Universität Konstanz
Fachbereich Mathematik und Statistik
Jun.-Prof. Dr. Arno Fehm
Aaron Kunert
SS 2012

Übungen zur Vorlesung Zahlentheorie

Blatt 5

Aufgabe 13

Beweisen Sie folgende Variante des Struktursatzes für endlich erzeugte Moduln über Hauptidealringen: Ist M ein endlich erzeugter Modul über einem Hauptidealring R, so existieren bis auf Assoziiertheit eindeutig bestimmte $d_1, \dots, d_n \in R$ mit $d_1 | d_2 | \dots | d_n$, so dass

$$M \;\cong\; R/(d_1) \oplus \cdots \oplus R/(d_n).$$

Beweis:
Wir zeigen zunächst die Existenz. Der Struktursatz besagt, dass Primelemente $p_1, \dots, p_r$ und dass für $i = 1, \dots, r$ ein $m_i \in \mathbb{N}_0$ und nichtnegative ganze Zahlen

$$e_{i1} \geq e_{i2} \geq \cdots \geq e_{im_r}$$

existieren mit

$$M \;\cong R^k \oplus \bigoplus_{i=1}^{r} \bigoplus_{j=1}^{m_i} R/(p_i^{e_{ij}}).$$

Setzen wir $e_{ij} = 0$ für $j > m_i$ und setzen wir $m := \max_i(m_i)$, so können wir ohne Einschränkung annehmen

$$M \;\cong \bigoplus_{i=1}^{r} \bigoplus_{j=1}^{m} R/(p_i^{e_{ij}}).$$

Schreiben wir $q_j := (p_1^{e_{1j}} p_2^{e_{2j}} \dots p_r^{e_{rj}})$, so folgt aus obigen Ungleichungen

$$q_m \mid q_{m-1} \mid \cdots \mid q_1.$$

Anwendung des chinesischen Restsatzes liefert dann

$$\begin{aligned} M \;&\cong R^k \oplus \bigoplus_{i=1}^{r} \bigoplus_{j=1}^{m} R/(p_i^{e_{ij}}) \\ &\cong R^k \oplus \bigoplus_{j=1}^{m} \bigoplus_{i=1}^{r} R/(p_i^{e_{ij}}) \\ &\cong R^k \oplus \bigoplus_{j=1}^{m} R/(p_1^{e_{1j}} p_2^{e_{2j}} \dots p_r^{e_{rj}}) \\ &\cong R^k \oplus R/q_1 \oplus \cdots \oplus R/q_m. \end{aligned}$$

Die Behauptung folgt dann für $d_1 := q_m, \dots, d_m := q_1, d_{m+1} := 0, \dots, d_{m+k} := 0$. Die Eindeutigkeit folgt sofort aus der Eindeutigkeit der Primfaktorzerlegung und der Eindeutigkeit der p_i und e_{ij} im Struktursatz.

Aufgabe 14

Sei R ein Ring. Ein R-Modul M heißt **artinsch**, wenn jede absteigende Kette

$$N_1 \supseteq N_2 \supseteq \dots$$

von Untermoduln von M stationär wird ("absteigende Kettenbedingung"). Der Ring R heißt artinsch, wenn er als R-Modul artinsch ist.

a) Sei N ein Untermodul von M. Zeigen Sie: Genau dann ist M artinsch, wenn sowohl N als auch M/N artinsch sind.
b) Zeigen Sie, dass jedes Primideal eines artinschen Rings maximal ist. Folgern Sie, dass ein integrer artinscher Ring ein Körper ist.
c) Geben Sie ein Beispiel für einen noetherschen Ring, der nicht artinsch ist.

