Karlsruher Institut für Technologie
Institut für Algebra und Geometrie
PD Dr. Stefan Kühnlein Dipl.-Math. Jochen Schröder

Einführung in Algebra und Zahlentheorie – Übungsblatt 14
Das ist ja wohl das Letzte!

Aufgabe 1 (4 Punkte)
Sei $R \neq 0$ ein kommutativer Ring. Zeige, dass R genau dann ein Hauptidealring ist, wenn für jedes $n \in \mathbb{N}$ jeder R-Untermodul von R^n frei ist, also eine R-Basis besitzt.

Lösung Aufgabe 1
„⇐“ Insbesondere sind alle Untermoduln von $R = R^1$ frei. Die Untermoduln von R sind aber gerade die Ideale von R. In R sind zwei Elemente r_1, r_2 stets linear abhängig, denn für $r_1, r_2 \neq 0$ ist $r_2 \cdot r_1 + (-r_1) \cdot r_2 = 0$ eine nichttriviale Darstellung der Null. Jedes Ideal $\neq 0$ besitzt also eine einelementige Basis und ist somit ein Hauptideal, 0 ist ebenfalls Hauptideal.

Es verbleibt zu zeigen, dass R nullteilerfrei ist (Nur hier benötigen wir $R \neq 0$.). **Annahme:** Es gibt Nullteiler $a \neq 0 \in R$, etwa sei $ab = 0$ für $b \neq 0$. Sei $I = (a)(\neq 0)$ das von a erzeugte Ideal. Wir halten fest, dass $\{a\}$ keine Basis von I ist, da $\{a\}$ wegen $ba = 0$ nicht linear unabhängig ist, aber I besitzt eine Basis $\{r\}$ für ein $r \neq 0$ und wegen der linearen Unabhängigkeit ist r kein Nullteiler. Aber wegen $(r) = (a)$ ist $r = sa$ für ein $s \in R$ und damit gilt $rb = sab = s \cdot 0 = 0$ und r eben doch ein Nullteiler. Dies ist ein Widerspruch.
(Achtung: wir können nicht davon ausgehen, dass a und r assoziiert sind, denn dafür bräuchten wir bereits die Nullteilerfreiheit.)

„⇒“ Wir schreiben den Beweis aus der Vorlesung für den Spezialfall $R = \mathbb{Z}$ (fast) ab.
Für $n = 0$ glauben wir die Aussage und das reicht bereits als Induktionsanfang (auch wenn wir es eigentlich nur für $n \in \mathbb{N}$ zeigen wollten...). Da R ein Hauptidealring ist (dies gibt für Ideale $I \neq 0$ ein einelementiges Erzeugendensystem), glauben wir die Aussage aber auch für $n = 1$, hierbei benötigen wir wieder die Nullteilerfreiheit (diese liefert die lineare Unabhängigkeit für das einelementige Erzeugendensystem).

Sei nun die Aussage wahr für $n \geq 1$ und $A \leq R^{n+1}$ eine Untergruppe. $\Phi : R^{n+1} \to R$ sei die Projektion auf die letzte Komponente. $K := \mathrm{Kern}(\Phi|_A) = \mathrm{Kern}(\Phi) \cap A = \{ \begin{pmatrix} x_1 \\ \cdots \\ x_n \\ 0 \end{pmatrix} \in A\}$ ist Untermodul von $\{ \begin{pmatrix} x_1 \\ \cdots \\ x_n \\ 0 \end{pmatrix} \in R^{n+1}\}$, wobei letzter Modul auf offensichtliche Art und Weise mit R^n identifiziert wird.
K kann also als Untermodul von R^n aufgefasst werden und besitzt nach Induktionsvoraussetzung eine Basis B.
Ist bereits $\Phi(A) = 0$, so ist $A = K$ und wir sind fertig.
Ohne Einschränkung sei also $\Phi(A) \neq 0$ ein echter Untermodul von R, dann gibt es eine einelementige Basis $\{z\}$ (Wir nutzen wie im Spezialfall $n = 1$, dass R Hauptidealring ist.). Es gibt ein Urbild $y = \begin{pmatrix} x_1 \\ \cdots \\ x_n \\ z \end{pmatrix}$ von z in A.

Behauptung: $B \cup \{y\}$ ist eine Basis von A.
Erzeugendensystem: Für $a \in A$ beliebig ist $\Phi(a) = rz$ für ein $r \in R$, denn z erzeugt $\Phi(A)$. Wegen $rz = r\Phi(y) = \Phi(ry)$ ist $0 = \Phi(a) - \Phi(ry) = \Phi(a - ry)$, also $a - ry \in K$ (denn wegen $a \in A, y \in A$ ist $a - ry \in A$). Also kann $a = ry + (a - ry)$ als Summe von Elementen in (y) und K geschrieben werden, was zu zeigen war.

lineare Unabhängigkeit: Ist $\sum_{b\in B} r_b \cdot b + ry = 0$, so ist $ry = -\sum_{b\in B} r_b \cdot b$. Das impliziert $ry \in K$, also $0 = \Phi(ry) = rz$. Aber wegen der Nullteilerfreiheit (und da im Fall $\Phi(A) \neq 0$ sicher $z \neq 0$ ist) impliziert das $r = 0$. Die Linearkombination ist also eine Linearkombination über B und da B eine Basis ist, müssen alle Koeffizienten 0 sein.

