Moduln und Matrizen

Vorlesung Kryptographie WS2006/7

F. Heß

16. Januar 2007

Im folgenden wird eine kurze Einführung in die lineare Algebra über Ringen (und nicht Körpern) gegeben. Dieses ist "Hintergrundwissen" und wird später in der Gittertheorie verwendet.

Matrizen über Ringen

Im folgenden bezeichnet R immer einen kommutativen, nullteilerfreien Ring mit $1 \neq 0$ (also einen Integritätsring). Als Beispiele betrachte man den Ring der ganzen Zahlen $\mathbb{Z}$ oder den Polynomring $k[x_1, \ldots, x_n]$ in n Variablen über einem Körper k. Für die Gittertheorie werden wir später nur $R = \mathbb{Z}$ benötigen (so daß man dies im folgenden zur Vereinfachung auch annehmen darf).

Wir können R in einen "kleinsten" Körper $K = \mathrm{Quot}(R)$ einbetten, den Quotientenkörper von R. Die Elemente von K sind formal Brüche a/b, wobei $a/b = c/d$ genau dann gilt, wenn es ein $e \in R$ mit $ead = ecb$ gibt. Es gilt beispielsweise $\mathbb{Q} = \mathrm{Quot}(\mathbb{Z})$ und $k(x) = \mathrm{Quot}(k[x])$, der Körper der rationalen Funktionen in x.

Wir betrachten nun Matrizen über R. Die Menge der $n \times m$ Matrizen (n Zeilen, m Spalten) wird mit $R^{n \times m}$ bezeichnet. Die Determinante von $M = (x_{i,j})_{i,j} \in R^{n \times n}$ wird wie üblich über K definiert, und ist ein Element von R. Hier sind ein paar der üblichen Regeln für Determinanten:

- Leibniz-Entwicklung: $\det(M) = \sum_{\sigma \in S_n} \mathrm{sign}(\sigma) x_{1,\sigma(1)} \cdots x_{n,\sigma(n)} \in R$.
- Für $N, M \in R^{n \times n}$ gilt $\det(MN) = \det(M)\det(N)$.
- det ist eine alternierende Multilinearform.

- Ist $M_{i,j} \in R^{(n-1)\times(n-1)}$ die Matrix, die durch Streichen der i-ten Zeile und j-ten Spalte von $M \in R^{n\times n}$ entsteht, so gilt die Laplace-Entwicklung

$$\det(M) = \sum_{i=1}^{n} (-1)^{i+j} x_{i,j} \det(M_{i,j}).$$

- Die Spalten oder Zeilen von M sind genau dann K-linear unabhängig, wenn $\det(M) \neq 0$.

Der letzte Punkt kann auch für R ausgesprochen werden. Zeilen oder Spalten heißen R-linear unabhängig, wenn es keine nicht-triviale Linearkombination mit Koeffizienten aus R gibt, welche Null ergibt. Da man Nenner immer herausmultiplizieren kann, sind Zeilen oder Spalten genau dann R-linear unabhängig, wenn sie K-linear unabhängig sind.

1 Satz. *(i) Sei $A \in R^{n\times n}$, $x = (x_i)^t \in R^n$ und $b = (b_i)^t \in R^n$ mit $Ax = b$. Ist B_i die Matrix, deren i-te Spalte gleich b ist und die ansonsten mit A übereinstimmt, so gilt $\det(B_i) = x_i \det(A)$.*

(ii) Sei $M \in R^{n\times n}$ und $M' = ((-1)^{i+j} \det(M_{j,i}))_{i,j} \in R^{n\times n}$, wobei $M_{i,j}$ die Matrix ist, die durch Streichen der i-ten Zeile und j-ten Spalte von M entsteht. Dann gilt $MM' = M'M = \det(M) I_n$.

(iii) Eine Matrix $M \in R^{n\times n}$ ist genau dann invertierbar, wenn $\det(M)$ in R invertierbar ist.