Die Symmetrie zwischen artinsch *und* noethersch *ist trügerisch: Im Kontrast zu c) kann man zeigen, dass jeder artinsche Ring noethersch ist!*

Beweis:

a) Seien zunächst N und M/N artinsch. Sei $M_1 \supseteq M_2 \supseteq M_3 \supseteq \dots$ eine absteigende Kette von Untermoduln von M. Dann betrachte die absteigendenden Ketten $N_i := M_i \cap N$, sowie $V_i := (M_i + N)/N$. Da sowohl N als auch M/N artinsch sind, gibt es ein $k \in \mathbb{N}$ mit $N_k = N_{k+l}$ und $V_k = V_{k+l}$ für alle $l \geq 0$. Sei nun $l \geq 0$ beliebig. Offensichtlich ist $M_{k+l} \subseteq M_k$ wir zeigen nun auch die umgekehrte Inklusion. Sei $x \in M_k$. Da $V_k = V_{k+l}$ ist, gibt es $z \in N$, sowie $y \in M_{k+l}$, so dass $x - y = z$ gilt. Dann ist $z \in (N \cap M_k) = (N \cap M_{k+l})$. Daher sind $y, z \in M_{k+l}$, also auch $x \in M_{k+l}$.
Sei umgekehrt M artinsch. Eine absteigende Folge von Untermoduln von N ist auch eine absteigende Folge von Untermoduln von M und wird daher stationär. Dies zeigt, dass N artinsch ist. Ist $V_1 \supseteq V_2 \supseteq \dots$ eine absteigende Folge von Untermoduln von M/N so ist $V_1 + N \supseteq V_2 + n \supseteq \dots$ eine absteigende Folge von Untermoduln von M und wird daher stationär, woraus folgt, dass auch die Folge V_i stationär wird.
b) Sei $\mathfrak{p}$ ein Primideal eines artinschen Rings. Dann ist $R/\mathfrak{p}$ ein artinscher Integritätsring. Wir zeigen, dass $A := R/\mathfrak{p}$ ein Körper ist. Dann muss $\mathfrak{p}$ schon ein maximales Ideal gewesen sein. Sei $0 \neq x \in A$. Dann haben wir eine absteigende Kette von Idealen
$$(x) \supseteq (x^2) \supseteq (x^3) \supseteq \dots$$
Da A artinsch ist, gibt es ein $k \geq 0$ mit $(x^{k+1}) = (x^k)$. Also existiert ein $a \in A$ mit $ax^{k+1} = x^k$. Da A integer ist, folgt $ax = 1$, also ist x eine Einheit und somit A ein Körper.
c) Der Ring $\mathbb{Z}$ ist ein Hauptidealring und daher noethersch. Allerdings ist er nicht artinsch, da er integer und kein Körper ist.

Aufgabe 15

a) Geben Sie ein Beispiel für einen noetherschen Ring, der nicht faktoriell ist.
b) Geben Sie ein Beispiel für einen faktoriellen Ring, der nicht noethersch ist. (*Sie könnten zum Beispiel zeigen, dass* $\mathbb{Q}[X_1, X_2, \dots]$ *die gewünschten Eigenschaften hat.*)

Beweis:

a) Der Ring $R := \mathbb{Z}[i\sqrt{5}]$ ist noethersch, da er schon als $\mathbb{Z}$–Modul noethersch ist. Aber R ist nicht faktoriell, denn in R gilt
$$6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5}).$$

Nun ist die Zahl 2 irreduzibel in R. Angenommen $2 = xy$ mit $x, y \in R$, etwa $x = a + bi\sqrt{5}$ und $y = c + di\sqrt{5}$. Dann ist

$$2 = |2| = |xy| = |x||y| = (a^2 + 5b^2)(c^2 + 5d^2).$$

Dies ist nur möglich, wenn $|x| = 1$, oder $|y| = 1$ ist. Also müsste dann x oder y gleich ± 1 sein. Wäre R faktoriell, so wäre 2 auch ein Primelement. Also müsste $(1 + i\sqrt{5})$ oder $(1 - i\sqrt{5})$ durch 2 teilbar sein, was offensichtlich nicht der Fall ist. Also kann R nicht faktoriell sein.