Aufgabe 2 (4 Punkte)

a) Sei G eine einfache Gruppe mit $\#G = 60$. Wieviele Elemente der Ordnung 5 besitzt G?

b) Zeige, dass es keine einfache Gruppe G mit $\#G = 56$ gibt.

Lösung Aufgabe 2

a) Auf Blatt 13 haben wir in Aufgabe 3 mithilfe der Elemente der Ordnung 7 die Anzahl der 7-Sylowgruppen der S_7 ermittelt, hier gehen wir genau andersherum vor.
Es ist $60 = 5 \cdot 12$ und für die Anzahl s_5 der 5-Sylowgruppen - was genau die Untergruppen mit 5 Elementen sind - gilt nach Sylow:
$s_5 \equiv 1\ (5), s_5|12$, aber da G einfach ist, kann s_5 nicht 1 sein, wieder nach Blatt 13, diesmal Aufgabe 4. Also muss $s_5 = 6$ sein, es gibt 6 Untergruppen der Ordnung 5.
Die Elemente der Ordnung 5 sind genau die nichttrivialen Elemente solcher Untergruppen und - wie bereits früher gesehen - zwei verschiedene Untergruppen der Ordnung 5 haben nur das triviale Element gemeinsam.
Für jede der sechs 5-Sylowgruppen finden wir also vier Elemente der Ordnung 5, für verschiedene 5-Sylowgruppen sind die vier Elemente paarweise verschieden, insgesamt gibt es also $6 \cdot 4 = 24$ Elemente der Ordnung 5.

b) Wir haben ja bereits mehrere Argumente gesehen, wie wir mit den Sylow-Sätzen die Nicht-Einfachheit einer Gruppe zeigen können. Hier gehen wir noch etwas anders vor.

Es ist $56 = 2^3 \cdot 7$ und für die Anzahl s_7 der 7-Sylowgruppen gilt $s_7|8, s_7 \equiv 1\ (7)$ und wir wissen (Blatt 13, A4a)), dass die einzige 7-Sylowgruppe ein nichttrivialer Normalteiler ist, falls $s_7 = 1$. Wir müssen also nur den Fall $s_7 = 8$ behandeln.
Analog wie in a) gibt es dann $8 \cdot 6 = 48$ Elemente der Ordnung 7.
Nach Sylow gibt es mindestens eine 2-Sylowgruppe mit 8 Elementen - diese muss genau aus den 8 verbleibenden Elementen bestehen, denn kein Element einer Gruppe mit 8 Elementen kann Ordnung 7 haben. Insbesondere kann es dann keine zweite 2-Sylowgruppe geben, es gibt ja gar keine Elemente mehr dafür!
Wieder mit Blatt 13, A4 folgern wir, dass die eine 2-Sylowgruppe ein nichttrivialer Normalteiler ist.

Aufgabe 3 (3 Punkte)
Berechne die Legendresymbole $\left(\frac{35}{151}\right)$ und $\left(\frac{541}{1223}\right)$.

Lösung Aufgabe 3
Das ist kein Problem, wenn wir uns an die Multiplikativität des Legendresymbols und das quadratische Reziprozitätsgesetz und seine Erweiterungssätze erinnern. Es ist

$\left(\frac{35}{151}\right) = \left(\frac{5}{151}\right)\cdot\left(\frac{7}{151}\right) = \left(\frac{151}{5}\right)\cdot(-1)^{\frac{151-1}{2}\cdot\frac{5-1}{2}}\cdot\left(\frac{151}{7}\right)\cdot(-1)^{\frac{151-1}{2}\cdot\frac{7-1}{2}} = \left(\frac{151}{5}\right)\cdot 1\cdot\left(\frac{151}{7}\right)\cdot(-1) = -\left(\frac{1}{5}\right)\cdot\left(\frac{4}{7}\right) = -1$,
da 1 modulo 5 und 4 modulo 7 natürlich Quadrate sind, sowie