Beweis. (i): Die i-te Spalte b in B_i ist die Linearkombination der Spalten von A mit den Koeffizienten x_i. Sei $A_{i,j}$ die Matrix, die an der i-ten Spalte die j-Spalte von A hat und ansonsten mit A übereinstimmt. Dann gilt $\det(A_{i,j}) = \delta_{i,j} \det(A)$ (Kronecker-Delta) und aufgrund der Linearität der Determinante ergibt sich $\det(B_i) = \sum_{j=1}^{n} x_j \det(A_{i,j}) = x_i \det(A)$.

(ii): Folgt aus (i), der obigen Entwicklung für Determinanten und durch Kürzen von $\det(M)$ (R Integritätsring).

(iii): Ist M invertierbar, so gilt $1 = \det(MM^{-1}) = \det(M)\det(M^{-1})$. Wegen $M^{-1} \in R^{n\times n}$ folgt auch $\det(M^{-1}) \in R$ und $\det(M)$ ist invertierbar in R.

Umgekehrt sei $M \in R^{n\times n}$ und M' wie in (ii). Ist $\det(M)$ invertierbar, so ist $M'/\det(M)$ über R definert und invers zu M. □

Satz 1, (i) ist als Cramersche Regel bekannt. Die Matrix M' in (ii) nennt man häufig Pseudoinverse von M. Invertierbare Matrizen über Ringen heißen auch unimodular.

Die Zeilen (oder Spalten) einer Matrix kann man mittels elementarer Transformationen bzw. den zugehörigen Transformationsmatrizen umformen, wie zum Beispiel im Gauß Algorithmus. Die elementaren, unimodularen Transformationsmatrizen korrespondieren zu den folgenden Transformationen: Zeile mit invertierbarem Element multiplizieren, Zeilen vertauschen, Vielfaches einer Zeile zu einer anderen addieren. Jede dieser Operationen kann man über R rückgängig machen.

Matrizen über Hauptidealringen

In diesem Abschnitt bezeichnet R einen Hauptidealring. Dies bedeutet, daß jedes Ideal von R ein Hauptideal ist, also von genau einem Element erzeugt wird. Äquivalent dazu ist, daß es zu je zwei Elementen $a, b \in R$ Elemente $\lambda, \mu \in R$ gibt, so daß $c = \lambda a + \mu b$ ein größter gemeinsamer Teiler von a, b ist. Dies wiederum heißt $a/c, b/c \in R$, und wenn $a/d, b/d \in R$ für ein $d \in R$, dann gilt auch $c/d \in R$. Beispiele für R sind $R = \mathbb{Z}$ und $R = k[x]$. Die Koeffizienten λ, μ können hier durch den euklidischen Algorithmus erhalten werden.

Über Hauptidealringen läßt sich jede unimodulare Transformation in die oben genannten, elementaren Transformationen faktorisieren. Wir leiten hier nun dies und weitere Aussagen über Matrixnormalformen her.

2 Lemma. *(i) Seien $a_1, \ldots, a_n \in R$. Dann gibt es eine unimodulare Matrix U in $R^{n\times n}$ mit $(a_1, \ldots, a_n)U = (d, 0, \ldots, 0)$, wobei $d = \gcd\{a_1, \ldots, a_n\}$ ist.*

(ii) Seien $a_1, \ldots, a_n \in R$. Dann gibt es eine Matrix A in $R^{n\times n}$, deren erste Zeile gleich $(a_1, \ldots, a_n)$ ist und für die $\det(A) = \gcd\{a_1, \ldots, a_n\}$ gilt.

