Einführung in die Algebra

Vorlesung im
Sommersemester 2006
Technische Universität Berlin

gehalten von
Prof. Dr. M. Pohst

Contents

CHAPTER 2

Ringe

1. Definition

Eine nicht leere Menge R mit zwei inneren Verknüpfungen $+$ (Addition), $\cdot$ (Multiplikation) heißt Ring $(R, +, \cdot)$, falls folgende drei Bedingungen erfüllt sind.

(1) $(R, +)$ ist abelsche Gruppe;
(2) $(R, \cdot)$ ist eine Halbgruppe;
(3) es gelten die Distributivgesetze:

$$\begin{aligned} x \cdot (y + z) &= (x \cdot y) + (y \cdot z), \\ (x + y) \cdot z &= (x \cdot z) + (y \cdot z) \quad \forall x,\, y,\, z \in R. \end{aligned}$$

Überdies heißt R kommutativ, falls $x \cdot y = y \cdot x \ \forall x,\, y \in R$ gilt. R heißt Ring mit Eins, falls $(R, \cdot)$ Monoid ist.

Bemerkung:
Statt $(R, x, \cdot)$ schreibt man oft kürzer R, statt $x \cdot y$ einfach $x\,y$. Vereinbarungsgemäß geht "Punktrechnung vor Strichrechnung". Das neutrale Element bzgl. $+$ wird als 0 geschrieben. Ein Einselement ist, falls es existiert, stets eindeutig bestimmt.

Beispiel:

(1) $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sind kommutative Ringe mit Eins, jedoch auch $R = \{0\}$ (pathologischer Ring).
(2) $(\mathbb{Z}/n\mathbb{Z})$ ist kommutativer Ring mit Eins $(n \in \mathbb{N})$.
(3) Die Endomorphismen eines Vektorraums V bilden einen Ring mit Einselement id. Dieser ist für $\dim V \geq 2$ nicht kommutativ.
(4) $R^{n \times n}$ ist Matrizenring über R.

1.1. Rechenregeln für Ringe. Für $x,\, y \in R$ gilt (vergleiche Lineare Algebra I):

(1) $0\,x = x\,0 = 0$,
(2) $(-x)\,y = -(x\,y) = x\,(-y)$,
(3) $(-x)\,(-y) = x\,y$,
(4) $(\mathbb{Z},\, R) \to R \ : \ (m,\, x) \mapsto mx = \underbrace{x + \ldots + x}_{m\text{-mal}}$,

$\mathbb{Z}$ operiert auf jedem Ring mittels $(n, x) \mapsto nx$.

Statt $x + (-y)$ schreibt man $x - y$.
Allgemein gilt für $x_i,\ y_j \in R$ $(1 \leq i \leq n,\ 1 \leq j \leq m,\ n,\ m \in \mathbb{N})$:

$$x_1 + \ldots + x_n = \sum_{i=1}^{n} x_i; \qquad x_1 \cdot \ldots \cdot x_n = \prod_{i=1}^{n} x_i;$$

leere Summe := 0; leeres Produkt := 1, falls $1 \in R$;

$$\begin{aligned}
\left(\sum_{i=1}^{n} x_i\right)\left(\sum_{j=1}^{m} y_j\right) &= \sum_{i=1}^{n}\sum_{j=1}^{m} x_i y_j, \\
x^n &= \prod_{i=1}^{n} x, \\
x^{n+m} &= x^n \cdot x^m, \\
(x^n)^m = x^{nm}, & \\
(x+y)^n &= \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y_i
\end{aligned}$$

in kommutativen Ringen mit 1.

2. Definition

Eine Teilmenge S von $(R, +, \cdot)$ heißt Teilring (Unterring) von R, falls $(S, +, \cdot)$ selbst Ring ist. In diesem Fall heißt R Oberring (Erweiterungsring) von S.

3. Hilfssatz

R sei Ring und $\emptyset \neq S \subseteq R$. Dann sind äquivalent:

(1) S Teilring von R,
(2) $SS \subseteq S$ und $S + (-S) \subseteq S$.

Beweis:
(i) $\Rightarrow$ (ii): Klar. Beachte

$$\begin{aligned}
SS &= \{xy \mid x \in S,\ y \in S\}, \\
S + (-S) &= \{x - y \mid x,\ y \in S\}.
\end{aligned}$$

(ii) $\Rightarrow$ (i):

$$\begin{aligned}
S + (-S) \subseteq S &\Rightarrow (S, +) \text{ Gruppe}, \\
SS \subseteq S &\Rightarrow (S, \cdot) \text{ Halbgruppe},
\end{aligned}$$

denn die Rechenregeln übertragen sich von R.

□

Beispiele:

(1) Für $n \in \mathbb{N}$ ist $n\mathbb{Z}$ Unterring von $\mathbb{Z}$.
(2) Die Diagonalmatrizen bilden einen Unterring von $R^{n\times n}$.

Bemerkung: Der Durchschnitt von Teilringen ist Teilring!

Wichtiger als Teilringe sind jedoch Ideale, die in gewisser Weise den Normalteilern in der Gruppentheorie entsprechen!

4. Definition

Es sei R ein Ring. $\mathfrak{a} \subseteq R$ heißt Linksideal (bzw. Rechtsideal) von R, falls gilt:

(1) $\mathfrak{a}$ ist Untergruppe von $(R, +)$, d.h. $\mathfrak{a} \neq \emptyset$ und $\mathfrak{a} + (-\mathfrak{a}) \subseteq \mathfrak{a}$.
(2) $\forall a \in \mathfrak{a} \ \forall x \in R \ : \ x\,a \in \mathfrak{a}$ (bzw. $ax \in \mathfrak{a}$), d.h. $R\,\mathfrak{a} \subseteq \mathfrak{a}$ (bzw. $\mathfrak{a} \supseteq \mathfrak{a}\,R$).

$\mathfrak{a} \subseteq R$ heißt Ideal, falls $\mathfrak{a}$ sowohl Links- als auch Rechtsideal ist.

Bemerkung:

(1) $\{0\}$, R sind stets Ideale von R; Ideale sind Teilringe (Umkehrung i.a. falsch: $\mathbb{Z} \subset \mathbb{Q}$)j für $R \ni 1$ und $1 \in \mathfrak{a}$ für ein Links- oder Rechtsideal $\mathfrak{a}$ von R folgt sofort $\mathfrak{a} = R$.
(2) Der Durchschnitt von (Links- bzw. Rechts-) Idealen ist wieder eins. Zu $A \subseteq R$ existiert folglich ein kleinstes Ideal, welches A umfaßt, das sogenannte von A erzeugte Ideal (A).

Beispiel:
Es sei $\mathfrak{a}$ ein Ideal von $\mathbb{Z}$. Wegen $\mathfrak{a} \neq \emptyset$ und $(-\mathfrak{a}) \subseteq \mathfrak{a}$ gilt entweder $\mathfrak{a} = \{0\}$, oder $\mathfrak{a}$ enthält eine kleinste natürliche Zahl m. Gemäß Division mit Rest gilt, daß m alle Zahlen von $\mathfrak{a}$ teilt. Also ist $\mathfrak{a} = \mathbb{Z}m = m\mathbb{Z}$.

5. Hilfssatz

Es sei $\emptyset \neq A \subseteq R$, R Ring. Dann besteht (A) aus allen endlichen Summen von Elementen der Form

$$n\,a,\ x\,a,\ a\,y,\ x\,a\,y \text{ mit } a \in A,\ x, y \in R,\ n \in \mathbb{Z}.$$

Beweis:

(1) Jedes Ideal $\mathfrak{a}$ mit $A \subseteq \mathfrak{a}$ enthält alle in (2.5) angegebenen Elemente.
(2) Die Menge der in (2.5) angegebenen Elemente ist ein Ideal.

□

6. Korollar

Es sei R ein Ring und $\emptyset \neq A \subseteq R$. Dann gilt:

(1) $(A) = \left\{ \sum_{\text{endl.}} x_i \cdot a_i \cdot y_i \;\middle|\; x_i,\, y_i \in R,\ a_i \in A \right\}$ für $R \ni 1$;

(2) $(A) = \left\{ \sum_{\text{endl.}} x_i \cdot a_i + \sum_{\text{endl.}} m_j \cdot b_j \;\middle|\; x_i \in R,\ m_j \in \mathbb{Z},\ a_i, b_j \in A \right\}$ für R kommutativ;

(3) $(A) = \left\{ \sum_{\text{endl.}} x_i \cdot a_i \;\middle|\; x_i \in R,\ a_i \in A \right\}$ für R kommutativ mit Eins.

Beweis: Unmittelbar klar nach (2.5)!

7. Definition

Ein Ideal $\mathfrak{a}$ eines Ringes R heißt Hauptideal, falls $\mathfrak{a} = (a)$ für $a \in R$ gilt. $\mathfrak{a}$ heißt endlich erzeugbar, falls $\mathfrak{a} = (A)$ mit $\sharp A < \infty$ gilt.

Beispiel:
Alle Ideale in $\mathbb{Z}$ sind Hauptideale.

Bemerkungen:

(1) R kommutativ $\Rightarrow\ (a) = Ra + \mathbb{Z}a$;
(2) R kommutativ mit Eins $\Rightarrow\ (a) = Ra$;
(3) R kommutativ ohne Eins: In $R = 2\mathbb{Z}$ ist $(2) = 4\mathbb{Z} + \mathbb{Z}2 = 2\mathbb{Z}$ von $2R = 4\mathbb{Z}$ verschieden;
(4) $R \ni 1\ \Rightarrow\ (1) = R$.

Arithmetik von Idealen:

8. Definition

Die Summe zweier (Links- bzw. Rechts-) Ideale $\mathfrak{a}_1$, $\mathfrak{a}_2$ ist definiert durch:

$$\mathfrak{a}_1 + \mathfrak{a}_2 = \{a_1 + a_2 \mid a_1 \in \mathfrak{a}_1,\ a_2 \in \mathfrak{a}_2\}.$$

Bemerkung:
Die Summe endlich vieler (Links- bzw. Rechts-) Ideale ist wieder eins.
Der Durchschnitt von Idealen ist wieder ein Ideal. Es gelten:

$$\mathfrak{a}_i \subseteq \mathfrak{a}_i + \ldots + \mathfrak{a}_n\ (1 \le i \le n), \quad \mathfrak{a}_i + \mathfrak{a}_i = \mathfrak{a}_i, \quad (A_1) + (A_2) = (A_1 \cup A_2).$$

Beispiel:
$R = \mathbb{Z}$:
$Ra + Rb = \{xa + yb \mid x, y \in \mathbb{Z}\} = c\mathbb{Z}$ mit $c = \mathrm{ggT}\,(a, b)$,
$Ra \cap Rb = d\mathbb{Z}$ mit $d = \mathrm{kgV}\,(a, b)$.

9. Definition

Das Produkt zweier (Links- bzw. Rechts-) Ideale $\mathfrak{a}_1$, $\mathfrak{a}_2$ ist definiert durch:

$$\mathfrak{a}_1 \cdot \mathfrak{a}_2 = \left\{ \sum_{\text{endl.}} a_{1i}\, a_{2i} \,|\, a_{1i} \in \mathfrak{a}_1,\ a_{2i} \in \mathfrak{a}_2 \right\}.$$

Bemerkung:

Das Produkt endlich vieler (Links- bzw. Rechts-) Ideale ist wieder eins. Es gelten die Rechenregeln:

$$\mathfrak{a}_1\,(\mathfrak{a}_2\mathfrak{a}_3) = (\mathfrak{a}_1\mathfrak{a}_2)\,\mathfrak{a}_3, \quad \mathfrak{a}_1\,(\mathfrak{a}_2 + \mathfrak{a}_3) = \mathfrak{a}_1\mathfrak{a}_2 + \mathfrak{a}_1\mathfrak{a}_3.$$

Ist R kommutativ, so gilt $\mathfrak{a}_1\mathfrak{a}_2 = \mathfrak{a}_2\mathfrak{a}_1$. Sind $\mathfrak{a}_1$, $\mathfrak{a}_2$ Linksideale, so gilt $\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}_2$; sind $\mathfrak{a}_1$, $\mathfrak{a}_2$ Rechtsideale, so gilt $\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}_1$, $(A_1)\,(A_2) = (A_1A_2)$ für R kommutativ.

