Erinnerung:

4.8.1 Satz: Sei A eine $m \times n$-Matrix über einem Hauptidealring R. Dann existieren Matrizen $U \in \mathrm{GL}_m(R)$ und $V \in \mathrm{GL}_n(R)$ sowie eine Zahl $0 \leqslant k \leqslant \min\{m,n\}$ und Elemente $e_1, \ldots, e_k \in R \smallsetminus \{0\}$ mit $e_1 | e_2 | \ldots | e_k$, so dass gilt

$$UAV = \left(\begin{array}{ccc|c} e_1 & & & \\ & \ddots & & \\ & & e_k & \\ \hline & & & \end{array}\right),$$

wobei alle nicht gezeigten Matrixkoeffizienten gleich 0 sind.

Bemerkung: Der Beweis liefert einen expliziten Algorithmus, sofern ein expliziter Algorithmus für den erweiterten euklidischen Algorithmus zur Verfügung steht.

4.8.2 Zusatz: (a) Die Zahl k ist der Rang von A als Matrix über dem Körper $\mathrm{Quot}(R)$.

(b) Für jedes $1 \leqslant \ell \leqslant k$ ist $e_1 \cdots e_\ell$ der grösste gemeinsame Teiler aller $\ell \times \ell$-Unterdeterminanten von A.

(c) Insbesondere sind sowohl k, als auch $e_1, \ldots, e_k$ bis auf Assoziiertheit, durch A eindeutig bestimmt.

4.8.3 Definition: Die Elemente $e_1, \ldots, e_k$ heissen die *Elementarteiler* von A.

Für jedes $1 \leq \ell \leq \min\{m,n\}$.

Lemma: Sei $\gamma_\ell(A)$ der ggT aller $\ell \times \ell$-Unterdeterminanten in A.

Damit: $\forall A, B$ mit Koeff. in R ist: $\gamma_\ell(A) \mid \gamma_\ell(AB)$.

$\Rightarrow \gamma_\ell(A) \mid \gamma_\ell(UAV) \mid \gamma_\ell(A)$

$\Rightarrow \gamma_\ell(A) \sim \gamma_\ell(UAV)$.

4.8.4 Folge: Für alle $n \geqslant 1$ und alle $a_1, \ldots, a_n$ in einem Hauptidealring R sind äquivalent:

(a) $\mathrm{ggT}(a_1, \ldots, a_n) \sim 1$.

(b) Es existiert eine Matrix B in $\mathrm{GL}_n(R)$ mit erster Zeile $(a_1, \ldots, a_n)$. $=: A$

Beweis: (b) $\Rightarrow \det(B) = \sum_{j=1}^{n} \underbrace{(-1)^{j-1} \cdot \det(B_j)}_{\in R} \cdot a_j$ ist ein Vielfaches von $\mathrm{ggT}(a_1, \ldots, a_n)$

$\det(B) \in R^\times$

$\Rightarrow \mathrm{ggT}(a_1, \ldots, a_n) \sim 1 \Rightarrow$ (a)

(a) $\Rightarrow$ Wende Elementarteilersatz auf A an: $UAV = (1, 0, \ldots, 0)$

1×1, $n \times n$, $U \in R^\times$

$\Rightarrow A = U^{-1} \cdot \underbrace{(1, 0, \ldots, 0)}_{\text{erste Zeile von } V^{-1}} \cdot V^{-1}$

$=$ erste Zeile von $U^{-1}V^{-1} =: B$.

qed.

4.8.5 Beispiel: Sei p ein Primelement eines Hauptidealrings R und seien $i, j \in \mathbb{Z}^{\geq 0}$ und $a \in R$. Ist $a \neq 0$, so sei k der grösste Exponent mit $p^k | a$. Dann sind die Elementarteiler der Matrix $\begin{pmatrix} p^i & a \\ 0 & p^j \end{pmatrix}$ gleich

$$(e_1, e_2) = \begin{cases} (p^i, p^j) & \text{falls } i \leqslant j \text{ und } p^i | a, \\ (p^j, p^i) & \text{falls } j \leqslant i \text{ und } p^j | a, \\ (p^k, p^{i+j-k}) & \text{falls } p^i \nmid a \text{ und } p^j \nmid a. \end{cases}$$

$i \leq k$

$j \leq k$

$k < i, j$.

Dann: $k = \mathrm{Rang}(A) = 2$. Sei $a \neq 0$

$e_1 \sim ggT(p^i, p^j, a, 0) \sim p^{\min\{i,j,k\}}$.

$e_1 \cdot e_2 \sim \det(A) = p^{i+j} \Rightarrow e_2 \sim p^{i+j-\min\{i,j,k\}}$

Bsp.: $A = \begin{pmatrix} 60 & 50 & 125 \\ 5 & 0 & 30 \end{pmatrix}$ mit $R = \mathbb{Z}$.