Beweis. (i): Für $i < j$ gibt es $\lambda, \mu \in R$ mit $\lambda a_i + \mu a_j = c$ und $c = \gcd\{a_i, a_j\}$. Die Matrix

$$T' = \begin{pmatrix} \lambda & -a_j/c \\ \mu & a_i/c \end{pmatrix}$$

ist in $R^{2\times 2}$, unimodular und erfüllt $(a_i, a_j)T' = (c, 0)$. Wir können T' zu einer unimodularen Matrix $T \in R^{n\times n}$ machen, indem wir T' als (erweiterten) Diagonalblock in I_n einbetten, so daß gilt:

$$\begin{aligned}(a_1, \ldots, a_{i-1}, a_i, a_{i+1}, \ldots, a_{j-1}, a_j, a_{j+1}, \ldots, a_n)T \\ = (a_1, \ldots, a_{i-1}, c, a_{i+1}, \ldots, a_{j-1}, 0, a_{j+1}, \ldots, a_n).\end{aligned}$$

Indem wir diese Schritte wiederholen und die so erhaltenen, unimodularen Transformationsmatrizen T aufmultiplizieren, erhalten wir schließlich ein unimodulares $U \in R^{n\times n}$ mit $(a_1, \ldots, a_n)U = (d, 0, \ldots, 0)$.

(ii): Sei U unimodular mit $(a_1, \ldots, a_n)U = (d, 0, \ldots, 0)$, $d = \gcd\{a_1, \ldots, a_n\}$ und $\det(U) = 1$ (andernfalls eine Spalte von U durch $\det(U)$ dividieren). Sei B die Matrix, deren erste Zeile $(d, 0, \ldots, 0)$ ist und die ansonsten mit I_n übereinstimmt. Dann gilt $\det(B) = d$ und die Matrix $A = BU^{-1}$ erfüllt die Bedingungen. □

Ein Element a von R heißt eine Einheit, wenn a in R invertierbar ist, wenn es also ein $b \in R$ mit $ab = 1$ gibt. Zwei Elemente heißen assoziiert, wenn ihr Quotient eine Einheit in R ist.

Sei $P \subseteq R$ ein Vertretersystem nicht-assoziierter Elemente von R und $R_b \subseteq R$ ein Vertretersystem für die Restklassen R/Rb für jedes $b \in P$. Zum Beispiel sind $-1, 1$ die Einheiten von $R = \mathbb{Z}$ und wir können die Vertretersysteme $P = \mathbb{Z}^{\geq 0}$ und $R_b = \{0, \ldots, b-1\}$ oder häufig besser $\{\lceil -(b-1)/2\rceil, \ldots, \lfloor b/2\rfloor\}$ wählen.

3 Definition. Sei $M = (m_{i,j}) \in R^{n\times m}$ und $I_j = \{\, i \mid m_{i,j} \neq 0 \text{ und } 1 \leq i \leq n\}$. Wir setzen $j_0 = \max\{\, j \mid I_j \neq \{\} \text{ und } 1 \leq j \leq m\}$, $i_j = \min I_j$ und definieren: M ist in unterer Spalten-Dreiecksgestalt, wenn $i_1 < \cdots < i_{j_0}$.

Die Matrix M in unterer Spalten-Dreiecksgestalt heißt in unterer Spalten-Hermite-Normalform, wenn für jedes $j = 1, \ldots, j_0$ gilt: $m_{i_j,j} \in P$ und $m_{i_j,k} \in R_{m_{i_j,j}}$ für $1 \leq k < j$.

Entsprechend können obere Spalten- und untere, obere Zeilenformen für M definiert werden.

Eine quadratische Matrix M mit $\det(M) \neq 0$ in Spalten-Hermite-Form ist also eine Dreiecksmatrix, in der die Koeffizienten neben der Diagonale modulo der Diagonalkoeffizienten reduziert ist.

4 Satz. *Zu einer Matrix $M \in R^{n\times m}$ gibt es eine unimodulare Matrix $T \in R^{m\times m}$, so daß MT in unterer Spalten-Dreiecksgestalt ist. Sind Vertretersysteme P und R_b gegeben, so kann T so gewählt werden, daß MT in unterer Spalten-Hermite-Normalform ist. In diesem Fall ist MT eindeutig durch M bestimmt.*