Ist R kommutativer Ring mit Eins und sind a, $b \in R$, so gilt

(1) $(a) + (b) = \{xa + yb \,|\, x,\, y \in R\} = Ra + Rb$.
(2) $(a)\,(b) = (ab)$, $Ra\,Rb = R\,(Ra)\,b = Rab$.
(3) $\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) \supseteq \mathfrak{a} \cap \mathfrak{b} + \mathfrak{a} \cap \mathfrak{c}$ mit Gleichheit für $\mathfrak{a} \supseteq \mathfrak{b} \vee \mathfrak{a} \supseteq \mathfrak{c}$.
(4) für $\mathfrak{a} + \mathfrak{b} = R$ ist $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$.

Beweis:

(1) klar.
(2) klar.
(3) $x \in \mathfrak{a} \cap \mathfrak{b},\ y \in \mathfrak{a} \cap \mathfrak{c} \ \Rightarrow\ x + y \in \mathfrak{a}, x + y \in \mathfrak{b} + \mathfrak{c}$.
Gilt oBdA $\mathfrak{a} \supseteq \mathfrak{b}$, so ist für $x \in \mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c})$ zunächst $x = b + c$ mit $b \in \mathfrak{b},\ c \in \mathfrak{c}$.
Wegen $\mathfrak{a} \supseteq \mathfrak{b}$ ist auch $b \in \mathfrak{a}$ und damit $c \in \mathfrak{a}$, also $b \in \mathfrak{a} \cap \mathfrak{b},\ c \in \mathfrak{a} \cap \mathfrak{c}$.
(4) Es ist

$$\begin{aligned}(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) &= \mathfrak{a}(\mathfrak{a} \cap \mathfrak{b}) + \mathfrak{b}(\mathfrak{a} \cap \mathfrak{b}) \subseteq \mathfrak{a}\mathfrak{b} \\ &\subseteq \mathfrak{a} \cap \mathfrak{b},\end{aligned}$$

also $(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) \subseteq \mathfrak{a}\mathfrak{b}$;
für $\mathfrak{a} + \mathfrak{b} = R$ gilt offenbar Gleichheit.

□

Bemerkung:
Ein Beispiel für $\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) \supset \mathfrak{a} \cap \mathfrak{b} + \mathfrak{a} \cap \mathfrak{c}$ wird im Anschluß an die Einführung von Polynomringen behandelt.

10. Satz

Es sei R ein Ring mit Ideal $\mathfrak{a}$. Dann läßt sich $R/\mathfrak{a}$ mittels

$$(x + \mathfrak{a}) + (y + \mathfrak{a}) =: (x + y) + \mathfrak{a}, (x + \mathfrak{a})(y + \mathfrak{a}) := xy + \mathfrak{a} \quad \forall x, y \in R$$

zu einem Ring machen, dem Faktorring $R/\mathfrak{a}$ oder Restklassenring R modulo $\mathfrak{a}$.

Beweis:
Zunächst ist $(\mathfrak{a}, +)$ additive Untergruppe von $(R, +)$, also $R/\mathfrak{a}$ eine additive Gruppe (vergleiche (1.17)). Wir zeigen: $(R/\mathfrak{a}, \cdot)$ ist Halbgruppe. Zunächst ist $\cdot$ innnere Verknüpfung. Dazu ist die Wohldefiniertheit nachzuweisen. Für

$$x + \mathfrak{a} = \tilde{x} + \mathfrak{a},\ y + \mathfrak{a} = \tilde{y} + \mathfrak{a} \quad \text{folgt} \quad x - \tilde{x},\ y - \tilde{y} \in \mathfrak{a}$$

und somit

$$xy - \tilde{x}\tilde{y} = (x - \tilde{x})\, y + \tilde{x}\,(y - \tilde{y}) \ \in \mathfrak{a},$$

da $\mathfrak{a}$ zweiseitiges Ideal ist. Also folgt $xy + \mathfrak{a} = \tilde{x}\tilde{y} + \mathfrak{a}$. Das Assoziativgesetz bzgl. $\cdot$ überträgt sich von R. Das gleiche gilt für die die Distributivgesetze, da ja vertreterweise mit den Idealklassen gerechnet wird.

□

Bemerkung:

(1) Für $1 \in R$ ist $1 + \mathfrak{a}$ Einselement von $R/\mathfrak{a}$. R kommutativ $\Rightarrow$ $R/\mathfrak{a}$ kommutativ.

(2) Für $x - y \in \mathfrak{a}$ schreibt man $x \equiv y$ modulo $\mathfrak{a}$ ("kongruent"). Hierfür gelten die Regeln:

$$\left.\begin{array}{l} x \equiv y \text{ modulo } \mathfrak{a} \\ u \equiv v \text{ modulo } \mathfrak{a} \end{array}\right\} \Rightarrow x \overset{+}{\underset{\bullet}{}} u \equiv y \overset{+}{\underset{\bullet}{}} v \text{ modulo } \mathfrak{a}.$$

Für $R = \mathbb{Z}$ bedeutet die alte Schreibweise $x \equiv y \bmod n$ gerade $x \equiv y$ modulo $n\mathbb{Z}$, denn sämtliche Ideale von $\mathbb{Z}$ waren ja als Hauptideale nachgewiesen. Die spezielle Äquivalenzrelation $\equiv$ heißt Kongruenzrelation.

11. Definition

Es seien R, S zwei Ringe. Unter einem Ringhomorphismus von R nach S versteht man eine Abbildung $f : R \to S$ mit

$$f(x+y) = f(x) + f(y),\ f(x \cdot y) = f(x) \cdot f(y) \quad \forall x, y \in R.$$

Bemerkung:

(1) Für Ringhomomorphismen $f : R \to S$ ist $\operatorname{Im} f = f(R)$ Unterring von S, $\ker f = f^{-1}(0)$ Ideal in R.
(2) Ist R ein Ring mit Ideal $\mathfrak{a}$, so ist $p : R \to R/\mathfrak{a} : x \mapsto x + \mathfrak{a}$ ein Ringepimorphismus, der sog. kanonische Epimorphismus. Es ist $\ker p = \mathfrak{a}$.

12. Hilfssatz

Eine Teilmenge $\mathfrak{a}$ eines Ringes R ist genau dann ein Ideal, wenn $\mathfrak{a}$ Kern eines Ringhomomorphismus ist.

13. Hilfssatz

Es seien R, S Ringe und $f : R \to S$ ein Ringhomomorphismus. Dann gilt:

(1) Ist $\mathfrak{b}$ ein Ideal in S, so ist $f^{-1}(\mathfrak{b})$ Ideal in R, $f^{-1}(\mathfrak{b}) \supseteq \ker f$.
(2) Ist $\mathfrak{a}$ Ideal in R und f surjektiv, so ist $f(\mathfrak{a})$ Ideal in S.

Beweis:
Gemäß (1.16) gelten die Aussagen bzgl. $+$.

(1) Es sei $s = f(r) \in \mathfrak{b}$ und $x \in R$. Dann ist
$$f(xr) = f(x)\, f(r) \ \in \mathfrak{b},$$
also mit r auch $xr \in f^{-1}(\mathfrak{b})$.
(2) Es sei $y = f(x)$ mit $x \in \mathfrak{a}$ und $z \in S$. Dann ist $z = f(r)$ für ein $r \in R$ und somit
$$zy = f(r)\, f(x) = f(rx) \ \in f(\mathfrak{a}).$$

□

14. Satz

Es seien R, S zwei Ringe.

(1) (Homomorphiesatz)
Ist $f : R \to S$ ein Ringhomomorphismus, dann gilt
$$R/\ker\varphi \cong \varphi(R).$$

(2) (Erster Isomorphiesatz)
Ist U Unterring und $\mathfrak{a}$ Ideal von R, so gilt
$$(U+\mathfrak{a})/\mathfrak{a} \cong U/U\cap\mathfrak{a}.$$

(3) (Zweiter Isomorphiesatz)
Für Ideale $\mathfrak{a}$, $\mathfrak{b}$ von R mit $\mathfrak{a}\subseteq\mathfrak{b}$ ist $\mathfrak{b}/\mathfrak{a}$ Ideal von $R/\mathfrak{a}$, und es gilt
$$(R/\mathfrak{a})/(\mathfrak{b}/\mathfrak{a}) \cong R/\mathfrak{b}.$$

Beweis: Siehe Übungsblatt 6.

15. Hilfssatz

Es sei $\mathfrak{a}$ ein Ideal des Ringes R. Die Mengen
$$I(\mathfrak{a}) := \{\mathfrak{b} \mid \mathfrak{b} \text{ Ideal von } R \text{ mit } \mathfrak{b}\supseteq\mathfrak{a}\}$$
und
$$J(\mathfrak{a}) := \{\overline{\mathfrak{b}} \mid \overline{\mathfrak{b}} \text{ Ideal von } R\backslash\mathfrak{a}\}$$
werden dann mittels $\psi : I(\mathfrak{a}) \to J(\mathfrak{a}) : \mathfrak{b}\mapsto\mathfrak{b}/\mathfrak{a}$ bijektiv aufeinander abgebildet.

Beweis:
Nach (2.14)(iii) ist ψ eine Abbildung von $I(\mathfrak{a})$ in $J(\mathfrak{a})$. Für
$$\psi(\mathfrak{b}_1)=\psi(\mathfrak{b}_2) \quad \text{folgt} \quad \mathfrak{b}_1=\mathfrak{b}_1+\mathfrak{a}=\mathfrak{b}_2+\mathfrak{a}=\mathfrak{b}_2,$$
also ist ψ injektiv. Ist schließlich $\overline{\mathfrak{b}}$ Ideal von $J(\mathfrak{a})$, so ist $p^{-1}(\overline{\mathfrak{b}})$ ein Ideal von R, welches $\mathfrak{a}$ umfaßt, also in $I(\mathfrak{a})$ liegt. Hierfür gilt $\psi(p^{-1}(\overline{\mathfrak{b}})) = \overline{\mathfrak{b}}$ nach Konstruktion.

□

16. Definition

Es sei R ein Ring. $0\neq a\in R$ heißt linker (rechter) Nullteiler, falls $b\in R$ mit $ab=0$ ($ba=0$) für ein $0\neq b\in R$ existiert. $x\in R$ heißt nilpotent, falls $m\in\mathbb{N}$ mit $x^m=0$ existiert. Für $1\in R$ heißt $e\in R$ Einheit (invertierbar), falls e in R ein Linksinverses und ein Rechtsinverses besitzt. $U(R)=R^\times$ bezeichnet die Menge der Einheiten von R.

Bemerkung:

(1) e Einheit $\Rightarrow$ e^{-1} existiert eindeutig.
Sei

$$ae = eb = 1 \quad \Rightarrow \quad a = a \cdot 1 = a\,(eb) = (ae)\,b = 1 \cdot b = b.$$

Für $ae = ea = 1$ und $be = eb = 1$ folgt

$$a = a \cdot 1 = a\,(eb) = (ae)\,b = 1 \cdot b = b.$$

(Vergleiche Gruppentheorie)

(2) Die Elemente von R, welche keine Nullteiler sind, bilden eine Halbgruppe. Es seien a, b keine Nullteiler; ist dann $x \in R$ mit $abx = 0$ so folgt

$$a\,(bx) = 0 \quad \Rightarrow \quad bx = 0 \quad \Rightarrow \quad x = 0.$$

(3) Einheiten sind keine Nullteiler und bilden folglich eine multiplikative Untergruppe von R.

$$e \in R^\times,\ x \in R:\ ex = 0 \quad \Rightarrow \quad e^{-1}ex = 0 \quad \Rightarrow \quad 1 \cdot x = x = 0.$$

Beispiele:
Bestimme Einheiten, Nullteiler und nilpotente Elemente in $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}$, $K^{n\times m}$, $R = \{0\}$.

(1) $0 \neq x \in R$ nilpotent $\Rightarrow$ x Nullteiler.
$0 = x^m = \left(x^{m-1}\right) x = x \left(x^{m-1}\right)$, wähle m minimal!

