Modulo 13 hat -1 zwei Quadratwurzeln, nämlich 5 und 8. Daher darf a modulo 13 nicht kongruent 5 oder 8 sein, da sonst $a^2 + 1$ durch 13 teilbar wäre.

NB: Wegen $a > 2$ ist nach a) sogar $a \geq 4$ und damit $a^2 + 1 > 13$.

Modulo 11 gibt es so eine Einschränkung nicht, da modulo 11 keine Quadratwurzel von -1 existiert, denn 11 ist kongruent zu 3 modulo 4.

c) Die Zahlen $a = 4,\ 6,\ 10$ sind drei mögliche Werte, da

$$17 = 4^2 + 1,\ 37 = 6^2 + 1 \text{ und } 101 = 10^2 + 1$$

allesamt Primzahlen sind.

Aufgabe 3 (5 Punkte)
Sei G eine Gruppe und $Z(G) = \{g \in G : gh = hg \text{ für alle } h \in G\}$ ihr Zentrum. Sei weiterhin p eine Primzahl.

a) Zeigen Sie, dass $Z(G)$ ein Normalteiler von G ist.

b) Sei $\#G = p^r, r \geq 1$. Zeigen Sie, dass dann $Z(G) \neq \{e_G\}$ ist.

c) Folgern Sie, dass jede Gruppe der Ordnung p^2 abelsch ist.

Lösung.

a) Für $z_1, z_2 \in Z(G)$ gilt:

$$\forall h \in G : hz_1z_2^{-1} = z_1hz_2^{-1} = z_1z_2^{-1}z_2hz_2^{-1} = z_1z_2^{-1}hz_2z_2^{-1} = z_1z_2^{-1}h.$$

Da $Z(G)$ sicher das neutrale Element enthält, ist es also eine Untergruppe von G. Außerdem ist

$$\forall h \in G : hZ(G) = \{hz \mid z \in Z(G)\} = \{zh \mid z \in Z(G)\} = Z(G)h,$$

was die Normalität von $Z(G)$ in G bedeutet.

b) Die Gruppe G operiert durch Konjugation auf sich selbst, und das Zentrum ist gerade die Menge aller Fixpunkte dieser Operation. Nach der Bahnbilanzformel hat jede Bahn als Ordnung eine p-Potenz. Die Anzahl der Fixpunkte ist daher die Gruppenordnung minus einer Summe von p-Potenzen, die jede für sich durch p teilbar ist.

Damit ist auch die Anzahl der Fixpunkte durch p teilbar, $Z(G)$ also nicht trivial.

c) Sei G eine Gruppe mit p^2 Elementen, p eine Primzahl.

Wäre G nicht kommutativ, so wäre das Zentrum nicht ganz G aber trotzdem – wegen b) – nicht trivial, also eine Gruppe der Ordnung p. Damit wäre $Z(G)$ zyklisch und von einem Element z erzeugt. Dies stimmte dann auch für die Faktorgruppe $G/Z(G)$ mit einem Erzeuger γ. Es sei $g \in G$ ein Vertreter von γ. Dann sind die Elemente von G gerade die Produkte

$$z^a g^b,\ 1 \leq a, b \leq p,$$

denn diese Menge enthält ein Vertretersystem von $G/Z(G)$ und den ganzen Kern der kanonischen Projektion. Also wird G von z und g erzeugt, die jedoch wegen $z \in Z(G)$ miteinander kommutieren. G ist also kommutativ, was der Annahme widerspricht, G sei nicht komutativ.

Aufgabe 4 (5 Punkte)
Sei p eine Primzahl, $G = S_p$.

a) Wieviele Elemente der Ordnung p und wieviele p-Sylowgruppen gibt es in G?

b) Sei P eine p-Sylowgruppe und $N := \{g \in G : gPg^{-1} = P\}$ ihr Normalisator. Bestimme $\#N$.

c) Zeigen Sie, dass es in G keine Untergruppe mit $p(3p-1)$ Elementen gibt.

Lösung.

a) Ein Element der Ordnung p ist zwangsläufig ein p-Zykel, also von der Gestalt $(1\ a_2\ a_3\ \ldots\ a_p)$, wobei $i \mapsto a_i$ eine beliebige Permutation von $\{2, \ldots, p\}$ ist. Es gibt demnach $(p-1)!$ Elemente der Ordnung p.

