18.12.13

Repetitorium WiSe 2013/14

Lineare Algebra Teil:

Gauß-Normalform, Satz von Frobenius

Zusätze zur Teilbarkeitslehre in Integritätsbereichen

Definitionen:

$a \cdot b = b \cdot a$ d.h. $0 = a \cdot b \Rightarrow a = 0 \vee b = 0$

Integritätsbereich/Integritätsring: Ring $R \neq \{0\}$ mit 1, der kommutativ und nullteilerfrei ist.

Einheit: $a \in R$ mit $a | 1$, d.h. $\exists c \in R: ac = 1$. Def.: $R^\times = \{a \in R \mid a \text{ Einheit}\}$

Ideal: Teilmenge $I \subseteq R$, $I \neq \emptyset$, eines IB's R mit: $\forall a, b \in I \ \forall r \in R$: $a - b \in I$, $r \cdot a \in I$

Hauptideal: Ideal $I \subseteq R$, das nur von einem El. $a \in R$ erzeugt wird:

$$I = Ra = (a) := \{r \cdot a \mid r \in R\} \text{ für ein } a \in R$$

[Bem.: schreiben $(a_1, \dots, a_m) = Ra_1 + \dots + Ra_m$ für das von $a_1, \dots, a_m$ erzeugte Ideal]

Hauptidealring: Ein IB R, in dem jedes Ideal ein Hauptideal ist.

Euklidischer Ring: Ein IB R mit eukl. Fkt. $\nu: R \setminus \{0\} \to \mathbb{N}_0$,

d.h. $\forall x, y \in R, y \neq 0 \ \exists q, r \in R: x = qy + r$ mit $r = 0$ oder $\nu(r) < \nu(y)$ ["Div. mit Rest"]

irreduzibles Element: $q \in R \setminus R^\times$: $\forall a, b \in R: q = ab \Rightarrow a \in R^\times \vee b \in R^\times$

Primelement: $p \in R \setminus R^\times$ (R ein IB), $p \neq 0$, $\forall a, b \in R: p | ab \Rightarrow p | a \vee p | b$

faktorieller Ring: IB R, in dem jedes El. $a \neq 0$ eine bis auf Assoziiertheit und Reihenfolge eind. best. Zerlegung in irreduzible Elemente besitzt.

Beispiele:

Integritätsbereich: $\mathbb{Z}$, Polynomring $k[X]$ für Körper k, $\mathbb{Z}[X]$, $k[X,Y]$, ...

nicht: $\mathbb{Z}/6$ da $\bar{2} \cdot \bar{3} = \bar{0}$ $\Rightarrow \exists$ Nullteiler

Ideal: $(2) = 2 \cdot \mathbb{Z} = \{a \in \mathbb{Z}; 2 | a\} \subseteq \mathbb{Z}$

Hauptideal: "

Hauptidealring: $\mathbb{Z}$, $k[X]$ für Körper k, aber nicht: $\mathbb{Z}[X]$, $k[X,Y]$ [Ideal (X,Y) ist kein Hauptideal]

Euklidischer Ring: $\mathbb{Z}$, $k[X]$ für Körper k: eukl. Fkt. ist Polynomgrad

irreduzibles Element: $2 \in \mathbb{Z}$

Primelement: $2 \in \mathbb{Z}$

faktorieller Ring: $\mathbb{Z}$, $k[X]$ für Körper k

Bem.: $d = ggT(a_1, \ldots, a_n)$, falls $(d) = (a_1, \ldots, a_n) := Ra_1 + \ldots + Ra_n$ [d eind. bis auf Assoziiertheit]
Haben: $d = ggT(ggT(a_1, \ldots, a_{n-1}), a_n)$. Zur ggT-Bestimmung kann dann der euklidische Algorithmus eingesetzt werden, vgl. Termin7_LA

Sätze:
(1) $a \in R$ prim $\Rightarrow a$ irreduzibel [Sonst $a = b \cdot c$ mit $b, c \notin R^\times \cup \{0\} \overset{a \text{ prim}}{\Rightarrow} a | b \vee a | c \Rightarrow c \in R^\times \vee b \in R^\times$ ↯]
(2) Sei R ein IB, in dem jedes El. $\neq 0$ eine Zerl. in irreduz. El. besitzt. Dann: Zerl. in irred. El. ist eindeutig bestimmt [bis auf Assoziiertheit/Reihenfolge]
$\Leftrightarrow$ jedes irred. El. ist auch Primelement.
(3) Ein IB R ist faktoriell genau dann, wenn eine der folgenden Bed. erfüllt ist:
(a) Jede aufsteigende Kette von Hauptidealen bricht ab,
d.h. $(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \ldots \Rightarrow \exists n_0 \, \forall n \geq n_0 : (a_n) = (a_{n_0})$.
(b) jedes irred. El. ist auch Primelement.
(4) Jeder Hauptidealring ist faktoriell [wegen (3)(a)]
(5) Jeder euklidische Ring ist Hauptidealring.
} Beispiele zu $\not\Leftarrow$ werden nicht behandelt