(2) $\mathbb{Z}/12\mathbb{Z} = \{\,\overline{i} \mid 0 \leq i \leq 11\}$
$\overline{j}^{\,m} \stackrel{?}{=} \overline{0} \ \Rightarrow\ j^m \equiv 0 \bmod 12\ (12 = 4 \cdot 3) \ \Rightarrow\ j = 0 \vee 6$
Nilpotente Elemente: $\overline{0}$, $\overline{6}$
Nullteiler: $\overline{6}$, $\overline{2}$, $\overline{4}$, $\overline{8}$, $\overline{10}$, $\overline{3}$, $\overline{9}$
Einheiten: $\overline{1}$, $\overline{5}$, $\overline{7}$, $\overline{11}$ $(\overline{1} = \overline{5}^2 = \overline{7}^2 = \overline{11}^2)$

(3) $R = \mathbb{Z}$
Nilpotente Elemente: 0,
Nullteiler: keine,
Einheiten: ± 1.

(4) $K^{n\times n}$
Nilpotente Elemente sind z.B. alle oberen $\triangle$-Matrizen mit 0-Diagonale,
Nullteiler: alle singulären Matrizen,
Einheiten: $\mathrm{GL}\,(n,\, K)$.

17. Definition

Ein Ring R mit $1 \neq 0$ heißt Schiefkörper, falls $R^\times = R\backslash\{0\}$ ist. Ist R kommutativ, so heißt R Körper.

18. Hilfssatz

Ein Ring R ist genau dann ein Schiefkörper, wenn $(R\backslash\{0\}, \cdot)$ Gruppe ist.

Beweis:
$\Rightarrow$: per Definition

$\Leftarrow$:
$R\backslash\{0\}$ enthält Eins e mit $0e = e0 = 0$. Also ist $R^\times = R\backslash\{0\}$.

□

Beispiele:

(1) Körper: $\mathbb{Q}$, $\mathbb{R}$, $(\mathbb{Z}/n\mathbb{Z})$ mit $n \in \mathbb{P}$.
(2) Schiefkörper: $\mathbb{R}+\mathbb{R}i+\mathbb{R}j+\mathbb{R}k$ Quaternionen (als $\mathbb{R}$-Vektorraum)

Bemerkung:

(1) R Ring mit Eins, $\mathfrak{a}$ Ideal von R mit $\mathfrak{a} \cap R^\times \neq \emptyset$. Dann ist $\mathfrak{a} = R$; denn zu $a \in \mathfrak{a} \cap R^\times$ existiert $a^{-1} \in R$ und $a^{-1}a \in R\mathfrak{a} = \mathfrak{a}$, also $1 \in \mathfrak{a}$ und $R = R\,1 \subseteq \mathfrak{a}$.
(2) Ein Schiefkörper R enthält nur die Ideale $\{0\}$ und R.
(3) Ist K ein Schiefkörper und $\varphi : K \to R$ ein Ringhomomorphismus, so ist $\varphi = \mathcal{O}$ oder φ injektiv.
(4) Es gibt keine endlichen Schiefkörper! (ohne Beweis)

19. Hilfssatz

(1) Es sei R ein Ring. Ist $a \in R$ kein Nullteiler, so gilt:

$$ax = ay \;\Rightarrow\; x = y; \quad xa = ya \;\Rightarrow\; x = y \quad \forall x, y \in R.$$

(2) Ein endlicher nullteilerfreier Ring $R \neq \{0\}$ ist ein Schiefkörper.

Beweis:

(1) $a\,(x - y) = 0 \;\Rightarrow\; x - y = 0 \;\Rightarrow\; x = y$; $\quad (x - y)\,a = 0 \;\Rightarrow\; x - y = 0 \;\Rightarrow\; x = y$.
(2) Zeige: $(R\backslash\{0\}, \cdot)$ ist Gruppe.

Für $x \in R$, $x \neq 0$, betrachte $\varphi_x : R\backslash\{0\} \to R\backslash\{0\}$: $a \mapsto xa$. φ_x ist injektiv (nach (i)), also wegen R endlich auch surjektiv. Dasselbe gilt für $\psi_x : a \mapsto ax$. Zu $a, b \in R\backslash\{0\}$ existieren folglich eindeutig $x, y \in R\backslash\{0\}$ mit $b = ax = ya$. Gemäß (1.5) ist $R^\times = R\backslash\{0\}$ Gruppe.

□

20. Definition

Es sei R ein Ring mit $1 \neq 0$. Existiert dann eine kleinste natürliche Zahl n mit $n\,1 = 0$, so heißt n die Charakteristik $\chi(R)$ von R. Existiert kein solches n, setzt man die Charakteristik $\chi(R)$ zu 0 fest.

Beispiele:
$\chi(\mathbb{Z}) = 0,\ \chi(\mathbb{Z}/n\mathbb{Z}) = n.$

21. Satz

Die Charakteristik eines nullteilerfreien unitären ($R \ni 1 \neq 0$) Rings R ist 0 oder eine Primzahl p. Im letzten Fall gilt $px = 0\ \forall x \in R$, sowie $kx = R(k,\, p)\, x$.

Beweis:
Es sei R Ring mit $\chi(R) \neq 0$ und $n \in \mathbb{N}$ die kleinste natürliche Zahl mit $n1 = 0$, also speziell $n \geq 2$. Ist n keine Primzahl, so gilt $n = pq$ mit $p,\, q \in \mathbb{Z}^{\geq 1},\ p < n,\ q < n$ und somit

$$0 = n1 = pq1 = (p1)\,(q1).$$

Da R nullteilerfrei ist, erhält man $p1 = 0$ oder $q1 = 0$ im Widerspruch zur Minimalität von n. Nunmehr ist $0 = n1$, also auch

$$nx = n\,(1x) = (n1)\,x = 0x = 0 \quad \forall x \in R.$$

□

Bemerkung:
Der Durchschnitt von Schiefkörpern ist wieder einer. Also enthält jeder Schiefkörper einen kleinsten Teilkörper, den sogenannten Primkörper.

22. Satz

Der Primkörper eines Schiefkörper K ist isomorph zu $\mathbb{Q}$ (für $\chi(K) = 0$) oder zu $\mathbb{Z}/Lp\mathbb{Z}$ für eine Primzahl p (für $\chi(K) = p$).

Beweis:
In K gilt $1 \neq 0$. Der Primkörper von K umfaßt daher alle Elemente der Form $m1$ ($m \in \mathbb{Z}$). Für $\chi(K) = 0$ sind diese alle ungleich 0 für $m \neq 0$. Also existiert $(m1)^{-1}$ und damit $(m1)\,(n1)^{-1}$ im Primkörper. Setze

$$P := \{(m1)\,(n1)^{-1} \mid m \in \mathbb{Z},\ n \in \mathbb{Z},\ n \neq 0\}.$$

Es gilt:

$$(m1)\,(n1)^{-1} = (n1)^{-1}(m1) \text{ wegen } (n1)\,(m1) = (m1)\,(n1) = (mn)\,1,$$
$$(mn1)^{-1} = (m1)^{-1}(n1)^{-1}.$$

Also ist P Körper, der im Primkörper enthalten ist, folglich gleich dem Primkörper.

$$\varphi\ :\ \mathbb{Q} \to P\ :\ \frac{m}{n} \mapsto (m1)\,(n1)^{-1}$$

ist dann ein Ringisomorphismus.

Für $\chi(K) = p,\ p$ Primzahl, ist $p1 = 0$. Für $x = k1\ (1 \leq k < p)$ existiert (Euklidischer Algorithmus in $\mathbb{Z}$) ein $l \in \mathbb{Z}$ mit $k \cdot l \equiv 1 \bmod p$, also $(k1)(l1) = 1$ in K. Setze

$$P := \{k1 \mid 0 \leq k < p,\ k \in \mathbb{Z}\}.$$

Dies ist bereits der Primkörper von K.

$$\varphi : (\mathbb{Z}/p\mathbb{Z}) \to P : k + p\mathbb{Z} \mapsto k1$$

ist Ringisomorphismus! (φ ist wohldefiniert wegen $(k + pm)1 = k1 + p1m1 = k1$.)

□

Wie bei Gruppen kann man für Ringe äußere Produkte (Summen) erklären.

Sind $R_1, \ldots, R_n$ Ringe, so wird $R_1 \times \ldots \times R_n =: \prod_{i=1}^{n} R_i = R$ zu einem Ring mittels

$$\begin{aligned}(x_1, \ldots, x_n) + (y_1, \ldots, y_n) &= (x_1 + x_2, \ldots, x_n + y_n),\\ (x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) &= (x_1 y_1, \ldots, x_n y_n).\end{aligned}$$

(Vergleiche Eigenschaften bei Gruppen, speziell ist $\varepsilon_i(R_i) = (0, \ldots, 0, R_i, 0, \ldots, 0)$ Ideal von R. Schreibweise: $R_1 \oplus \ldots \oplus R_n$.)

Ist andererseits R ein Ring mit Idealen $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$, so heißt R (innere) direkte Summe von $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$, falls

$$R = \mathfrak{a}_1 + \ldots + \mathfrak{a}_n \quad \text{und} \quad R\mathfrak{a}_i \cap \sum_{\substack{j=1\\ j\neq i}}^{n} \mathfrak{a}_j = \{0\}$$

ist (vgl. (1.23)). (Schreibweise: $R = \mathfrak{a}_1 \dot{+} \ldots \dot{+} \mathfrak{a}_n$)

Ein Element $e \in R$ mit $e \neq 0$ und $e^2 = e$ heißt Idempotente von R. Zwei Idempotente $e,\ f$ heißen orthogonal, falls $ef = fe = 0$ ist.

Beispiel:

$R = \mathbb{Z}/6\mathbb{Z}$. Es gilt: $R = <3 + 6\mathbb{Z}> \dot{+} <4 + 6\mathbb{Z}>$.

Hierin sind $e_1 = 3 + 6\mathbb{Z}$ und $e_2 = 4 + 6\mathbb{Z}$ Idempotente. Wir haben hier eine Zerlegung der Eins in orthogonale Idempotente: $1 + 6\mathbb{Z} = (3 + 6\mathbb{Z}) + (4 + 6\mathbb{Z})$.

Bemerkung:

Ringe R mit $1 \in R$ haben mit einer Idempotenten $e \neq 1$ stets eine weitere: $1 - e$. Es gilt

$$\begin{aligned}1 &= e + (1 - e),\\ (1 - e)^2 &= 1^2 - 1 \cdot e - 1 \cdot e + e^2\\ &= 1 - e - e + e\\ &= 1 - e.\end{aligned}$$

$1-e$ und e sind orthogonale Idempotente wegen

$$e\,(1-e) = e - e^2 = 0 = (1-e)\,e.$$

Somit gilt

$$R = R\,1 = R\,(e + (1-e))\& \subseteq \&R\,e \dot{+} R\,(1-e).\& \subseteq \&R$$

, also überall Gleichheit.

Beachte: Orthogonale Idempotente sind Nullteiler.

Es sei R ein kommutativer Ring mit $1 \neq 0$. Zwei Ideale $\mathfrak{a}$, $\mathfrak{b}$ von R mit $\mathfrak{a} + \mathfrak{b} = R$ heißen komaximal. Speziell existieren $e \in \mathfrak{a}$, $f \in \mathfrak{b}$ mit $e + f = 1$. (Allerdings wird nicht gefordert, daß e, f orthogonale Idempotente sind.)

Beispiel: $R = \mathbb{Z},\ m, n \in \mathbb{Z}$ teilerfremd $\Rightarrow\ m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$ und $mu + nv = 1$ für passende $u,\ v \in \mathbb{Z}$.

23. Hilfssatz

Es sei R ein kommutativer Ring mit $1 \neq 0$. Dann gilt für Ideale $\mathfrak{a}, \mathfrak{a}_1, \ldots, \mathfrak{a}_n, \mathfrak{b}_1, \ldots, \mathfrak{b}_n$ mit $\mathfrak{a}_i + \mathfrak{a}_j = R (\mathfrak{a}_i,\ \mathfrak{a}_j$ komaxial$)(1 \leq i < j \leq n),\ \mathfrak{a} + \mathfrak{b}_i = R\ (1 \leq i \leq n)$:

(1) $\mathfrak{a} + \mathfrak{b}_1 \cdot \ldots \cdot \mathfrak{b}_n = R$,
(2) $\mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n = \mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n$.

