

---

Lösungsblatt 3 zur Zahlentheorie

---

**Aufgabe 1.**

Sei  $M \subset \mathbb{Q}$  ein endlich erzeugter  $\mathbb{Z}$ -Modul, etwa mit Erzeugern  $x_1, \dots, x_n \in \mathbb{Q}$ . Wir schreiben  $x_i = \frac{a_i}{b_i}$  mit  $a_i, b_i \in \mathbb{Z}, b_i \neq 0$ . Sei  $k$  ein gemeinsames Vielfaches der  $b_1, \dots, b_n$ . Dann ist  $kM \subset \mathbb{Z}$  ein  $\mathbb{Z}$ -Modul und daher ein Hauptideal. Es gibt also ein  $t \in \mathbb{Z}$  mit  $kM = \mathbb{Z}t$ . Multiplikation mit  $\frac{1}{k}$  liefert  $M = \mathbb{Z}\frac{t}{k}$ , was zeigt, dass  $M$  frei vom Rang 1 ist.

Angenommen  $\mathbb{Q}$  wäre als  $\mathbb{Z}$ -Modul endlich erzeugt, so gäbe es ein  $\frac{a}{b} \in \mathbb{Q}$  mit  $a, b \in \mathbb{Z}$  und  $b \neq 0$ , so dass  $\mathbb{Q} = \mathbb{Z}\frac{a}{b}$  ist. Ist jedoch  $p$  eine Primzahl mit  $p \nmid b$ , so ist  $\frac{1}{p} \notin \mathbb{Z}\frac{a}{b}$ . Widerspruch.

**Aufgabe 2.**

(a) Seien  $x_1, \dots, x_n$  Erzeuger von  $M$ . Dann ist die Abbildung

$$\begin{aligned} \phi: R^n &\longrightarrow M \\ (r_1, \dots, r_n) &\longmapsto r_1x_1 + \dots + r_nx_n \end{aligned}$$

ein  $R$ -Modulhomomorphismus. Da die  $x_1, \dots, x_n$  den Modul  $M$  erzeugen, ist  $\phi$  surjektiv. Sei  $i: \ker(\phi) \rightarrow R^n$  die natürliche Inklusionsabbildung. Dann ist

$$0 \longrightarrow \ker(\phi) \xrightarrow{i} R^n \xrightarrow{\phi} M \longrightarrow 0$$

nach Konstruktion von  $i$  und  $\phi$  eine kurze exakte Sequenz.

(b) Wir betrachten obige kurze exakte Sequenz und erhalten mit Aufgabe 1.(b) von Blatt 2, dass  $M \cong R^n / \ker(\phi)$  ist. Da direkte Summen und Untermoduln von halbeinfachen Moduln halbeinfach sind, ist sowohl  $R^n$  als auch  $\ker(\phi)$  halbeinfach. Schließlich sind auch Quotienten von halbeinfachen Moduln halbeinfach, woraus die Behauptung folgt.

(c) Wegen Teil (b) genügt es zu zeigen, dass  $R = M_{n \times n}(K)$  aufgefasst als  $R$ -Modul halbeinfach ist. Für  $i = 1, \dots, n$  bezeichnen wir mit  $M_i$  die Menge Matrizen in  $R$ , die Einträge verschieden von 0 nur in der  $i$ -ten Spalte haben. Offenbar ist jedes dieser  $M_i$  ein  $R$ -Untermodul von  $R$ . Weiter ist  $R = \sum_{i=1}^n M_i$ . Ist  $A \in M_i \cap \sum_{j \neq i} M_j$ . So hat  $A$  auf der einen Seite nur in Zeile  $i$  Einträge ungleich 0, auf der anderen Seite ist  $A$  die Summe von Matrizen, die alle in Zeile  $i$  nur den Eintrag 0 haben. Daher muss  $A = 0$  sein und wir erhalten  $R = \bigoplus_{i=1}^n M_i$ . Zuletzt bleibt noch zu zeigen, dass die  $M_i$  einfach sind. Angenommen  $0 \neq A \in M_i$ . Wir fassen die  $i$ -te Spalte von  $A$  als Vektor  $v \in K^n \setminus \{0\}$  auf. Sei  $w \in K^n$  beliebig. Dann gibt es eine Matrix  $B \in R$  mit  $Bv = w$ . Insbesondere ist die  $i$ -te Spalte von  $BA$  der Vektor  $w$ . Also gilt  $RA = M_i$ . Dies zeigt, dass  $M_i$  ein einfacher Modul ist, denn jedes von 0 verschiedene Element erzeugt ganz  $M_i$ .

**Aufgabe 3.**

Sei

$$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$$

eine kurze exakte Sequenz. Wir konstruieren ein  $j: N \rightarrow M$  mit  $g \circ j = \text{id}_N$ . Sei  $(a_i)_{i \in I}$  eine Basis von  $N$ . Da  $N$  frei ist, lässt sich jede Wahl von Werten auf den  $(a_i)$  zu einem Modulhomomorphismus fortsetzen. Sei  $y_i \in M$  mit  $g(y_i) = a_i$ . Solch ein  $y_i$  existiert für jedes  $i \in I$ , da  $g$  surjektiv ist. Wir definieren  $j(a_i) = y_i$ . Dann ist  $g \circ j(a_i) = g(y_i) = a_i$ . Also ist  $g \circ j = \text{id}_N$  auf einer Basis von  $N$  und damit auf ganz  $N$ . Dies zeigt, dass die exakte Sequenz zerfällt.

Ist hingegen zwar  $M$  frei nicht jedoch  $N$ , so muss diese Sequenz im Allgemeinen nicht zerfallen. Sei dazu  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  mit  $f(z) = 2z$  und  $g: \mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z}$  die natürliche Projektion. Dann ist

$$0 \rightarrow \mathbb{Z} \xrightarrow{f} \mathbb{Z} \xrightarrow{g} \mathbb{Z}/2\mathbb{Z} \rightarrow 0$$

eine kurze exakte Sequenz von  $\mathbb{Z}$ -Moduln. Würde diese zerfallen, so wäre  $\mathbb{Z}/2\mathbb{Z}$  ein direkter Summand von  $\mathbb{Z}$ , insbesondere wäre  $\mathbb{Z}/2\mathbb{Z}$  ein Untermodul von  $\mathbb{Z}$ . Doch dann gäbe es ein  $0 \neq x \in \mathbb{Z}$  mit  $x + x = 0$ . Dies widerspricht der Nullteilerfreiheit von  $\mathbb{Z}$ .

#### Aufgabe 4.

Diese Aussage ist falsch. Wir betrachten dazu die  $\mathbb{Z}$ -Moduln  $\mathbb{Z}/4\mathbb{Z}$  und  $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ . Es ist

$$\mathbb{Z}/4\mathbb{Z} \supset 2\mathbb{Z}/4\mathbb{Z} \supset 0$$

und

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \supset 0 \oplus \mathbb{Z}/2\mathbb{Z} \supset 0$$

jeweils eine Kompositionsreihe von  $\mathbb{Z}/4\mathbb{Z}$  bzw.  $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ . Beide setzen sich zusammen aus zweimal dem Faktor  $\mathbb{Z}/2\mathbb{Z}$ . Allerdings gilt  $\mathbb{Z}/4\mathbb{Z} \not\cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ . Denn in erstem gibt es ein Element  $x$  mit  $x + x \neq 0$ , in letzterem gilt stets  $x + x = 0$ .