Beweis. Beginnend bei der ersten Zeile von M wenden wir Lemma 2, (i) sukzessive an. Dies zeigt, daß eine untere Spalten-Dreiecksgestalt erreicht werden kann. Durch Multiplikation der Spalten mit Einheiten erreichen wir die Bedingung $m_{i_j,j} \in P$, durch Addieren von Vielfachen der j-ten Spalte zu den k-ten mit $k < j$ beginnend bei $j = 1$ erreichen wir die Bedingung $m_{i_j,k} \in R_{m_{i_j,j}}$. Aufgrund der Dreieckecksform bleibt die Matrix oberhalb der

i_j-ten Zeile unberührt. Die Eindeutigkeitsaussage erhält man am leichtesten aus der Interpretation der Spalten von MT als Modulbasis, siehe später. □

Eine unimodulare Matrix $M \in R^{n\times n}$ kann nach dem Satz in eine untere Dreiecksmatrix mit Einheiten bzw. Einsen auf der Diagonalen transformiert werden. Indem noch noch links reduziert (Hermiteform bilden), erhält man I_n. Dies zeigt, daß sich jede unimodulare Matrix über R in ein Produkt der elementaren, unimodularen Matrizen T' bzw. T aus Lemma 2 zerlegen läßt.

Will man Hermite-Normalformen "von Hand" ausrechnen, kann man wie folgt vorgehen. Man führt den euklidischen Algorithmus bezüglich der Elemente der ersten Zeile aus, rechnet aber mit den ganzen Spalten. Hierbei addiert man also in jedem Schritt ein Vielfaches einer Spalte zu einer anderen Spalte. Bei Bedarf multipliziert man Spalten mit -1. Zum Schluß sind in der ersten Zeile alle Elemente bis auf das erste Null. Das erste ist der größte gemeinsame Teiler der Ausgangszeilenelemente und kann auch Null sein. Dann fährt man induktiv mit der zweiten Spalte ab dem zweiten Element fort. Komplexitätstechnisch gibt es wesentlich effizientere Verfahren zur Hermite-Normalformberechnung.

Eine r-Minore der Matrix $M \in R^{n\times n}$ für $r \leq n$ ist die Determinante einer $(r \times r)$-Matrix, die durch Streichen von $n - r$ Zeilen und Spalten aus M entsteht. Wir definieren $d_r(M)$ als den größten gemeinsamen Teiler aller r-Minoren von M (ist bis auf Einheiten eindeutig bestimmt).

5 Lemma. (*i*) *Sei $M \in R^{n\times n}$ eine Diagonalmatrix mit den Diagonaleinträgen $a_1, \ldots, a_n$. Dann gibt es unimodulare Matrizen $U, V \in R^{n\times n}$, so daß UMV diagonal ist mit den Diagonaleinträgen $b_1, \ldots, b_n$ und $b_1 \mid \cdots \mid b_n$ gilt.*

(*ii*) *Sei $M \in R^{n\times n}$ und $U, V \in R^{n\times n}$ unimodular. Dann gilt $d_{r-1}(M) \mid d_r(M)$ und $d_r(M) = d_r(UMV)$.*

Beweis. (*i*): Sei M' die Diagonalmatrix mit a_i, a_j auf der Diagonalen und gelte $i < j$. Die unimodularen Transformationen gehen wie folgt: Addiere die zweite Zeile von M' zur ersten. Wende T' aus Lemma 2, (*i*) von rechts auf M' an. Dies liefert

$$\begin{pmatrix} c & 0 \\ \mu a_2 & d \end{pmatrix}$$

mit $c = \gcd\{a_i, a_j\}$ und $d = a_i a_j / c = \operatorname{lcm}\{a_i, a_j\}$. Nun ziehen wir das μ-fache der ersten Zeile von der zweiten Zeile ab und erhalten die Diagonalmatrix mit c, d auf der Diagonalen und es gilt $c \mid d$. Durch sukzessives Vorgehen und Aufmultiplizieren der entsprechenden unimodularen Transformationsmatrizen folgt (*i*).

(ii): Eine r-Minore kann nach dem Laplaceschen Entwicklungssatz als Linearkombination von $(r-1)$-Minoren geschrieben werden. Daher ist das von den r-Minoren erzeugte Hauptideal in dem von den $(r-1)$-Minoren erzeugten Hauptideal enthalten und es folgt $d_{r-1}(M) \mid d_r(M)$.