Eine p-Sylowgruppe ist eine Untergruppe von S_p mit p Elementen, da $\mathrm{v}_p(p!) = 1$. Jede solche Gruppe wird also von einem Element der Ordnung p erzeugt, und je $p-1$ Elemente der Ordnung p liegen in einer gegebenen p-Sylowgruppe. Von diesen gibt es demnach $(p-1)!/(p-1) = (p-2)!$ Stück.

b) Da nach den Sätzen von Sylow die Gruppe G transitiv auf der Menge aller p-Sylowgruppen operiert, ist – nach der Bahnbilanzformel – der Index des Normalisators N von P gleich der Anzahl der p-Sylowgruppen, also $(p-2)!$. Daher hat N genau $p!/(p-2)!$ Elemente, also $p(p-1)$.

c) Wenn es in G ein Untergruppe U mit $p(3p-1)$ Elementen gäbe, so enthielte sie eine p-Sylowgruppe von G. Die Anzahl der p-Sylowgruppen in U wäre nach den Sylowsätzen ein Teiler von $3p-1$ und modulo p kongruent zu 1. Demnach müsste sie 1, $p+1$ oder $2p+1$ sein.

Im letzten Fall gilt offensichtlich $2p+1 = 3p-1$, da $2(2p+1) > 3p-1$. Es folgt $p = 2$, und $U \leq S_2$ müsste 10 Elemente haben, was nicht geht.

Im vorletzten Fall müsste aus ähnlichen Gründen $2(p+1) = 3p-1$ gelten (sonst wäre $p = 1$), also $p = 3$. Dann hat aber S_3 eine Untergruppe mit 24 Elementen, was auch absurd ist.

Es verbleibt der Fall, dass die p-Sylowgruppe in U normal ist. Dann ist aber U im Normalisator einer p-Sylowgruppe enthalten und damit ist $p(3p-1)$ ein Teiler von $p(p-1)$, was impliziert, dass $3p-1$ ein Teiler von $p-1$ ist. Das geht natürlich nicht, da $3p-1 > p-1$.

Folglich sind alle drei Fälle zum Widerspruch geführt, es kann keine Untergruppe mit $3p-1$ Elementen in $G = S_p$ geben.

Aufgabe 5 (4 Punkte)
Gegeben seien $A = \begin{pmatrix} 2 & 4 & 6 \\ 3 & 1 & 1 \\ 1 & 2 & 0 \end{pmatrix} \in \mathbb{Z}^{3\times 3}$, $b = \begin{pmatrix} -2 \\ 1 \\ -7 \end{pmatrix} \in \mathbb{Z}^3$.

a) Bestimmen Sie unimodulare Matrizen S, T, so dass SAT in Elementarteilernormalform vorliegt. Geben Sie die Elementarteiler an.

b) Lösen Sie mit Hilfe der Elementarteilernormalform das ganzzahlige lineare Gleichungssystem $Ax = b$.

Lösung.
a) Die Determinante von A ist 30, also quadratfrei, und daher sind die Elementarteiler $e_1 = 1,\ e_2 = 1,\ e_3 = 30$, denn $e_1 \mid e_2 \mid e_3$ und $e_1 \cdot e_2 \cdot e_3 = 30$.
Dies lässt sich auch durch elementare Spalten- und Zeilentransformationen einsehen. Zieht man zum Beispiel erst das Dreifache der dritten Zeile von der zweiten und das Doppelte von der ersten ab, vertauscht dann erste und dritte Zeile und zieht anschließend das 6-fache der zweiten Zeile von der dritten ab, so ist das die Multiplikation mit

$$S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -6 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & -2 \\ 0 & 1 & -3 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & -3 \\ 1 & -6 & 16 \end{pmatrix}$$

von links. Es ist dann

$$SA = \begin{pmatrix} 1 & 2 & 0 \\ 0 & -5 & 1 \\ 0 & 30 & 0 \end{pmatrix}.$$

Addiert man jetzt das 5-fache der dritten Spalte zur zweiten, vertauscht diese beiden Spalten und zieht dann noch das Doppelte der ersten Spalte von der dritten ab, so ist dies die Rechtsmultiplikation mit

$$T = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 5 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & -2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & -2 \\ 0 & 0 & 1 \\ 0 & 1 & 5 \end{pmatrix}.$$