$\Rightarrow e_1 \sim e_2 \sim 5$.

$\rightsquigarrow k = \mathrm{Rang}(A) = 2$

$e_1 \sim ggT \sim 5$

$e_1 e_2 \sim ggT(5 \cdot 50, 50 \cdot 30, 60 \cdot 30 - 5 \cdot 125)$

$\sim 5^2 \cdot ggT(10, 12 \cdot 6 - 25) \sim 5^2$

$= 47$

4.9 Moduln

Sei R ein beliebiger kommutativer unitärer Ring

4.9.1 Definition: Ein *Modul über R* oder kurz ein *R-Modul* ist ein Tupel $(M, +, \cdot, 0)$ bestehend aus einer Menge M mit zwei Abbildungen

$$+ : \quad M \times M \to M, \quad (m, n) \mapsto m + n$$
$$\cdot : \quad R \times M \to M, \quad (x, m) \mapsto xm$$

und einem ausgezeichneten Element $0 \in M$, so dass gilt:

(a)	$(M, +, 0)$ ist eine abelsche Gruppe.	
(b)	$\forall x \in R\ \forall m, n \in M:\ x(m + n) = xm + xn$	(Linksdistributivität)
(c)	$\forall x, y \in R\ \forall m \in M:\ (x + y)m = xm + ym$	(Rechtsdistributivität)
(d)	$\forall x, y \in R\ \forall m \in M:\ x(ym) = (xy)m$	(Assoziativität)
(e)	$\forall m \in M:\ 1 \cdot m = m$	(Einselement)

4.9.2 Beispiel: Ein Modul über einem Körper K ist also einfach ein K-Vektorraum.

4.9.3 Beispiel: Jede Menge mit einem Element besitzt eine eindeutige Struktur als R-Modul und heisst dann *Nullmodul*.

4.9.4 Beispiel: Mit den Operationen $+$ und $\cdot$ von R ist R selbst ein R-Modul.

Genauso R^n.

4.9.5 Definition: Ein *Untermodul* eines R-Moduls M ist eine Teilmenge $N \subset M$ mit den Eigenschaften:

(a) $N \neq \varnothing$.

(b) $\forall n, n' \in N\colon\ n + n' \in N$.

(c) $\forall x \in R\ \forall n \in N\colon\ xn \in N$.

$\forall m \in R: \quad -1_R \cdot m = -m$

4.9.6 Proposition: Eine Teilmenge $N \subset M$ ist ein Untermodul genau dann, wenn sie zusammen mit den Restriktionen der Addition und der skalaren Multiplikation von M selbst einen R-Modul bildet.

4.9.7 Beispiel: Jeder R-Modul M hat die Untermoduln $\{0\}$ und M selbst.

4.9.8 Beispiel: Die Untermoduln von R als R-Modul sind genau die Ideale von R.

4.9.9 Proposition: Der Durchschnitt jeder nichtleeren Kollektion von Untermoduln von M ist ein Untermodul von M.

4.9.10 Proposition-Definition: Für jede Teilmenge S eines R-Moduls M existiert ein eindeutiger kleinster Untermodul $\langle S \rangle \subset M$, welcher S enthält. Dieser heisst das *Erzeugnis von S* oder *von S erzeugt*. Für endlich viele Elemente $m_1, \ldots, m_n \in M$ gilt

$$\langle \{m_1, \ldots, m_n\} \rangle \ = \ \left\{ x_1 m_1 + \ldots + x_n m_n \ \middle|\ \forall i\colon x_i \in R \right\}.$$

Ein von endlich vielen Elementen erzeugter Modul heisst *endlich erzeugt*.

4.9.11 Proposition-Definition: Die *Summe* von Untermoduln $M_1, \ldots, M_n$

$$M_1 + \ldots + M_n \;:=\; \{\, m_1 + \ldots + m_n \;\mid\; \forall i\colon m_i \in M_i \,\}$$

ist ein Untermodul. Ist die Abbildung

$$M_1 \times \ldots \times M_n \to M_1 + \ldots + M_n,\ (m_1, \ldots, m_n) \mapsto m_1 + \ldots + m_n$$

bijektiv, so heisst die Summe *direkt* oder eine *innere direkte Summe* und wird bezeichnet mit

$$M_1 \oplus \ldots \oplus M_n \;=\; \bigoplus_{i=1}^{n} M_i.$$

4.9.12 Proposition-Definition: Das kartesische Produkt von R-Moduln $M_1 \times \ldots \times M_n$ versehen mit komponentenweiser Addition und skalarer Multiplikation sowie dem Nullelement $(0, \ldots, 0)$ ist ein R-Modul. Er heisst das *(direkte) Produkt* oder, da endlich, die *äussere direkte Summe* von $M_1, \ldots, M_n$ und wird bezeichnet mit

$$M_1 \boxplus \ldots \boxplus M_n \;=\; \boxplus_{i=1}^{n} M_i.$$

Sind alle Faktoren gleich, so schreibt man auch $M^n := \boxplus_{i=1}^{n} M$.