Eine r-Minore von MV kann als R-Linearkombination von r-Minoren von M geschrieben werden, wegen der Linearität der Determinante in den Spalten und da jede Spalte von MV eine Linearkombination der Spalten von M ist. Daher folgt wie eben $d_r(M) \mid d_r(MV)$. Weil V unimodular ist, gilt auch $d_r(MV) \mid d_r(M)$ für MV und $M = (MV)V^{-1}$. Analog folgt die Aussage für MV und UMV. □

6 Satz. *Sei $M \in R^{n\times n}$. Dann gibt es unimodulare Matrizen $U, V \in R^{n\times n}$, so daß UMV diagonal ist und für die Diagonalelemente $b_1 \mid \cdots \mid b_n$ gilt. Die b_i sind bis auf Einheiten eindeutig bestimmt.*

Beweis. Wir wenden Lemma 2, (i) abwechselnd auf die erste Zeile (unimodulare Transformation von rechts) und erste Spalte (unimodulare Transformation von links) an. Die auftretenden Elemente in Position $(1,1)$ erzeugen eine Folge von absteigenden ggT's bzw. eine aufsteigende Kette von Idealen, welche stationär wird. Dann gilt aber, daß in der ersten Zeile und Spalte außer dem Element an Position $(1,1)$ alle Elemente Null sind. Induktiv können wir M durch unimodulare Transformationen von links und rechts diagonalisieren. Mit Lemma 5, (i) erreichen wir die aufsteigende Teilbedingung.

Es gilt $d_r(UMV) = \prod_{i=1}^{r} b_i$ und somit nach Lemma 5, (ii) auch $b_r = d_r(UMV)/d_{r-1}(UMV) = d_r(M)/d_{r-1}(M)$ oder $b_r = 0$. Folglich sind die b_r eindeutig durch M bzw. den Rang von M und bis auf Einheiten bestimmt. □

7 Definition. Matrizen UMV in der Diagonalform von Satz 6 nennt man auch in Smith-Normalform oder Elementarteilerform. Die Einträge b_i nennt man Elementarteiler von M. Man kann zusätzlich fordern, daß die b_i in einem Vertretersystem P modulo Einheiten liegen.

Will man die Smith-Normalform "von Hand" ausrechnen, kann man wie im Beweis vorgehen. Man tut so, als wollte man die Spalten-Hermite-Normalform ausrechnen und transformiert die erste Zeile in die Form $(*, 0, \ldots, 0)$. Dann fährt man fort, die Zeilen-Hermite-Normalform auszurechen und transformiert die erste Spalte in die Form $(*, 0, \ldots, 0)^{tr}$. Dadurch wird im allgemeinen die erste Zeile wieder durcheinandergebracht, aber $*$ wird "kleiner", bis $*$ alle Elemente der ersten Zeile und Spalte teilt, und diese dann ohne etwas wieder durcheinanderzubringen zu Null gemacht werden können. Komplexitätstechnisch gibt es wieder wesentlich effizientere Verfahren zur Smith-Normalformberechnung.

Moduln

Ein Modul ist ein „Vektorraum“ über K, wobei K nicht unbedingt ein Körper, sondern nur noch ein Ring zu sein braucht.

8 Definition. Sei M eine abelsche Gruppe. Wir betrachten eine Multiplikation $\cdot : R \times M \to M$ mit $r \cdot (x + y) = r \cdot x + r \cdot y$, $(r + s) \cdot x = r \cdot x + s \cdot x$ (Distributivgesetze) und $(sr) \cdot x = s \cdot (r \cdot x)$ (Assoziativitätsgesetz) für alle $r, s \in R$ und $x, y \in M$. Außerdem gelte $1 \cdot x = x$ für alle $x \in M$. Dann heißt M zusammen mit $\cdot$ ein R-Modul.