Beweis:

(1)

$$\begin{aligned} R &= R^n \\ &= \prod_{i=1}^{n} (\mathfrak{a} + \mathfrak{b}_i) \qquad \text{(wegen } 1 \in R\text{)} \\ &= \mathfrak{a}\,(\mathfrak{a}^{n-1} + \ldots) + \mathfrak{b}_1 \cdot \ldots \cdot \mathfrak{b}_n \qquad (R \text{ kommutativ}) \\ &\subseteq \mathfrak{a} + \mathfrak{b}_1 \cdot \ldots \cdot \mathfrak{b}_n \\ &\subseteq R, \end{aligned}$$

also muß überall Gleichheit gelten.

(2) Beweis per Induktion über n.

$n = 1$: Klar.

$n = 2$: vgl. Beweis zu Bem. (iv) auf Seite 45.

$n \to n+1$:

$$\begin{aligned} \mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_{n+1} &= (\mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n)\,\mathfrak{a}_{n+1} \\ &\overset{(*)}{=} (\mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n) \cap \mathfrak{a}_{n+1} \\ &\overset{\text{Ind. Vor.}}{=} \bigcap_{i=1}^{n+1} \mathfrak{a}_i \end{aligned}$$

$(*)$: Per Induktionsvoraussetzung für $n = 2$ und (i).

24. Chinesischer Restsatz

Es sei R ein kommutativer Ring mit 1. Dann gilt für paarweise komaximale Ideale $\mathfrak{a}_i$ $(1 \leq i \leq n)$ (d.h. $\mathfrak{a}_i + \mathfrak{a}_j = R$ $(1 \leq i < j \leq n)$):

$$R/\mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n \cong \prod_{i=1}^{n} R/\mathfrak{a}_i$$

Lösung simultaner Kongruenzen:

Suche alle x mit

$$\begin{aligned} x &\equiv 2 \bmod 5, \quad \mathfrak{a}_1 = 5\mathbb{Z} \\ x &\equiv 4 \bmod 11, \quad \mathfrak{a}_2 = 11\mathbb{Z} \\ x &\equiv 7 \bmod 12, \quad \mathfrak{a}_3 = 12\mathbb{Z} \end{aligned}$$

oder "ewiger Kalender".

Beweis:
Betrachte Abbildung

$$\phi : R \to \prod_{i=1}^{n} R/\mathfrak{a}_i \ : \ x \mapsto (x + \mathfrak{a}_1, \ldots, x + \mathfrak{a}_n).$$

Offensichtlich ist ϕ ein Ringhomomorphismus mit $\ker \phi = \mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n = \mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n$. Es bleibt "$\phi$ surjektiv" zu zeigen, dann folgt die Behauptung aus dem Homomorphiesatz für Ringe (2.14)(i). Nach Voraussetzung existieren $e_{ij} \in \mathfrak{a}_i$, $e_{ji} \in \mathfrak{a}_j$ mit $1 = e_{ij} + e_{ji}$ $(1 \leq i < j \leq n)$. Setze

$$\tilde{e}_i := \prod_{\substack{j=1 \\ j \neq i}}^{n} e_{ji} \quad (1 \leq i \leq n).$$

$$\tilde{e}_i \equiv \begin{cases} 0 \bmod \mathfrak{a}_j \\ 1 \bmod \mathfrak{a}_i \quad (j \neq i). \end{cases}$$

Ist dann $(x_1 + \mathfrak{a}_1, \ldots, x_n + \mathfrak{a}_n) \in \prod_{i=1}^{n} R/\mathfrak{a}_i$ vorgelegt, so ist dies Bild von $x = \sum_{i=1}^{n} x_i \tilde{e}_i$. Denn für $\tilde{e}_i$ gilt $\tilde{e}_i \in \mathfrak{a}_j$ $(1 \leq j \leq n,\, j \neq i)$,

$$\tilde{e}_i \equiv \begin{cases} 1 \bmod \mathfrak{a}_i \\ 0 \bmod \mathfrak{a}_j \quad (j \neq i) \end{cases}.$$

□

$$R/(\mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n) \ = \ \dot{+}_{i=1}^{n} \Big(R/(\mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n)\Big)\tilde{e}_i \ \cong \ R/\mathfrak{a}_1 \oplus \ldots \ \oplus R/\mathfrak{a}_n.$$

Bemerkung:
Der Satz sagt aus, daß sich simultane Kongruenzen nach komaximalen Idealen stets lösen lassen. Er beschreibt die Lösungsmenge und gibt sogar ein (konstruktives) Verfahren zu ihrer Bestimmung an.

("Zerlegung der Eins in orthogonale Idempotente").

Newton-Verfahren

Eine explizite Berechnung des Urbildes von $(x_1 + \mathfrak{a}_1, \cdots, x_n + \mathfrak{a}_n)$ ist allerdings schneller möglich mit dem folgenden Verfahren, welches der Newton-Interpolation ähnelt.
Setze

$$e_i := \prod_{j=1}^{i-1} e_{ji} \quad (1 < i \leq n)$$

ähnlich zum Beweis sowie $y_1 = x_1$ und iterativ $y_{k+1} = y_k + (x_{k+1} - y_k)e_{k+1} \quad (1 \leq k < n)$.

Dann leistet $x = y_n$ das Gewünschte.

Beispiel:
Löse $x \equiv 2 \bmod 5,\ x \equiv 4 \bmod 11,\ x \equiv 7 \bmod 12$.
1. Lösungmöglichkeit: Raten.
2. Lösungmöglichkeit: per (2.38)!
$\mathfrak{a}_1 = 5\mathbb{Z},\ \mathfrak{a}_2 = 11\mathbb{Z},\ \mathfrak{a}_3 = 12\mathbb{Z},\ R = \mathbb{Z}$.
$\mathfrak{a}_i + \mathfrak{a}_j = R,\ e_{ij} + f_{ij} = 1$ mit $e_{ij} \in \mathfrak{a}_i$ und $f_{ij} \in \mathfrak{a}_j$.

i	1	1	2	2	3	3
j	2	3	1	3	1	2
e_{ij}	-10	25	11	-11	-24	12
f_{ij}	11	-24	-10	12	25	-11

,

$$\begin{array}{rcccl} \tilde{e}_1 & = & f_{12}\, f_{13} & = & -264 \\ \tilde{e}_2 & = & f_{21}\, f_{23} & = & -120 \\ \tilde{e}_3 & = & f_{31}\, f_{32} & = & -75 \end{array} .$$

Gesucht sind u, v mit $u \cdot 5 + v \cdot 11 = 1 \ \Rightarrow\ 1 = -2 \cdot 5 + (+11) = 5 \cdot 5 - 2 \cdot 12 = -11 + 12$.

$$\begin{aligned} x &= x_1\tilde{e}_1 + x_2\tilde{e}_2 + x_3\tilde{e}_3 \\ &= -2 \cdot 264 - 4 \cdot 120 - 7 \cdot 275 \\ &= -528 - 480 - 1925 \\ &= -2933; \end{aligned}$$

das Ergebnis ist modulo $5 \cdot 11 \cdot 12 = 660$ eindeutig, also ist die kleinste positive Lösung 367, die betraglich kleinste Lösung -293.
Gesamtlösung ist $367 + 660\mathbb{Z}$.

Nach dem Newton Verfahren verläuft die Berechnung wie folgt:
$e_1 = 1, e_2 = -10, e_3 = -275$,
$y_1 = 2, y_2 = 2 + (4 - 2)(-10) = -18$,
$y_3 = -18 + (7 - (-18))(-275) = -6893 \equiv -293 \bmod 660$.

25. Definition

Es sei M eine nicht leere Menge. Eine Relation $\leq$ auf M heißt Halbordnung, falls die Bedingungen

(1) $x \leq x$
(2) $x \leq y \wedge y \leq x \;\Rightarrow\; x = y$
(3) $x \leq y \wedge y \leq z \;\Rightarrow\; x \leq z$

$\forall x,\, y,\, z \in M$ erfüllt sind.

Beispiele:

(1) $(\mathbb{Z}, \geq 0)$, $(\mathbb{R}, \geq 0)$, lexikographische Ordung im $\mathbb{R}^n$;
(2) $(\mathbb{C}, |\ |)$ erfüllt (i), (iii) aber nicht (ii);
(3) $\mathfrak{P}(M)$ mit $\subseteq$:
$M = \{1, 2\}$ hat $\mathfrak{P}(M) = \{\emptyset, \{1\}, \{2\}, M\}$.
$\emptyset \subseteq \{1\} \subseteq M$, $\emptyset \subseteq \{2\} \subseteq M$. $\{1\}$ ist in $\{2\}$ nicht enthalten.

26. Definition

Es sei M eine nicht leere Menge. Eine Halbordung $\leq$ auf M heißt Ordnung, falls für alle $x,\, y \in M$ stets $x \leq y$ oder $y \leq x$ gilt. In diesem Fall heißt M Kette.

Beispiel:
$(\mathbb{R}, \geq)$, nicht aber $(\mathbb{C}, |\ |)$.

27. Definition

Es sei $M \neq \emptyset$ und $\leq$ eine Halbordnung auf M. Für $A \subseteq M$ heißt $s(A) \in M$ obere Schranke von A, falls $x \leq s(A)\ \forall a \in A$ gilt. Für $A \subseteq M$ heißt $m(A) \in A$ maximales Element von A, falls aus $a \in A$ und $m(A) \leq a$ stets $a = m(A)$ folgt. Eine Teilmenge X von M heißt induktiv geordnet, falls jede Kette in X eine obere Schranke in X (!) besitzt.

Beispiel:
$A = \{\{1\}, \{2\}, \emptyset\} \subseteq \mathfrak{P}(\{1, 2\})$;
Es ist $s(A) = \{1, 2\}$; sowohl $\{1\}$ als auch $\{2\}$ sind maximale Elemente von A.

28. Zornsches Lemma

Jede nicht leere induktiv geordnete Menge besitzt ein maximales Element.

29. Definition

Es sei R Ring mit Ideal $\mathfrak{a}$. $\mathfrak{a}$ heißt maximal, falls es kein Ideal $\mathfrak{b}$ mit $\mathfrak{a} \subset \mathfrak{b} \subset R$ gibt.

30. Satz

Es sei V ein Vektorraum über dem Körper K und $M \subseteq V$ linear unabhängig. Dann existiert eine Basis B von V mit $M \subseteq B$.

Beweis:

Es bestehe $Q \subseteq P(V)$ aus allen linear unabhängigen Teilmengen von V, die M enthalten. Wegen $M \in Q$ folgt $Q \neq \emptyset$. Ist K eine Kette in Q, so gilt

$$m(K) := \bigcup_{N \in K} N \ \in Q.$$

Denn sind $x_1, \ldots, x_n \in m(K)$, d.h. $x_i \in N_i \ (1 \leq i \leq n)$, so existiert ein maximaler Index j, mit $x_i \in N_j \ (1 \leq i \leq n)$, also sind $x_1, \ldots, x_n$ linear unabhängig.

Nach dem Zornschen Lemma existiert in Q ein maximales Element B. Nach Voraussetzung ist B linear unabhängig. Es bleibt $[B] = V$ zu zeigen.

Ist $x \in V \backslash [B]$, so gilt speziell $x \neq 0$, und $\tilde{B} := B \cup \{x\}$ ist linear abhängig. Also existieren $x_1, \ldots, x_r \in B$ und $\lambda_1, \ldots, \lambda_r, \ \lambda \in K$, nicht alle 0, mit

$$\sum_{i=1}^{r} \lambda_i x_i + \lambda\, x = 0.$$

Für $\lambda \neq 0$ folgt $x \in [B]$. Für $\lambda = 0$ folgt B linear abhängig. Widerspruch!

□

Bemerkung:

Also folgt die Behauptung. Für $M = \emptyset$ liefert dies die Existenz einer Basis von V.