Spezial: $R^n = \boxplus_{i=1}^{n} R$.

4.9.13 Konvention: Oft werden innere und äussere direkte Summe mit demselben Symbol $\bigoplus$ bezeichnet. Welche dann jeweils gemeint ist, muss man aus dem Zusammenhang erschliessen.

4.9.14 Definition: Eine Abbildung zwischen zwei R-Moduln $\varphi\colon M \to N$ mit

(a) $\forall m, m' \in M : \varphi(m + m') = \varphi(m) + \varphi(m')$ und

(b) $\forall m \in M\ \forall x \in R : \varphi(xm) = x \cdot \varphi(m)$

heisst *R-linear* oder ein *(R-Modul)-Homomorphismus.* Die Menge aller Homomorphismen $M \to N$ wird bezeichnet mit $\mathrm{Hom}_R(M, N)$. Ein Homomorphismus $M \to M$ heisst ein *Endomorphismus von M*, und wir schreiben $\mathrm{End}_R(M) := \mathrm{Hom}_R(M, M)$.

4.9.15 Proposition: Für jeden Homomorphismus $\varphi\colon M \to N$ gilt:

(a) $\mathrm{Kern}(\varphi) := \{m \in M \mid \varphi(m) = 0\}$ ist ein Untermodul von M.

(b) $\mathrm{Bild}(\varphi)$ ist ein Untermodul von N.

(c) φ ist injektiv genau dann, wenn $\mathrm{Kern}(\varphi) = 0$ ist.

(d) φ ist surjektiv genau dann, wenn $\mathrm{Bild}(\varphi) = N$ ist.

4.9.16 Beispiel: Die *identische Abbildung* $\mathrm{id}_M\colon M \to M$, $m \mapsto m$ ist ein Homomorphismus.

4.9.17 Proposition: Die Komposition zweier Homomorphismen ist ein Homomorphismus.

4.9.18 Proposition: Schreibe die Elemente der R-Moduln R^n und R^m als Spaltenvektoren. Dann induziert jede Matrix $A \in \mathrm{Mat}_{m\times n}(R)$ einen Homomorphismus

$$L_A\colon\ R^n \to R^m,\ m \mapsto Am.$$

Umgekehrt ist jeder Homomorphismus $R^n \to R^m$ gleich L_A für ein eindeutiges A. Weiter gilt für je zwei komponierbare Matrizen $L_{AB} = L_A \circ L_B$.

4.9.19 Definition: Ein Homomorphismus $\varphi\colon M \to N$ mit einem beidseitigem Inversen $\varphi^{-1}\colon N \to M$ heisst ein *Isomorphismus*, und wir schreiben dann $\varphi\colon M \xrightarrow{\sim} N$. Existiert ein Isomorphismus $M \xrightarrow{\sim} N$, so heissen M und N *isomorph* und wir schreiben $M \cong N$.

4.9.20 Proposition: Ein Homomorphismus ist ein Isomorphismus genau dann, wenn er bijektiv ist.

4.9.21 Proposition: Die Komposition zweier Isomorphismen ist ein Isomorphismus. Das Inverse eines Isomorphismus ist eindeutig bestimmt und selbst ein Isomorphismus. Isomorphie von R-Moduln ist eine Äquivalenzrelation.

4.9.22 Definition: Jeder zu R^n isomorphe R-Modul heisst *frei vom Rang n*.

4.9.23 Beispiel: Für jedes Ideal $(0) \subsetneq \mathfrak{a} \subsetneq R$ ist der R-Modul $R/\mathfrak{a}$ nicht frei.

Wäre $R/\mathfrak{a} \xrightarrow[\sim]{\varphi} k^n$, dann wäre $n \geq 1$

Sei $x \in R$ mit $[x] \mapsto \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$

Sei $a \in \mathfrak{a} \setminus \{0\} \Rightarrow \quad 0 = [ax] = a \cdot [x] \xmapsto{\varphi} a \cdot \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ 0 \\ \vdots \\ 0 \end{pmatrix} \neq 0 \Rightarrow$ Widerspruch! qed.

4.9.24 Definition: Ein Isomorphismus $M \xrightarrow{\sim} M$ heisst ein *Automorphismus von M*.

4.9.25 Proposition-Definition: Die Menge $\mathrm{Aut}_R(M)$ aller Automorphismen von M ist eine Gruppe bezüglich Komposition mit dem Einselement id_M, genannt die *Automorphismengruppe von M*.