Wie bei der Multiplikation in Ringen lassen schreiben wir auch häufig rx für $r \cdot x$. Als Beispiel betrachten wir die folgenden Situationen. Jeder Vektorraum über einem Körper K ist ein K-Modul. Das Produkt von Ringen R^n (Tupel mit Einträgen aus R) bildet einen R-Modul. Abelsche Gruppen M sind $\mathbb{Z}$-Moduln.

9 Definition. Ein Homomorphismus $f : M \to N$ der R-Moduln M und N ist ein Homomorphismus der abelschen Gruppen M und N, welcher R-linear ist, für den also $f(rx) = rf(x)$ für alle $x \in M$ und $r \in R$ gilt. Die Menge der Homomorphismen von M nach N wird mit $\mathrm{Hom}_R(M, N)$ bezeichnet. Für $f, g \in \mathrm{Hom}_R(M, N)$ definieren wir $f + g \in \mathrm{Hom}_R(M, N)$ durch $(f + g)(x) = f(x) + g(x)$. Damit wird $\mathrm{Hom}_R(M, N)$ zu einer abelschen Gruppe.

Hier sind weitere Definitionen, die auf der Hand liegen: Ist $U \subseteq M$ eine Untergruppe des R-Moduls M und gilt $RU \subseteq U$, so heißt U ein Untermodul von M. Für zwei Untermoduln U, V von M ist die Summe abelscher Gruppen $U + V$ wieder ein Untermodul von M (also unter Multiplikation mit R abgeschlossen), ebenso $U \cap V$. Wie bei Vektorräumen definieren wir Linearkombination, Erzeugendensystem, endlich erzeugt, linear unabhängig über R, Basis, innere und direkte Summe, Mono-, Epi-, Iso-, Endo- und Automorphismen. Hintereinanderausführung von Abbildungen liefert einen Homomorphismus $\mathrm{Hom}_R(M, N) \times \mathrm{Hom}_R(N, P) \to \mathrm{Hom}_R(M, P)$. Die zu einem Isomorphismus inverse Abbildung ist wieder ein Isomorphismus. Sei $f \in \mathrm{Hom}_R(M, N)$. Dann sind der Kern $\ker(f)$ und das Bild $\mathrm{im}(f)$ als abelsche Gruppen wegen der R-Linearität von f Untermoduln von M bzw. N. Für einen Untermodul U von M können wir M/U als Faktorgruppe abelscher Gruppen betrachten. Wegen $RU \subseteq U$ können wir auf den Klassen vertreterweise eine Multiplikation mit R definieren, dies macht M/U zu einem R-Modul, dem Faktormodul von M nach U.

10 Definition. Der Modul M heißt frei, wenn er eine Basis besitzt.

Der Begriff „frei“ soll heißen, daß es ein Erzeugendensystem von M gibt, welches frei von nicht trivialen R-linearen Relationen ist. Nicht jeder Modul ist frei: Als Beispiel betrachte man den $\mathbb{Z}$-Modul $\mathbb{Z}/3\mathbb{Z}$. Die Moduln R^n sind frei, die Einheitsvektoren liefern eine Basis.

Ist $T \in R^{n\times n}$, M ein R-Modul und $a_1, \ldots, a_n, b_1, \ldots, b_n \in M$ mit $(a_1, \ldots, a_n)T = (b_1, \ldots, b_n)$, so ist jedes b_i eine Linearkombination der a_i und der von den b_i erzeugte Untermodul U_2 von M ist also ein Untermodul des von den a_i erzeugten Moduls U_1. Umgekehrt gilt für unimodulares T aber auch $(a_1, \ldots, a_n) = (b_1, \ldots, b_n)T^{-1}$, so daß sich jedes b_i als Linearkombination der a_i schreiben läßt und somit $U_1 = U_2$ gilt. Aus Satz 1, (ii) folgt für beliebiges T, daß $\det(T)U_1 \subseteq U_2$ ist. Sind die a_i und die b_i Basen von M, so gibt es ein unimodulares $T \in R^{n\times n}$ mit $(a_1, \ldots, a_n)T = (b_1, \ldots, b_n)$.