Def.: Für $A \in K^{n \times n}$ heißt $M_A(X) = X I_n - A \in K[X]^{n \times n}$ die charakteristische Matrix zu A.

Satz von Frobenius: Für $A, B \in K^{n \times n}$ gilt: A ähnlich zu B (d.h. $A = S^{-1} B S$)
$\Leftrightarrow M_A(X)$ äquivalent zu $M_B(X)$ über $K[X]$ (d.h. $M_A(X) = U^{-1} M_B(X) V$ für $U, V \in K[X]^{n \times n}$).

Weiter hatten wir in Termin5_LA, S.-3- gesehen:
Jede Matrix $A \in K^{m \times n}$ ist zu $\left(\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right)$ äquivalent, $r = \operatorname{rg} A$, $I_r \in K^{r \times r}$ Einheitsmatrix, diese Form kann durch elementare Zeilen- und Spaltenumformungen erreicht werden.
Eine Verallgemeinerung davon ist der folgende Satz:

Gaußsche Normalform für euklidische Ringe:

Vor.: R eukl. Ring, $C \in R^{n \times n}$.

Beh.: • C äquivalent zu Diagonalmatrix $\operatorname{diag}(c_1, \dots, c_n) = \begin{pmatrix} c_1 & & 0 \\ & c_2 & \\ 0 & & \ddots \, c_n \end{pmatrix}$,
für die $\boxed{c_i \mid c_{i+1}}$ für alle $i = 1, \dots, n-1$ gilt.

• Die c_i sind eindeutig bis auf Assoziiertheit,
d.h. bis auf Multiplikation mit einer Einheit $\in R^\times$.

• Diese Gauß-Normalform läßt sich durch wiederholte Anwendung elementarer Zeilen- und Spaltenumformungen (Addition des r-fachen einer Zeile/Spalte zu einer anderen Zeile/Spalte) sowie Vertauschen zweier Zeilen/Spalten aus A erreichen.

Def.: Die $c_i(A) = c_i$, $i = 1, \dots, n$, heißen Invariantenteiler von A.

"Die" Ringelemente $d_j(A) := ggT(\det(A_{IJ});\ \# I = j = \# J)$, mit $I, J \subseteq \{1, \dots, n\}$, wo A_{IJ} die Submatrix von A ist, die aus den Zeilen mit Nr. $\in I$ und Spalten mit Nr. $\in J$ gebildet wird, heißen auch Determinantenteiler von A. [Eind. bis auf Assoziiertheit, daher "die"..]

Offenbar ist $d_1(A) = ggT(a_{ij},\ 1 \le i,j \le n)$, $d_n(A) = \det A$.

Eigenschaften: • $d_j(A) \mid d_j(AB)$ und $d_j(A) \mid d_j(BA)$

• Sind $A, B \in R^{n \times n}$ äquivalent, so ist $d_j(A) = d_j(B)$

• $d_{j-1}(A) \mid d_j(A)$

• Für eine Diagonalmatrix gilt: $d_1 = c_1$, $d_2 = c_1 c_2$, $d_3 = c_1 c_2 c_3, \dots,$
$d_n = c_1 c_2 \cdots c_n$

Satz: Für die Invarianten- und Determinantenteiler von $A \in R^{n \times n}$, R euklidischer Ring, gilt: • $A \underset{\text{äquivalent}}{\sim} B \iff c_i(A) = \varepsilon c_i(B)$ für alle i, ein $\varepsilon \in R^\times$
$\iff d_i(A) = \mu d_i(B)$ für alle i, ein $\mu \in R^\times$

• $\varepsilon_1 c_i = d_i d_{i-1}^{-1}$, $\quad \varepsilon_2 d_i = \prod_{j=1}^{i} c_j$ mit gewissen $\varepsilon_1, \varepsilon_2 \in R^\times$.