4.9.26 Proposition: Für jede natürliche Zahl n haben wir einen Gruppen-Isomorphismus

$$\mathrm{GL}_n(R) \xrightarrow{\sim} \mathrm{Aut}_R(R^n),\ A \mapsto L_A.$$

4.9.27 Proposition-Definition: Sei N ein Untermodul von M. Für jedes $m \in M$ betrachte die *Nebenklasse*

$$m + N \;:=\; \{m + n \mid n \in N\} \;\subset\; M.$$

Für alle $m, m' \in M$ gilt

$$m + N = m' + N \iff m \in m' + N \iff m' \in m + N \iff (m + N) \cap (m' + N) \neq \varnothing.$$

Insbesondere ist M die disjunkte Vereinigung aller Nebenklassen von N. Die Menge aller Nebenklassen

$$M/N \;:=\; \{m + N \mid m \in M\}$$

besitzt eine eindeutige Struktur eines R-Moduls, so dass gilt:

(a) $\forall m, m' \in M : (m + N) + (m' + N) = (m + m') + N.$

(b) $\forall m \in M \; \forall x \in R : x \cdot (m + N) = xm + N.$

Für diese gilt weiter:

(c) Das Nullelement von M/N ist $0 + N = N$.

(d) Das additive Inverse jedes Elements $m + N$ ist $-(m + N) = (-m) + N$.

4.9.28 Definition: Der Modul M/N heisst der *Faktormodul von M nach N*.

4.9.29 Proposition: Die Abbildung $\pi \colon M \to M/N$, $m \mapsto m + N$ ist ein surjektiver Modulhomomorphismus mit Kern N.

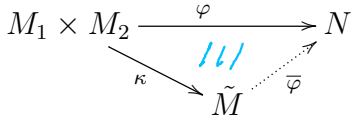
4.9.30 Homomorphiesatz: Jeder Homomorphismus $\varphi\colon M \to N$ induziert einen Isomorphismus

$$M/\operatorname{Kern}(\varphi) \xrightarrow{\sim} \operatorname{Bild}(\varphi),\ m + \operatorname{Kern}(\varphi) \mapsto \varphi(m).$$

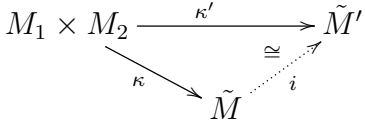
Das Tensorprodukt von R-Moduln wird genauso definiert und konstruiert wie das Tensorprodukt von Vektorräumen:

4.9.31 Definition: Ein *Tensorprodukt zweier R-Moduln M_1 und M_2* besteht aus einem R-Modul $\tilde{M}$ und einer R-bilinearen Abbildung $\kappa\colon M_1 \times M_2 \to \tilde{M}$ mit der *universellen Eigenschaft:*

Für jeden R-Modul N und jede R-bilineare Abbildung $\varphi\colon M_1 \times M_2 \to N$ existiert genau eine R-lineare Abbildung $\overline{\varphi}\colon \tilde{M} \to N$ mit $\overline{\varphi} \circ \kappa = \varphi$, das heisst, so dass das folgende Diagramm kommutiert:



4.9.32 Proposition: Ein Tensorprodukt ist eindeutig bis auf eindeutige Isomorphie, mit anderen Worten: Ist sowohl $(\tilde{M}, \kappa)$ wie $(\tilde{M}', \kappa')$ ein Tensorprodukt von M_1 und M_2, so existiert ein eindeutiger R-Modul-Isomorphismus $i\colon \tilde{M} \xrightarrow{\sim} \tilde{M}'$ mit $i \circ \kappa = \kappa'$, das heisst, so dass das folgende Diagramm kommutiert:



4.9.33 Satz: Ein Tensorprodukt existiert immer.

4.9.34 Konvention: Wir fixieren ein für alle Mal ein Tensorprodukt $(\tilde{M}, \kappa)$ und bezeichnen den Modul $\tilde{M}$ mit $M_1 \otimes_R M_2$ und die Abbildung κ mit

$$M_1 \times M_2 \to M_1 \otimes_R M_2, \ (m_1, m_2) \mapsto m_1 \otimes m_2.$$

Deren Rechenregeln sowie die Grundeigenschaften des Tensorprodukts entsprechen denen im Fall von Vektorräumen. Analog werden höhere Tensorpotenzen, symmetrische und alternierende Potenzen, sowie die Tensor-, symmetrische, bzw. äussere Algebra eines Moduls konstruiert.

Wichtig: $\mathbb{Z}$-Modul $\equiv$ abelsche Gruppe.

Bsp.: $\mathbb{Z}$ hat (minimales) Erzeugendensystem $\{1\}$, aber auch $\{2, 3\}$.

als $\mathbb{Z}$-Modul

hat maximale lin. unabh. Teilmenge $\{1\}$, aber auch $\{2\}$.