Moduln über Hauptidealringen

Wir verwenden jetzt die Ergebnisse über Matrizen über Hauptidealringen, um Aussagen über endlich erzeugte Moduln über Hauptidealringen zu erhalten. Im folgenden bezeichnet R immer einen Hauptidealring.

Die Hermite-Normalform läßt folgende Interpretation zu. Sei $A \in R^{n\times m}$ und M der von den Spalten von A erzeugte R-Modul in R^n. Ist $T \in R^{m\times m}$ unimodular und AT in Hermite-Normalform, so bilden die Spalten von AT zunächst ein Erzeugendensystem von M, da T unimodular ist. Wegen der Dreiecksgestalt bilden sie aber auch eine Basis von M. Die Spalten von AT können aus M schrittweise wie folgt gewonnen werden: Im j-ten Schritt betrachten wir die Untermoduln M_{i_j}, welche aus Spalten bestehen, so daß die ersten $i_j - 1$ Koordinaten Null sind, aber Einträge ungleich Null in der i_j-ten Koordinate existieren. Diese bilden ein Ideal und es gibt eine Spalte b_j, deren i_j-te Koordinate dieses Ideal erzeugt. Die i_j sollen darüberhinaus eine streng wachsende Folge bilden. Dann bilden die b_j eine Basis von M. Die Stufenelemente sind bis auf Einheiten eindeutig bestimmt, und b_j ist darüberhinaus eindeutig modulo $M_{i_{j+1}}$ bestimmt. Dies liefert im wesentlichen die Eindeutigkeitsaussage in Satz 4. Wir brauchen auch nicht anzunehmen, daß M endlich erzeugt ist. Dies ergibt sich als Konsequenz der Überlegung.

Die Smith-Normalform als Aussage über die Existenz und „diagonale“ Lage von Erzeugendensystemen von Moduln und Untermoduln gesehen werden.

11 Satz. *Sei M ein endlich erzeugter Modul über dem Hauptidealring R. Dann gibt es bis auf Einheiten eindeutig bestimmte b_i (nicht notwendigerweise*

$\neq 0$*) mit* $b_1 \mid \cdots \mid b_r$ *und*

$$M \cong R/b_1R \oplus \cdots \oplus R/b_rR.$$

Beweis. Da M endlich erzeugt ist, gibt es $n \in \mathbb{Z}^{\geq 1}$ und einen Epimorphismus $f : R^n \to M$. Der Untermodul $N = \ker(f)$ ist nach den obigen Bemerkungen bzw. Satz 4 endlich erzeugt und besitzt eine Basis w_i mit $m \leq n$ Elementen. Wir ergänzen diese Basis um $n-m$ Nullspalten zu einem Erzeugendensystem und bezeichnen die resultierende Matrix mit $A \in R^{n\times n}$. Die Einheitsvektoren e_i in R^n bilden eine Basis von M, und es gilt $(e_1, \ldots, e_n)A = (w_1, \ldots, w_n)$. Nach Satz 6 angewendet auf A erhalten wir eine andere Basis e'_i von R^n und ein anderes Erzeugendensystem w'_i von N, so daß $w'_i = b_ie'_i$ gilt. Daraus ergibt sich $M \cong R^n/N \cong R/b_1 \oplus \cdots \oplus R/b_nR$. □

Sind $a, b \in R$ teilerfremd, so gilt nach dem chinesischen Restsatz $R/Rab \cong R/Ra \oplus R/Rb$. Dies erlaubt es, die direkte Summe in Satz 11 weiter zu zerlegen, so daß die b_i nur noch Potenzen von Primelementen sind. Für $R = \mathbb{Z}$ liefert der Satz den Struktursatz über endlich erzeugte, abelsche Gruppen.

Ein R-Modul M heißt torsionsfrei, wenn für $r \in R$ und $x \in M$ aus $rx = 0$ bereits $r = 0$ oder $x = 0$ folgt.

12 Korollar. *Ein endlich erzeugter, torsionsfreier Modul M über dem Hauptidealring R ist frei.*

Beweis. Mit Satz 11 folgt, daß alle $b_i = 0$ sein müssen, also $M \cong R^n$. □