Es ergibt sich

$$SAT = \operatorname{diag}(1, 1, 30).$$

b) Wir sehen

$$Ax = b \iff SATT^{-1}x = Sb,$$

das heißt

$$T^{-1}x = \operatorname{diag}(1, 1, 30)^{-1} \cdot Sb = \operatorname{diag}(1, 1, 30)^{-1} \begin{pmatrix} -7 \\ 22 \\ -120 \end{pmatrix},$$

also

$$x = T \cdot \begin{pmatrix} -7 \\ 22 \\ -4 \end{pmatrix} = \begin{pmatrix} 1 \\ -4 \\ 2 \end{pmatrix}.$$

Aufgabe 6 (4 Punkte)

a) Bestimmen Sie $\overline{44}^{-1}$ in $\mathbb{Z}/79\mathbb{Z}$ mit Hilfe des euklidischen Algorithmus.

b) Finden Sie anschließend alle ganzzahligen Lösungen des folgenden Systems simultaner Kongruenzen:
$x \equiv 2 \pmod 4$
$x \equiv 5 \pmod{11}$
$x \equiv 12 \pmod{79}$

Lösung.
a) Es ist

$$79 - 44 = 35, \quad 44 - 35 = 9, \quad 4 \cdot 9 - 35 = 1,$$

also

$$1 = 4 \cdot 44 - 5 \cdot 35 = 9 \cdot 44 - 5 \cdot 79,$$

und damit die Klasse von 9 modulo 79 zu 44 invers.

b) Wir setzen an:

$$x = 4n + 2 \equiv 5 \bmod 11.$$

Wegen $3 \cdot 4 \equiv 1 \pmod{11}$ folgt daraus

$$n \equiv 9 \pmod{11}, \quad \text{sagen wir : } \quad n = 11m + 9,$$

das macht zusammen

$$x = 44m + 38.$$

Als nächste Kongruenzbedingung haben wir noch

$$44m + 38 \equiv 12 \pmod{79},$$

und hier hilft wegen a) die Multiplikation mit 9. Es folgt

$$m \equiv 9 \cdot (-26) = -234 \equiv 3 \pmod{79},$$

und wenn wir also

$$m = 79l + 3$$

setzen, so ergibt sich

$$x = 170 + 3476 \cdot l,$$

wobei nun endlich $l \in \mathbb{Z}$ beliebig ist.

Aufgabe 7 (3 Punkte)

a) Zitieren Sie das quadratische Reziprozitätsgesetz und die beiden zugehörigen Ergänzungssätze.

b) Berechnen Sie das Legendre-Symbol $\left(\frac{514}{557}\right)$.

Dass 557 und 257 Primzahlen sind, können Sie hierbei ohne Nachweis verwenden.

Lösung.
a) Für zwei verschiedene ungerade Primzahlen p, q gilt für das Legendresymbol $\left(\frac{\cdot}{\cdot}\right)$ die Regel

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{q}{p}\right).$$

Weiter gelten für eine ungerade Primzahl p die Formeln

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

und

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Letzteres ist 1 genau dann, wenn p modulo 8 zu 1 oder -1 kongruent ist.

b) Es ist $514 = 2 \cdot 257$, und wegen der Multiplikativität des Legendresymbols folgt

$$\left(\frac{514}{557}\right) = \left(\frac{2}{557}\right) \cdot \left(\frac{257}{557}\right) = -1 \cdot \left(\frac{557}{257}\right).$$

Dabei benutzen wir für den ersten Faktor das zweite Ergänzungsgesetz und für den zweiten das Quadratische Reziprozitätsgesetz. Nun ist aber 557 modulo 257 zur Primzahl 43 kongruent, und es folgt, wieder mit dem Rezioprozitätsgesetz und wegen $257 = 6 \cdot 43 - 1$, dass

$$\left(\frac{557}{257}\right) = \left(\frac{43}{257}\right) = \left(\frac{257}{43}\right) = \left(\frac{42}{43}\right) = \left(\frac{-1}{43}\right) = -1,$$

denn 43 ist 3 modulo 4.
Insgesamt ist damit

$$\left(\frac{514}{557}\right) = (-1) \cdot (-1) = 1.$$