b) Der Ring $R = \mathbb{Q}[X_1, X_2, \ldots]$ ist nicht noethersch. Allerdings ist R faktoriell: Ist $f \in R$, so involviert f nur endlich viele Variablen, liegt also in dem faktoriellen Ring $R_k := \mathbb{Q}[X_1, \ldots, X_k]$ und besitzt eine Zerlegung $f = f_1 \ldots f_r$ mit f_i prim in R_k. Es bleibt also zu zeigen, dass ein primes Element $g \in R_k$ auch in R prim bleibt. Sei also g in R_k prim. Dann ist g auch in R_l mit $l \geq k$ prim: Dazu genügt es zu zeigen, dass g irreduzibel ist, da R_l ein faktorieller Ring ist. Ist aber $g = fg$ in R_l, so liegen $f, g \in R_k$, da $\deg_{x_j}(g) = \deg_{x_j}(f) \deg_{x_j}(h)$ gilt. Daher ist g in allen R_l mit $l \geq k$ ein Primelement. Ist also $g \mid fh$ für $f, h \in R$, so gilt $sg = fh$ für ein $s \in R$. Da nur endlich viele Variablen involviert sind, gilt diese Gleichung auch in einem R_l für $l \geq k$. Insbesondere gilt $g \mid f$ oder $g \mid h$ in R_l und damit in R. Dies zeigt die Behauptung.

Aufgabe 16

Sei R ein Ring, $R[t]$ der Polynomring über R, M ein endlich erzeugter freier R-Modul mit Basis $x_1, \ldots, x_n$ und $\varphi \in \mathrm{Hom}_R(M, M)$ ein Endomorphismus von M. Sei $A = (a_{ij})_{ij} \in \mathrm{Mat}_n(R)$ die darstellende Matrix von φ bezüglich $x_1, \ldots, x_n$, d.h. $\varphi(x_i) = \sum_{j=1}^{n} a_{ij} x_j$, und sei $\chi_A(t) = \det(t\mathbb{I} - A) \in R[t]$ das charakteristische Polynom von A.

a) Der R-Modul M wird durch $tx := \varphi(x)$ zu einem $R[t]$-Modul.
b) Im $R[t]$-Modul M ist $\chi_A(t)x_i = 0$ für jedes i.
c) Im Ring $\mathrm{Mat}_n(R)$ ist $\chi_A(A) = 0$ (Satz von *Cayley-Hamilton* für Moduln).

Beweis:

a) Obige Vorschrift induziert einen Ringhomomorphismus

$$\begin{aligned} R[t] &\longrightarrow \mathrm{End}_R(M) \\ p(t) &\longmapsto p(\phi), \end{aligned}$$

woraus alle Modulaxiome direkt folgen.

b) Es ist $\varphi(x_i) = \sum_{j=1}^{n} a_{ij} x_j$ daher ist $\sum_{j=1}^{n} (\delta_{ij} \varphi(x_j) - a_{ij} x_j)$ und somit $\sum_{j=1}^{n} (\delta_{ij} t - a_{ij}) x_j = 0$. Wir setzen $b_{ij} := \delta_{ij} t - a_{ij}$ und schreiben B für die Matrix mit Einträgen b_{ij}. Dann ist B eine $n \times n$–Matrix mit Einträgen aus $R[t]$. Wir schreiben C für die Adjunkte zu B (diese existiert über beliebigen kommutativen Ringen). Es gilt also $BC = CB = \det(B)\mathbb{I}$. Die Einträge von C bezeichnen wir entsprechend mit c_{ij}. Es ist daher $\sum_{k=1}^n c_{ik} b_{kj} = \delta_{ij} \det(B)$.

$$\begin{aligned}
\sum_{j=1}^n b_{kj} x_j = 0 &\Longrightarrow \sum_{k=1}^n c_{ik} \sum_{k=1}^n b_{kj} x_j = 0 \\
&\Longrightarrow \sum_{k=1}^n \sum_{j=1}^n c_{ik} b_{kj} x_j = 0 \\
&\Longrightarrow \sum_{j=1}^n \sum_{k=1}^n c_{ik} b_{kj} x_j = 0 \\
&\Longrightarrow \sum_{j=1}^n \delta_{ij} \det(B) x_j = 0 \\
&\Longrightarrow \det(B) x_i = 0.
\end{aligned}$$

Dies zeigt die Behauptung, denn $\det(B) = \det(t\mathbb{I} - A) = \chi_A(t)$.

c) Sei $S = \chi_A(A)$ mit den Einträgen s_{ij}. Dann ist für alle $i = 1, \ldots, r$

$$0 = \sum s_{ij} x_j = \chi_A(t) x_i.$$

Da M frei ist, folgt $s_{ij} = 0$ für alle $1 \leq i, j \leq n$ und damit $S = 0$.