31. Satz

Es sei R ein Ring mit $1 \neq 0$ und $\mathfrak{a} \neq R$ ein Ideal von R. Dann ist $\mathfrak{a}$ in einem maximalen Ideal $\mathfrak{m}$ von R enthalten.

Bemerkung:

Für $\mathfrak{a} = \{0\}$ liefert dies die Existenz maximaler Ideale (in Ringen R mit Eins).

Beweis:

Es sei $\mathfrak{M}$ die Menge aller Ideale $\mathfrak{b}$ von R mit $R \supset \mathfrak{b} \supseteq \mathfrak{a}$, dann ist $\mathfrak{M} \neq \emptyset$ induktiv geordnet bzgl. $\subseteq$. (Die Vereinigungsmenge einer aufsteigenden Kette von Idealen ist wieder ein Ideal, welches in unserem Fall 1 nicht enthält.)

Nach dem Zornschen Lemma existiert ein maximales Element $\mathfrak{m}$ aus $\mathfrak{M}$. Wegen $1 \notin \mathfrak{m}$ ist $\mathfrak{m}$ maximales Ideal.

□

Bemerkung:

(1) In $\mathbb{Z}$ sind $p\mathbb{Z}$, p Primzahl, genau die maximalen Ideale.
(2) Ist R Körper, so ist $\{0\}$ einziges maximales Ideal.

32. Satz

Es sei R ein Ring mit Ideal $\mathfrak{m}$. Dann gilt:

(1) $\mathfrak{m} \neq R$ ist maximal $\Leftrightarrow$ $R/\mathfrak{m}$ enthält nur die Ideale $\mathfrak{m}$ und $R/\mathfrak{m}$.
(2) Ist R kommutativ mit $1 \neq 0$, so ist $\mathfrak{m}$ genau dann maximal, falls $R/\mathfrak{m}$ Körper ist.

Beweis:

(1) Gemäß (2.15).
(2)

$$\begin{aligned} R/\mathfrak{m} \text{ Körper} &\Leftrightarrow \forall x \in R\backslash\mathfrak{m},\ \exists\, \lambda \in R :\ (x+\mathfrak{m})\,(\lambda+\mathfrak{m}) = 1+\mathfrak{m} \\ &\Leftrightarrow \forall x \in R\backslash\mathfrak{m},\ \exists \lambda \in R :\ \lambda x \equiv 1 \bmod \mathfrak{m} \\ &\Leftrightarrow \forall x \in R\backslash\mathfrak{m},\ \exists m \in \mathfrak{m},\ \exists \lambda \in R :\ \lambda x + m = 1 \\ &\Leftrightarrow Rx + \mathfrak{m} = R\ \ \forall x \in R\backslash\mathfrak{m} \\ &\Leftrightarrow \mathfrak{m} \text{ maximal.} \end{aligned}$$

□

33. Definition

Ein kommutativer Ring R mit Eins heißt lokaler Ring, falls R genau ein maximales Ideal besitzt.

34. Hilfssatz

R kommutativ mit 1. R lokaler Ring $\Leftrightarrow$ $R\backslash R^\times$ ist Ideal in R.

Beweis:
"$\Leftarrow$":
Jedes Ideal $\mathfrak{a}$ in R mit $\mathfrak{a} \neq R$ beteht aus Nichteinheiten.

"$\Rightarrow$":
Für $x \in R,\ x \notin U(R)$, folgt $Rx = (x) \subseteq \mathfrak{m}$ für ein passendes maximales Ideal $\mathfrak{m}$ von R.

□

Beispiel:
$\dfrac{\mathbb{Z}}{\mathbb{Z}\backslash p\mathbb{Z}} = \left\{ \dfrac{r}{s} \in \mathbb{Q} \,\middle|\, r \in \mathbb{Z},\ p \nmid s \right\}$ ist lokaler Ring mit $\mathfrak{m} = \dfrac{p\mathbb{Z}}{\mathbb{Z}\backslash p\mathbb{Z}}$.

Quotientenbildung bei kommutativen Ringen R. Es sei R ein kommutativer Ring und $S \subseteq R$ eine multiplikative Halbgruppe. Als "Brüche" (mit Nennern in S) definiert man die Menge $R \times S$ der geordneten Paare $(r,\, s)$. Wie bei der Konstruktion der rationalen aus den ganzen Zahlen bildet man auf $R \times S$ eine Äquivalenzrelation, deren Klassen dann die gewünschten Brüche bilden. Wegen der möglichen Existenz von Nullteilern muß man allgemeiner

$$(r,\, s) \sim (\tilde{r},\, \tilde{s}) \quad :\Leftrightarrow \quad \exists t \in S \,:\, t\,(r\tilde{s} - \tilde{r}s) = 0 \text{ definieren.}$$

Dies ist tatsächlich eine Äquivalenzrelation, denn Reflexivität und Symmetrie sind klar und bzgl. der Transitivität bemerken wir:

$$\begin{aligned}
&(r_1,\, s_1) \sim (r_2,\, s_2) \,\wedge\, (r_2,\, s_2) \sim (r_3,\, s_3)\\
&\Leftrightarrow\ \exists t_1,\, t_2 \in S \,:\, t_1\,(r_1 s_2 - r_2 s_1) = 0 = t_2\,(r_2 s_3 - r_3 s_2)\\
&\Rightarrow\ \exists t_1,\, t_2 \in S \,:\quad 0 \;=\; t_1 t_2 s_3\,(r_1 s_2 - r_2 s_1) + t_1 t_2 s_1\,(r_2 s_3 - r_3 s_2)\\
&\qquad\qquad\qquad\quad\;\; =\; t_1 t_2 s_2\,(s_3 r_1 - s_1 r_3)\\
&\qquad\qquad\qquad\quad\;\; =\; t\,(s_3 r_1 - s_1 r_3) \ \text{ für } \ t = t_1 t_2 s_2\\
&\Rightarrow\ \exists t \in S \,:\, t\,(s_3 r_1 - s_1 r_3) = 0\\
&\Leftrightarrow\ (r_1,\, s_1) \sim (r_3,\, s_3).
\end{aligned}$$

Die Äquivalenzklassen bilden Brüche:

$$K_{r,s} := \{(\tilde{r},\, \tilde{s}) \in R \times S \,|\, (r,\, s) \sim (\tilde{r},\, \tilde{s})\} =: \frac{r}{s}.$$

Setze

$$\begin{aligned}
K_{r_1,s_1} + K_{r_2,s_2} &= K_{r_1 s_2 + r_2 s_1,\, s_1 s_2},\\
K_{r_1,s_1} \cdot K_{r_2,s_2} &= K_{r_1 s_1,\, r_2 s_2}.
\end{aligned}$$

(Für die Äquivalenzklassen $\frac{r_1}{s_1}$, $\frac{r_2}{s_2}$ von $(r_1,\, s_1)$, $(r_2,\, s_2) \in R \times S$ definieren wir eine Addition und eine Multiplikation über die Vertreter:

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} := \frac{r_1 s_2 + r_2 s_1}{s_1 s_2}, \quad \frac{r_1}{s_1} \cdot \frac{r_2}{s_2} := \frac{r_1 r_2}{s_1 s_2}.)$$

Zur Multiplikation: Sind auch $(\tilde{r}_1,\, \tilde{s}_1) \in \frac{r_1}{s_1}$, $(\tilde{r}_2,\, \tilde{s}_2) \in \frac{r_2}{s_2}$, so ist $(r_1 r_2,\, s_1 s_2) \sim (\tilde{r}_1 \tilde{r}_2,\, \tilde{s}_1 \tilde{s}_2)$ wegen

$$\begin{aligned}
&(r_1,\, s_1) \sim (\tilde{r}_1,\, \tilde{s}_1) \,\wedge\, (r_2,\, s_2) \sim (\tilde{r}_2,\, \tilde{s}_2)\\
&\Leftrightarrow\ \exists t_1,\, t_2 \in S \,:\, t_1\,(r_1 \tilde{s}_1 - \tilde{r}_1 s_1) = 0 = t_2\,(r_2 \tilde{s}_2 - s_2 \tilde{r}_2)\\
&\Rightarrow\ \exists t_1,\, t_2 \in S \,:\, 0 = t_1 t_2\,(r_1 r_2 \tilde{s}_1 \tilde{s}_2 - \tilde{r}_1 r_2 s_1 \tilde{s}_2) + t_1 t_2\,(\tilde{r}_1 r_2 s_1 \tilde{s}_2 - \tilde{r}_1 \tilde{r}_2 s_1 s_2)\\
&\Rightarrow\ \exists t_1 t_2 \in S \,:\, 0 = t_1 t_2\,(r_1 r_2 \tilde{s}_1 \tilde{s}_2 - \tilde{r}_1 \tilde{r}_2 s_1 s_2)\\
&\Leftrightarrow\ (r_1 r_2,\, s_1 s_2) \sim (\tilde{r}_1 \tilde{r}_2,\, \tilde{s}_1 \tilde{s}_2);
\end{aligned}$$

für die Addition folgert man aus

$$\begin{aligned}
&\exists t_1,\, t_2 \in S \,:\, 0 = t_1\,(r_1 \tilde{s}_1 - \tilde{r}_1 s_1) = t_2\,(r_2 \tilde{s}_2 - s_2 \tilde{r}_2)\\
&\Rightarrow\ \exists t_1,\, t_2 \in S \,:\, 0 = t_1 t_2\,(r_1 \tilde{s}_1 s_2 \tilde{s}_2 - \tilde{r}_1 s_1 s_2 \tilde{s}_2 + r_2 \tilde{s}_2 s_1 \tilde{s}_1 - s_2 \tilde{r}_2 s_1 \tilde{s}_1)\\
&\Rightarrow\ \exists t_1,\, t_2 \in S \,:\, 0 = t_1 t_2\,((r_1 s_2 + r_2 s_1)\,\tilde{s}_1 \tilde{s}_2 - (\tilde{r}_1 \tilde{s}_2 + \tilde{r}_2 \tilde{s}_1)\,s_1 s_2)\\
&\Leftrightarrow\ (r_1 s_2 + r_2 s_1,\, s_1 s_2) \sim (\tilde{r}_1 \tilde{s}_2 + \tilde{r}_2 \tilde{s}_1,\, \tilde{s}_1 \tilde{s}_2).
\end{aligned}$$

Die Rechengesetze von R übertragen sich über die Vertreter auf

$$R_S := \left\{ \frac{r}{s} \mid r \in R,\ s \in S \right\} \quad \text{für} \quad \frac{r}{s} = K_{r,s}.$$

Hierfür sind die Assoziativität von Addition und Multiplikation nachzurechnen. Neues Nullelement ist $K_{0,s}$, inverses Element zu $K_{r,s}$ ist $K_{-r,s}$.

Folglich bildet R_S einen kommutativen Ring mit Einselement $\frac{s}{s}$:

$$\frac{r}{s} \cdot \frac{s}{s} = \frac{r}{s} \quad \forall \frac{r}{s} \in R_S.$$

R läßt sich homomorph in R_S abbilden mittels

$$\iota \ :\ R \to R_S \ :\ r \mapsto \frac{rs}{s}$$

für ein beliebiges $s \in S$.

Im Fall, daß $S \neq 0$ keine Nullteiler enthält, ist ι sogar Monomorphismus, also Einbettung, d.h. R_S läßt sich als Ringerweiterung von R auffassen.

Spezialfälle:

(1) $S \ni 0 \ \Rightarrow\ R_S$ ist trivial.
(2) $\emptyset \neq S$ besteht aus allen Nicht-Nullteilern $\neq 0$ von R. In diesem Fall heißt R_S der (vollständige) Quotientenring $\mathfrak{Q}(R)$ von R. Sind speziell alle Elemente $\neq 0$ keine Nullteiler, so ist $\mathfrak{Q}(R)$ ein Körper.