$\left(\frac{541}{1223}\right) = \left(\frac{1223}{541}\right)\cdot(-1)^{\frac{1223-1}{2}\cdot\frac{541-1}{2}} = \left(\frac{1223}{541}\right) = \left(\frac{141}{541}\right) = \left(\frac{3}{541}\right)\cdot\left(\frac{47}{541}\right) = \left(\frac{541}{3}\right)\cdot(-1)^{\frac{541-1}{2}\cdot\frac{3-1}{2}}\cdot\left(\frac{541}{47}\right)\cdot(-1)^{\frac{541-1}{2}\cdot\frac{47-1}{2}} = \left(\frac{541}{3}\right)\cdot\left(\frac{541}{47}\right) = \left(\frac{1}{3}\right)\cdot\left(\frac{24}{47}\right) \overset{\left(\frac{1}{3}\right)=1}{=} \left(\frac{24}{47}\right) = \left(\frac{3}{47}\right)\cdot\left(\frac{2}{47}\right)^3 \overset{(*)}{=} \left(\frac{47}{3}\right)\cdot(-1)^{\frac{47-1}{2}\cdot\frac{3-1}{2}}\cdot\left(\frac{2}{47}\right) \overset{(**)}{=} -\left(\frac{47}{3}\right)\cdot 1 = -\left(\frac{2}{3}\right) = 1$, da 2 kein Quadrat modulo 3 ist, was man sieht oder mit Bemerkung 4.1.7 folgert.
$(*)$ nutzt gerade, dass $a^3 = a$ für $a \in \{-1, 0, 1\}$, die dritte Potenz des Legendresymbols also das Legendresymbol selbst ist, und $(**)$ benutzt die Bemerkung 4.1.7 aus dem Skript, die aussagt, dass $\left(\frac{2}{47}\right) = 1$ ist.

Aufgabe 4 (5 Punkte)
Seien p, q zwei ungerade Primzahlen mit $p = q + 9a$ für ein $a \in \mathbb{Z}$. Zeige die folgenden Aussagen:

a) $\left(\frac{p}{q}\right) = \left(\frac{a}{q}\right)$ und $\left(\frac{-q}{p}\right) = \left(\frac{a}{p}\right)$.

b) Für $a \equiv 0$ modulo 4 gilt $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.

c) Finde einen Zusammenhang zwischen den Legendresymbolen $\left(\frac{a}{p}\right)$, $\left(\frac{a}{q}\right)$ für $a \equiv 2$ modulo 4.
(*Hinweis*: Der Zusammenhang ist abhängig von p.)

Lösung Aufgabe 4
Zunächst halten wir fest, dass ohne Einschränkung p, q beide nicht 3 sind. Sonst müsste nämlich – da $3|9a$ und p, q prim – $a = 0$, also $p = q$ gelten, die Aussagen sind dann offensichtlich, die Voraussetzung in c) wäre sogar gar nicht erfüllbar. Insbesondere ist 9 also über p, q ein „echtes“ Quadrat, das Legendresymbol jeweils 1.

a) Es ist $\left(\frac{p}{q}\right) = \left(\frac{q+9a}{q}\right) = \left(\frac{9a}{q}\right) = \left(\frac{9}{q}\right) \cdot \left(\frac{a}{q}\right) \overset{\left(\frac{9}{q}\right)=1}{=} \left(\frac{a}{q}\right)$ sowie
$\left(\frac{-q}{p}\right) = \left(\frac{9a-p}{p}\right) = \left(\frac{9a}{p}\right) = \left(\frac{9}{p}\right) \cdot \left(\frac{a}{p}\right) \overset{\left(\frac{9}{p}\right)=1}{=} \left(\frac{a}{p}\right)$.

b) Wegen $4|a$ gilt auch $4|(p-q)$, also lassen p, q modulo 4 beide Rest 1 (Fall 1) oder beide Rest 3 (Fall 2). Dann gilt
$\left(\frac{a}{q}\right) \overset{a)}{=} \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} = \begin{cases} \left(\frac{q}{p}\right) & \text{im Fall 1} \\ -\left(\frac{q}{p}\right) & \text{im Fall 2} \end{cases}$ sowie
$\left(\frac{a}{p}\right) \overset{a)}{=} \left(\frac{-q}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{q}{p}\right) \overset{4.1.4}{=} \begin{cases} \left(\frac{q}{p}\right) & \text{im Fall 1} \\ -\left(\frac{q}{p}\right) & \text{im Fall 2} \end{cases}$, womit die Gleichheit gezeigt wäre.

c) Ist $a \equiv 2$ (4), so ist auch $p - q \equiv 2$ (4). Mit dem quadratischen Reziprozitätsgesetz folgt dann $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ $(*)$, denn (genau) eine der beiden Primzahlen lässt Rest 1 modulo 4. Dann gilt:
$\left(\frac{a}{q}\right) \overset{a)}{=} \left(\frac{p}{q}\right) \overset{(*)}{=} \left(\frac{q}{p}\right)$ sowie
$\left(\frac{a}{p}\right) \overset{a)}{=} \left(\frac{-q}{p}\right) \overset{4.1.4}{=} \begin{cases} \left(\frac{q}{p}\right) & \text{falls } p \equiv 1 \text{ (4)} \\ -\left(\frac{q}{p}\right) & \text{falls } p \equiv 3 \text{ (4)} \end{cases}$.
Also ist $\left(\frac{a}{q}\right) = \left(\frac{a}{p}\right)$, falls $p \equiv 1$ (4), und $\left(\frac{a}{q}\right) = -\left(\frac{a}{p}\right)$, falls $p \equiv 3$ (4).