Beispiel:

(1) $R = \mathbb{Z},\ S = \mathbb{Z}\backslash\{0\} \ \Rightarrow\ R_S \cong \mathbb{Q}$.
(2) $R = \mathbb{Z},\ S = \{2^\nu \mid \nu \in \mathbb{Z}^{\geq 0}\} \ \Rightarrow\ R_S = \{\frac{a}{2^\nu} \mid \nu \in \mathbb{Z}^{\geq 0}\}$.
(3) $R = \mathbb{Z},\ S = \mathbb{Z}\backslash p\mathbb{Z} \quad (p \in \mathbb{P}) \ \Rightarrow\ R_S = \mathbb{Z}_{(p)}$ ("p-Lokalisierung von $\mathbb{Z}$").

35. Definition

Es sei R ein kommutativer Ring. Ein Ideal $R \supsetneq \mathfrak{p}$ von R heißt Primideal, falls für $a,\ b \in R$ mit $ab \in \mathfrak{p}$ stets $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$ folgt.

Beispiele:

(1) $R = \mathbb{Z}$, alle Primideale sind von der Form $p\mathbb{Z}$ mit p Primzahl.
(2) $\{0\}$ ist Primideal, falls R keine Nullteiler $\neq 0$ besitzt.

36. Satz (Charakterisierung von Primidealen)

Es sei R ein kommutativer Ring und $\mathfrak{a} \subsetneq R$ ein Ideal in R. Dann sind äquivalent:

(1) $\mathfrak{a}$ Primideal,
(2) $\forall a,\ b \in R$ mit $a \notin \mathfrak{a}$ und $b \notin \mathfrak{a} \ \Rightarrow\ ab \notin \mathfrak{a}$,
(3) Für Ideale $\mathfrak{b}, \mathfrak{c}$ von R mit $\mathfrak{bc} \subseteq \mathfrak{a}$ folgt $\mathfrak{b} \subseteq \mathfrak{a}$ oder $\mathfrak{c} \subseteq \mathfrak{a}$.

(4) $R\backslash\mathfrak{a}$ ist multiplikative Halbgruppe,
(5) $R/\mathfrak{a}$ ist nullteilerfrei.

Beweis:
(i) $\Rightarrow$ (ii): nach Definition;

(ii) $\Rightarrow$ (iii): Wäre die Aussage falsch, existierten Elemente $b \in \mathfrak{b} \setminus \mathfrak{a},\ c \in \mathfrak{c} \setminus \mathfrak{a}$ mit $b \cdot c \in \mathfrak{a}$ im Widerspruch zur Voraussetzung.

(iii) $\Rightarrow$ (iv): Sind $a, b \in R \setminus \mathfrak{a}$, so folgt $(a) = Ra + \mathbb{Z}a$, $(b) = Rb + \mathbb{Z}b$, $(a)(b) = Rab + \mathbb{Z}ab = (ab)$. Wegen $(a) \not\subseteq \mathfrak{a}$ und $(b) \not\subseteq \mathfrak{a}$ muss $(ab) \not\subseteq \mathfrak{a}$ gelten, also $ab \notin \mathfrak{a}$.

(iv) $\Rightarrow$ (v): für $a+\mathfrak{a}$, $b+\mathfrak{a}$, beide ungleich $\mathfrak{a}$, folgt $a,\ b \in R\backslash\mathfrak{a}$, damit $ab \in R\backslash\mathfrak{a}$ und

$$(a + \mathfrak{a})\,(b + \mathfrak{a}) = ab + \mathfrak{a} \neq \mathfrak{a};$$

(v) $\Rightarrow$ (i): es seien $a,\ b \in R$ mit $ab \in \mathfrak{a}$, also

$$\mathfrak{a} = ab + \mathfrak{a} = (a + \mathfrak{a})\,(b + \mathfrak{a})$$

und folglich $(a + \mathfrak{a} = \mathfrak{a} \ \Leftrightarrow\ a \in \mathfrak{a})$ oder $(b + \mathfrak{a} = \mathfrak{a} \ \Leftrightarrow\ b \in \mathfrak{a})$.

□

Bemerkung:

(1) In einem kommutativen Ring mit 1 ist jedes maximale Ideal ein Primideal, also ist jedes Ideal $\mathfrak{a} \subset R$ von R in einem Primideal enthalten.
(2) In einem kommutativen Ring R mit Primideal $\mathfrak{p}$ bildet $R\backslash\mathfrak{p}$ eine multiplikative Halbgruppe S. Dann heißt

$$R_S = R_{R\backslash\mathfrak{p}} = \frac{R}{R\backslash\mathfrak{p}} =: R_{\mathfrak{p}}$$

Lokalisierung von R bei $\mathfrak{p}$. $R_{\mathfrak{p}}$ ist ein lokaler Ring (siehe Übungsblatt 7).

(Falls $R \ni 1\ :\ R \to \frac{R}{R\backslash\mathfrak{p}}\ :\ r \mapsto \frac{r}{1}$ ist Ringmonomorphismus.)

Speziell: $R = \mathbb{Z},\ \mathfrak{p} = p\mathbb{Z}$ für $p \in \mathbb{P}$:

$$R_{(p)} = \left\{ \frac{m}{n} \,\middle|\, m \in \mathbb{Z},\ n \in \mathbb{Z} \text{ mit } p \nmid n \right\}.$$

(3) 0 Primideal $\Rightarrow$ R nullteilerfrei.
(4) $R \ni 1$, $\mathfrak{p}$ Primideal, $R/\mathfrak{p}$ nullteilerfrei:
$R/\mathfrak{p}$ endlich $\Rightarrow$ $R/\mathfrak{p}$ Körper
$\overset{2.29}{\Rightarrow}$ $\mathfrak{p}$ maximales Ideal.

Beispiele:

(1) $\mathfrak{p} = 2\mathbb{Z} \ \Rightarrow\ R_{\mathfrak{p}} = \left\{ \frac{a}{b} \,\middle|\, a,\ b \in \mathbb{Z},\ 2 \nmid b \right\}$.

(2) $R = 2\mathbb{Z}, \mathfrak{a} = 4\mathbb{Z}$:
$2 \cdot 2 \in \mathfrak{a}$, also ist $\mathfrak{a}$ kein Primideal. $\mathfrak{a}$ ist maximal, denn $x \in R \backslash \mathfrak{a}$ hat die Gestalt $2(2m+1)$,
$(\mathfrak{a}, x) \ni x - 4m = 2$.

37. Definition

Ein Ring R, in dem jedes Ideal endlich erzeugt ist, heißt noetherscher Ring.

Beispiel: $R = \mathbb{Z}$, dort ist jedes Ideal Hauptideal.

38. Satz (Charakterisierung noetherscher Ringe)

Für Ringe R sind folgende Aussagen äquivalent:

(1) R ist noethersch;
(2) Jede aufsteigende Kette von Idealen $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \ldots \subseteq \mathfrak{a}_k \subseteq \ldots$ wird stationär (bricht ab), d.h. es existiert $n \in \mathbb{N}$ mit $\mathfrak{a}_{n+i} = \mathfrak{a}_n \; \forall i \in \mathbb{N}$;
(3) In jeder nicht leeren Menge von Idealen gibt es ein (bzgl. $\subseteq$) maximales Element.

Beweis:
(i) $\Rightarrow$ (ii):
Für eine vorgelegte Kette von Idealen ist deren Vereinigung $\mathfrak{a}$ wieder ein Ideal(!), welches etwa durch $a_1, \ldots, a_m$ erzeugt wird. Für $a_i \in \mathfrak{a}_{j_i}$ $(1 \leq i \leq m)$ gilt dann also $\mathfrak{a}_{j_0} \supseteq (a_1, \ldots, a_m) \supseteq \mathfrak{a}_{j_0}$, $a_i \in \mathfrak{a}_{j_0}$ $(1 \leq i \leq m)$ mit $j_0 := \max\{j_1, \ldots, j_m\}$, und wir erhalten etwa $n = j_0$, d.h. die Kette wird ab $\mathfrak{a}_{j_0}$ stationär.

(ii) $\Rightarrow$ (iii):
Es sei $\mathfrak{M} \neq \emptyset$ eine Menge von Idealen. Wähle $\mathfrak{a}_1 \in \mathfrak{M}$. Ist $\mathfrak{a}_1$ maximal, so sind wir fertig. Ist $\mathfrak{a}_1$ nicht maximal, so exitiert $\mathfrak{a}_2 \in \mathfrak{M}$, $\mathfrak{a}_2 \supset \mathfrak{a}_1$. Man erhält so eine aufsteigende Kette, die nach Voraussetzung stationär werden muß. Das diesbezügliche $\mathfrak{a}_n$ ist dann in $\mathfrak{M}$ maximal.

(iii) $\Rightarrow$ (i):
Es sei $\mathfrak{a}$ ein Ideal von R. Bilde

$$\mathfrak{M} := \{\mathfrak{b} \mid \mathfrak{b} \text{ endlich erzeugtes Ideal in } R \text{ mit } \mathfrak{b} \subseteq \mathfrak{a}\}.$$

Wegen $\{0\} \in \mathfrak{M}$ ist $\mathfrak{M} \neq \emptyset$. Sei $\mathfrak{m}$ maximales Element von $\mathfrak{M}$, etwa $\mathfrak{m} =< a_1, \ldots, a_k >$. Für beliebiges $a \in \mathfrak{a}$ ist $\tilde{\mathfrak{m}} := (a_1, \ldots, a_k, a)$ in $\mathfrak{M}$, also gleich $\mathfrak{m}$, also folgt $\mathfrak{a} = \mathfrak{m}$.

□

Bemerkung:
Es sei R ein noetherscher Ring und $f : R \to S$ ein Ringepimorphismus. Dann ist S noethersch.
(Speziell: Ist $\mathfrak{a}$ ein Ideal von R, so ist $R/\mathfrak{a}$ noethersch.)

Beweis:
Es sei $\mathfrak{a}$ ein Ideal von S, dann ist etwa $f^{-1}(\mathfrak{a}) =< a_1, \ldots, a_k >$, und es folgt $\mathfrak{a} = (f(a_1), \ldots, f(a_k))$.

□

Teilbarkeit in Ringen

Sinnvollerweise sind Nullteiler auszuschließen!
Ferner: $R \ni 1 \neq 0$ und R sollte kommutativ sein.

39. Definition

Ein nullteilerfreier, kommutativer Ring $R \neq \{0\}$ heißt Integritätsring.

Bemerkung:
In Integritätsringen gilt die Kürzungsregel (2.19)(i), endliche Integritätsringe sind Körper (2.19)(ii). R kommuativer Ring, $\mathfrak{a} \subset R$ Ideal: $\mathfrak{a}$ Primideal $\Leftrightarrow$ $R/\mathfrak{a}$ Integritätsring nach (2.33).

Beispiel: Alle Ideale $\neq \{0\}$ in $\mathbb{Z}$ und Körper sind Integritätsringe.

40. Definition

Es seien R ein Integritätsring mit 1 und $a, b \in R$.
a heißt Teiler von b (a teilt b, b ist Vielfaches von a, $a|b$), falls $c \in R$ mit $b = ac$ existiert.
a heißt assoziiert zu b $(a \sim b)$, falls $a|b$ und $b|a$ gilt.
$c \in R$ heißt größter gemeinsamer Teiler (ggT) von a, b, falls $c|a$ und $c|b$ und für alle $d \in R$ mit $d|a$, $d|b$ auch $d|c$ gilt.
a, b heißen teilerfremd, falls ggT $(a, b) \in U(R)$ ist.
$c \in R$ heißt kleinstes gemeinsames Vielfaches (kgV) von a, b, falls $a|c$, $b|c$ und für alle $d \in R$ mit $a|d$, $b|d$ auch $c|d$ gilt.
Ein Element $p \in R \backslash U(R)$, $p \neq 0$, heißt Primelement von R, wenn für alle $a, b \in R$ mit $p|ab$ stets $p|a$ oder $p|b$ folgt.
Ein Element $a \in R \backslash U(R)$, $q \neq 0$ heißt irreduzibel (unzerlegbar), wenn für alle $a, b \in R$ mit $ab = q$ stets $a \in U(R)$ oder $b \in U(R)$ folgt.

Beispiele:

(1) Übliche Definitionen in $\mathbb{Z}$; die zu $a \in \mathbb{Z}$ assoziierten Elemente sind $\pm a$ $(U(R) = \{\pm 1\})$, die Primzahlen sind die Primelemente und stimmen mit den irreduziblen Elemente überein.
(2) Es sei $R = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$. Es gibt unendlich viele assoziierte Elemente $a\,(-1)^h\,(1+\sqrt{2})^k$ $(h \in \{0, 1\},\ k \in \mathbb{Z})$.

$$1+\sqrt{2} = \frac{(1+\sqrt{2})\,(1-\sqrt{2})}{1-\sqrt{2}} = \frac{-1}{1-\sqrt{2}} \quad \Rightarrow \quad \begin{array}{rcl} (1-\sqrt{2})^{-1} & = & -(1+\sqrt{2}), \\ (1+\sqrt{2})^{-1} & = & -(1-\sqrt{2}) \end{array}$$

$((1+\sqrt{2})^k$ $(k \in \mathbb{Z})$ sind alle verschieden!)

$\sqrt{2}$ ist irreduzibel (und sogar Primelement!).
(Denn für $S := \mathbb{Z}[\sqrt{m}]$ $(m \in \mathbb{Z},\ \nexists a \in \mathbb{Z}^{\geq 2} : a^2|m)$ ist

$$N : \mathbb{Z}[\sqrt{m}] \to \mathbb{Z} : a + b\sqrt{m} \mapsto a^2 - mb^2$$

eine multiplikativer Homomorphismus. Wäre nun $\sqrt{2} = xy$ in $\mathbb{Z}[\sqrt{2}]$, so folgte $N(\sqrt{2}) = -2 = N(x)\,N(y)$ in $\mathbb{Z}$, also $N(x) = \pm 1$ oder $N(y) = \pm 1$. Ist o.B.d.A. $N(x) = \pm 1$, so gilt für $x = u+v\sqrt{2}$: $\pm 1 = (u+v\sqrt{2})\,(u-v\sqrt{2})$, d.h. $x \in U(R)$.)
Der Primelementnachweis verläuft ähnlich.

(3) Es sei $R = \mathbb{Z}[\sqrt{-5}]$. Hierin ist $U(R) = \{\pm 1\}$ $(= U(\mathbb{Z}))$, wegen

$$N(a + b\sqrt{-5}) = a^2 + 5b^2 = 1 \quad \Leftrightarrow \quad b = 0,\ a = \pm 1.$$

Ferner ist $21 = 3 \cdot 7 = (4 + \sqrt{-5})\,(4 - \sqrt{-5}) = (1 + 2\sqrt{-5})\,(1 - 2\sqrt{-5})$.
Hierin sind die beteiligten Elemente offenbar (!) keine Primelemente, jedoch irreduzibel.

Beweis:
Es ist $N(3) = 9$, für $3 = xy$ mit $x,\ y \notin \{\pm 1\}$ folgt $N(x) = N(y) = 3$, jedoch ist $N(u + v\sqrt{-5}) = u^2 + 5v^2 = 3$ unlösbar in $\mathbb{Z}$. Also ist 3 irreduzibel. Der Nachweis für die anderen Elemente geht analog.

Bemerkung:
Jede Einheit teilt alle Elemente aus R; $x|x$ und $x|0$ für alle $x \in R$; $a \in R$ mit $a|1 \ \Rightarrow\ a$ ist Einheit $(a \in U(R))$; $a,\ b,\ x \in R$ und $a|b \ \Rightarrow\ ax|bx$; $a,\ r_i,\ x_i \in R$ $(1 \leq i \leq n)$ und $a|x_i$ $(1 \leq i \leq n) \ \Rightarrow\ a\Big|\sum_{i=1}^{n} r_i x_i$; $a,\ b,\ c \in R$ und $a|b,\ b|c \ \Rightarrow\ a|c$; $a,\ b \in R$: $a|b \ \Leftrightarrow\ b \in Ra \ \Leftrightarrow\ Rb \subseteq Ra$; $a,\ b \in R$:
$a \sim b \ \Leftrightarrow \exists e \in U(R) : b = ae \ \Leftrightarrow\ Ra = Rb$.
Jedes Primelement ist irreduzibel; dies ist eine Konsequenz des folgenden Hilfssatzes.

41. Hilfssatz

Es sei R ein Integritätsring mit 1 und $a \in R\backslash U(R),\ a \neq 0$. Dann gilt:

(1) a Primelement $\Leftrightarrow$ Ra Primideal;
(2) a irreduzibel $\Leftrightarrow$ Ra maximales Hauptideal von R.
(a reduzibel $\Leftrightarrow$ Ra nicht maximal in der Menge der Hauptideale von R.)

Beweis:

(1)

$$\begin{aligned} a \text{ Primelement} &\Leftrightarrow (\forall x,\, y \in R :\ a|xy \ \Rightarrow\ a|x \vee a|y) \\ &\Leftrightarrow (\forall x,\, y \in R :\ xy \in Ra \ \Rightarrow\ x \in Ra \vee y \in Ra) \\ &\Leftrightarrow Ra \text{ Primideal.} \end{aligned}$$

(2)

$$\begin{aligned} a \text{ irreduzibel} &\Leftrightarrow (\forall x,\, y \in R :\ a = xy \ \Rightarrow\ x \in U(R) \vee y \in U(R)) \\ &\Leftrightarrow (\forall x \in R :\ Ra \subseteq Rx \ \Rightarrow\ x \in U(R) \vee x \sim a) \\ &\Leftrightarrow (\forall x \in R :\ Ra \subset Rx \ \Rightarrow\ x \in U(R)) \\ &\Leftrightarrow Ra \text{ maximales Hauptideal von } R. \end{aligned}$$

□

42. Definition

Ein Integritätring mit 1, in dem jedes Ideal Hauptideal ist, heißt Hauptidealring.

Bemerkung:

(1) Hauptidealringe sind noethersch.
(2) $\mathbb{Z}$ ist Hauptidealring, ebenso sind alle Körper Hauptidealringe.
(3) Für Elemente $a \neq 0$ in Hauptidealringen gilt:

a Primelement $\Rightarrow$ a irreduzibel $\overset{(2.41)(\text{ii})}{\Rightarrow}$ Ra maximales Hauptideal $\Rightarrow$ Ra Primideal $\overset{(2.41)(\text{i})}{\Rightarrow}$ a Primelement.

Merke: In Hauptidealringen stimmen irreduzible und Primelemente überein. Speziell ist also $\mathbb{Z}[\sqrt{-5}]$ kein Hauptidealring.

(4) Es seien $d, a_1, \ldots, a_n$ aus einem Hauptidealring R. Dann gilt:

$$d = \mathrm{ggT}\,(a_1, \ldots, a_n) \quad \Leftrightarrow \quad (a_1, \ldots, a_n) = Rd.$$

Dies bedeutet, daß ein größter gemeinsamer Teiler von $a_1, \ldots, a_n$ sich als $d = \sum_{i=1}^{n} r_i\, a_i$ $(r_i \in R)$ darstellen läßt.

Beweis:
Für jeden gemeinsamen Teiler $\tilde{d}$ von $a_1, \ldots, a_n$ gilt:

$$a_i = b_i\, \tilde{d} \quad \Leftrightarrow \quad (a_1, \ldots, a_n) \subseteq R\tilde{d}.$$

Ferner ist $(a_1, \ldots, a_n)$ ein Hauptideal Rd, für das dann $\tilde{d}|d$ und damit $d = \mathrm{ggT}\,(a_1, \ldots, a_n)$ gelten muß.

□

43. Satz

In einem Hauptidealring R läßt sich jedes $x \in R\backslash U(R),\ a \neq 0$, als Produkt von Primelementen darstellen.

Beweis:
Gemäß der vorrangehenden Bemerkung (iii) genügt es, eine Darstellung von x als Produkt irreduzibler Elemente nachzuweisen.

Ist x irreduzibel, sind wir fertig. Ansonsten existieren $x_1,\ x_2 \in R\backslash U(R)$ mit $x = x_1 x_2$, und es ist $(x) \subsetneqq (x_i)\ \ (1 \leq i \leq 2)$. Analog versuchen wir $x_1,\ x_2$ zu faktorisieren und erhalten so nach n Schritten x als Produkt von $y_1, \ldots, y_n \in R\backslash U(R)$. Dabei werden die Faktoren so angeordnet, daß im Falle nicht irreduzibler Faktoren diese die höchsten Indizes bekommen. Wegen

$$(x) \subsetneqq (y_2 \cdot \ldots \cdot y_n) \subsetneqq \ldots \subsetneqq (y_{n-1}\, y_n) \subsetneqq (y_n)$$

muß dieser Prozeß abbrechen (R ist als Hauptidealring noethersch), d.h. nach endlich vielen Schritten wird x ein Produkt irreduzibler Elemente.

□

44. Definition

Ein Integritätsring mit 1 heißt ZPE-Ring (Ring mit eindeutiger Primelementzerlegung, faktorieller Ring), falls sich jedes $x \in R\backslash U(R),\ x \neq 0$, bis auf Einheiten eindeutig als Produkt irreduzibler Elemente darstellen läßt.

(Aus $x = \varepsilon\, q_1 \cdot \ldots \cdot q_r = \tilde{\varepsilon}\, \tilde{q}_1 \cdot \ldots \cdot \tilde{q}_s$ mit $\varepsilon,\ \tilde{\varepsilon} \in U(R),\ q_i,\ \tilde{q}_j$ irreduzibel folgt $r = s$ und nach eventueller Umnumerierung $q_i \sim \tilde{q}_i\ (1 \leq i \leq r)$.)

45. Satz

Für Integritätsringe R mit 1 sind äquivalent:

(1) R ist ZPE-Ring;
(2) jedes $x \in R\backslash U(R),\ x \neq 0$, ist Produkt irreduzibler Elemente, und jedes irreduzible Element von R ist Primelement;
(3) jedes $x \in R\backslash U(R),\ x \neq 0$, ist Produkt von Primelementen.

Beweis:
(i) $\Rightarrow$ (ii):
Es bleibt zu zeigen, daß jedes irreduzible Element von R ein Primelement ist. Es seien dazu $a,\ b \in R$ und $\pi \in R$ irreduzibel mit $\pi \mid ab$. Da $a,\ b$ sich eindeutig als Produkte irreduzibler Elemente schreiben lassen, ergibt sich die Zerlegung von ab in irreduzible Elemente aus der von a bzw. b. Nach Voraussetzung muß also ein zu π assoziiertes Element in der Faktorisierung von a oder b auftreten, es folgt $\pi | a$ oder $\pi | b$.

(ii) $\Rightarrow$ (iii): Trivial.

(iii) $\Rightarrow$ (ii):

Ist π irreduzibel, so besitzt π eine Darstellung als Produkt von Primelementen. Diese besteht dann notwendig aus nur einem Faktor.

(ii) $\Rightarrow$ (i):
Es seien

$$x = \varepsilon\, q_1 \cdot \ldots \cdot q_r = \tilde{\varepsilon}\, \tilde{q}_1 \cdot \ldots \cdot \tilde{q}_s$$

mit $\tilde{\varepsilon}$, $\varepsilon \in U(R)$ und q_i, $\tilde{q}_j$ irreduzibel $(1 \leq i \leq r,\ 1 \leq j \leq s)$. Da q_r Primelement ist, muß q_r eins der $\tilde{q}_j$ teilen, also zu ihm assoziiert sein. Wir ordnen nun gegebenenfalls um, so daß $q_r | \tilde{q}_s$ gilt. Daraus folgt

$$\varepsilon\, q_1 \cdot \ldots \cdot q_{r-1} = \hat{\varepsilon}\, \tilde{q}_1 \cdot \ldots \cdot \tilde{q}_{s-1}$$

mit $\hat{\varepsilon} \in U(R)$. Nach r-maliger Anwendung folgt so $r = s$ und bei passender Numerierung $q_i \sim \tilde{q}_i$ $(1 \leq i \leq r)$.

□

Bemerkung:

(1) Als direkte Konseqenz von (2.43) folgt, daß jeder Hauptidealring auch ZPE-Ring ist.
(2) Wählt man aus jeder Klasse assoziierter Primelemente einen Vertreter aus und bezeichnet die Menge dieser Vertreter mit P so läßt sich in ZPE-Ringen jedes $x \in R,\ x \neq 0$, eindeutig als

$$x = \varepsilon \prod_{p \in P} p^{\nu_p(x)}, \quad y = \eta \prod_{p \in P} p^{\nu_p(y)}$$

($\nu_p(x) \in \mathbb{Z}^{\geq 0}$, ε, $\eta \in U(R)$, nur endlich viele $\nu_p(x)$ ungleich Null, $\nu_p(x)$ ist der genaue Exponent, mit dem p gerade x teilt) schreiben. Für x, $y \in R \backslash \{0\}$ folgt dann insbesondere:

$$\begin{aligned} x\, y &= \varepsilon\, \eta \prod_{p \in P} p^{\nu_p(x) + \nu_p(y)}, \\ \mathrm{ggT}\,(x,\, y) &= \prod_{p \in P} p^{\min\{\nu_p(x),\, \nu_p(y)}, \\ \mathrm{kgV}\,(x,\, y) &= \prod_{p \in P} p^{\max\{\nu_p(x),\, \nu_p(y)}, \\ x \,|\, y &\Leftrightarrow \nu_p(x) \leq \nu_p(y) \ \ \forall p \in P. \end{aligned}$$

Ohne Euklidischen Algorithmus ist es i.a. ein schwieriges Problem, wie man in Hauptidealringen ein erzeugendes Element eines Ideals, etwa von $(a_1, \ldots, a_n)$, findet, d.h. einen ggT berechnet. Eine Faktorisierung in Primelemente ist meist zu aufwendig, etwa schon bei großen Zahlen in $\mathbb{Z}$.

46. Definition

Ein Integritätsring R heißt euklidischer Ring, wenn es eine Abbildung $v : R\backslash\{0\} \to \mathbb{Z}^{\geq 0}$ gibt, derart daß für beliebige $a, b \in R,\ b \neq 0$, zwei Elemente $Q(a, b),\ R(a, b) \in R$ mit

$$a = Q(a, b)\, b + R(a, b) \quad \text{und} \quad R(a, b) = 0 \quad \text{oder} \quad v(R(a, b)) < v(b)$$

gibt.

Bemerkung:

(1) Euklidische Ringe sind Ringe mit Einselement.
Die Menge $\{v(x) \mid x \in R\backslash\{0\}\}$ enthält ein minimales Element $v(x_0)$. Hierfür ist notwendig $R(a, x_0) = 0\ \forall a \in R$, also teilt x_0 alle $a \in R$. Ferner ist $0 \neq Q(x_0, x_0)$ Linkseins:

$$Q(x_0, x_0)\, y = Q(x_0, x_0)\, Q(y, x_0)\, x_0 = Q(y, x_0)\, Q(x_0, x_0)\, x_0 = Q(y, x_0)\, x_0 = y, \quad \forall y \in R.$$

Da R kommutativ ist, ist $Q(x_0, x_0)$ Einselement von R.

(2) $\mathbb{Z}$ mit $v = |\ |$ (Betragsfunktion) und $K[t]$ mit $v = \deg(\ )$ sind euklidische Ringe, es existiert der euklidische Algorithmus, der zur Berechnung eines ggT zweier Ringelemente dient. Jeder Körper ist ein euklidischer Ring.

Beispiel: (Übung)
$R = \mathbb{Z}[-1]$ (Gaußsche ganze Zahlen) mit $v : a + b\sqrt{-1} \mapsto a^2 + b^2$.

47. Satz

Jeder euklidische Ring R ist Hauptidealring.

Beweis:
Es sei $\mathfrak{a} \neq \{0\}$ ein Ideal von R. Ferner sei $a \in \mathfrak{a}$ mit $v(a) = \min\{v(x) \mid x \in \mathfrak{a},\ x \neq 0\}$. Für $x \in a$ gilt dann $x = Q(x, a)\, a$, da notwendig $R(x, a)$ verschwinden muß. Also gilt $Ra \subseteq \mathfrak{a} \subseteq Ra$.

□

Polynomringe als Gruppenringe

48. Definition

Es sei S ein Halbgruppe und R ein Ring. Dann definert man den sogenannten Halbgruppenring

$$R[S] := \{f : S \to R \mid f(s) = 0 \text{ für fast alle } s \in S\}$$

mit den Verküpfungen:

$$\text{Addition} : \quad f + g : S \to R : s \mapsto f(s) + g(s),$$

$$\text{Multiplikation} : \quad f\, g : S \to R : \sum_{\substack{t_1 t_2 = s \\ t_1, t_2 \in S}} f(t_1)\, g(t_2) \qquad (\text{Faltungsprodukt})$$

für alle $f, g \in R[S]$.

Wir rechnen hier nur das Assoziativgesetz bezüglich der Multiplikation nach:

Für $s \in S$ beliebig gilt

$$\begin{aligned}
(f\,(g\,h))\,(s) &= \sum_{t_1 t_4 = s} f(t_1)\,(g\,h)\,(t_4) \\
&= \sum_{t_1 t_4 = s} f(t_1) \sum_{t_2 t_3 = t_4} g(t_2)\,h(t_3) \\
&= \sum_{t_1 t_2 t_3 = s} f(t_1)\,g(t_2)\,h(t_3) \\
&= \sum_{t_5 t_3 = s} \left(\sum_{(} t_1 t_2 = t_5) f(t_1) g(t_2) \right) h(t_3) \\
&= \sum_{t_5 t_3 = s} (f g)\,(t_5)\,h(t_3) \\
&= ((f\,g)\,h)\,(s).
\end{aligned}$$

Einbettung von R, S in $R[S]$:

(1) S sei Monoid. Setze

$$\iota_R \,:\, R \to R[S] \,:\, r \mapsto f_r \quad \text{mit} \quad f_r(s) = \begin{cases} r & \text{für } s = e \\ 0 & \textit{sonst} \end{cases}$$

mit $e = 1_S$. Dann ist ι_R Ringhomomorphismus wegen l_e von l_R

$$\begin{aligned}
f_{r+\tilde{r}}(s) &= \begin{cases} r+\tilde{r} & \text{für} s = e \\ 0 & \text{sonst} \end{cases} \\
&= \begin{cases} r & \text{für} s = e \\ 0 & \text{sonst} \end{cases} + \begin{cases} \tilde{r} & \text{für} s = e \\ 0 & \text{sonst} \end{cases} \\
&= f_r(s) + f_{\tilde{r}}(s), \\
f_{r\tilde{r}}(s) &= \begin{cases} r\tilde{r} & \text{für } s = e \\ 0 & \text{sonst} \end{cases} \\
&= \sum_{t_1 t_2 = s} \begin{cases} r & \text{für } t_1 = e \\ 0 & \text{sonst} \end{cases} \begin{cases} \tilde{r} & \text{für} t_2 = e \\ 0 & \text{sonst} \end{cases} \\
&= f_r\, f_{\tilde{r}}(s).
\end{aligned}$$

(2) R sei Ring mit 1. Setze

$$\iota_S \,:\, S \to R[S] \,:\, s \mapsto F_s \quad \text{mit} \quad F_s(t) = \begin{cases} 1 & \text{für } t = s \\ 0 & \text{sonst} \end{cases} = \delta_{ts}.$$

l_s ist Homomorphismus wegen

$$\begin{aligned} F_{s\tilde{s}}(t) &= \delta_{t,s\tilde{s}} \\ &= \begin{cases} 1 & \text{für } s\tilde{s} = t \\ 0 & \text{sonst} \end{cases} \\ &= \sum_{t_1 t_2 = t} \delta_{t_1 s}\, \delta_{t_2 \tilde{s}} \\ &= \sum_{t_1 t_2 = t} \begin{cases} 1 & \text{für } t_1 = s \\ 0 & \text{sonst} \end{cases} \begin{cases} 1 & \text{für } t_2 = \tilde{s} \\ 0 & \text{sonst} \end{cases} \\ &= F_s(t)\, F_{\tilde{s}}(t) \end{aligned}$$

Falls S zusätzlich Monoid ist, besitzt $R[S]$ ein Einselement, nämlich F_e.

$$\begin{aligned} F_e(t)\, f(t) &= \sum_{t_1 t_2 = t} F_e(t_1)\, f(t_2) \\ &= \sum_{t_1 t_2 = t} \delta_{e t_1}\, f(t_2) \\ &= f(t) \qquad \forall f \in R[S]. \end{aligned}$$

(3) Falls $R \ni 1$ gilt, erhalten wir

$$\begin{aligned} R[S] &= \left\{ \sum_{s \in S} a_s\, F_s \;\middle|\; a_s \in R,\ a_s = 0 \text{ für fast alle } s \in S \right\} \\ &\overset{(*)}{=} \left\{ \sum_{s \in S} a_s\, s \;\middle|\; a_s \in R,\ a_s = 0 \text{ für fast alle } s \in S \right\}. \end{aligned}$$

$(*)$: gilt dabei wegen der Definition der Einbettung l_s.

Dann kann man in $R[S]$ wie folgt rechnen:

$$\begin{aligned} \alpha \left(\sum_{s \in S} a_s\, s \right) &= \sum_{s \in S} (\alpha\, a_s)\, s \quad \forall \alpha \in R, \\ \sum_{s \in S} a_s\, s + \sum_{s \in S} b_s\, s &= \sum_{s \in S} (a_s + b_s)\, s, \\ \left(\sum_{s \in S} a_s\, s \right) \left(\sum_{s \in S} b_s\, s \right) &= \sum_{s,t \in S} a_s\, b_t\, s\, t \\ &= \sum_{s \in S} \left(\sum_{t_1 t_2 = s} a_{t_1}\, b_{t_2} \right) s. \end{aligned}$$

Beispiele:

(1) $S = \{ t^\nu \mid \nu \in \mathbb{Z}^{\geq 0} \} \cong \mathbb{Z}^{\geq 0}$, R kommutativer Ring mit 1.

$$R[S] = \left\{ \sum_{\nu=0}^{\infty} a_\nu\, t^\nu \;\middle|\; a_\nu \in R,\ a_\nu \neq 0 \text{ nut für endlich viele } \nu \right\} =: R[t]$$

ist der Polynomring in der Variablen t über R mit Elementen

$$f(t) = \sum_{i=0}^{\infty} a_\nu \, t^\nu$$

($a_\nu \in R$, fast alle $a_\nu = 0$).

(2)
$$S = \bigtimes_{i=1}^{n} \{t_i^{\nu_i} \in \mathbb{Z}^{\geq 0}\} \cong (\mathbb{Z}^{\geq 0})^n,$$

R kommutativer Ring mit 1. Die Elemente von S lassen sich als $\underline{t}^{\underline{\nu}} := t_1^{\nu_1} \cdot \ldots \cdot t_n^{\nu_n}$ mit $\underline{\nu} \in (\mathbb{Z}^{\geq 0})^n$ schreiben. Es ist

$$R[S] = \left\{ \sum_{\underline{\nu} \in (\mathbb{Z}^{\geq 0})^n} a_{\underline{\nu}} \, \underline{t}^{\underline{\nu}} \;\middle|\; a_{\underline{\nu}} \in R, a_{\underline{\nu}} \neq 0 \text{ nur für endlich viele } a_{\underline{\nu}} \right\} =: R[t_1, \ldots, t_n]$$

ist der Polynomring in n Variablen $t_1, \ldots, t_n$ über R mit den Elementen

$$f(\underline{t}) = \sum_{\underline{\nu} \in (\mathbb{Z}^{\geq 0})^n} a_{\underline{\nu}} \, \underline{t}^{\underline{\nu}} \quad (a_{\underline{\nu}} \in R, \text{ fast alle } a_{\underline{\nu}} = 0).$$

(3) S Gruppe, R Ring mit 1. $R[S]$ ist Gruppenring.

Wissen im Gruppenring liefert Information über die Gruppe selbst.

(Higman: G, H endliche abelsche Gruppen mit $\mathbb{Z}[G] \cong \mathbb{Z}[H] \Rightarrow G \cong H$.)

Polynomringe in mehreren Variablen. Bemerkung:
Wir erhalten

$$\begin{aligned} R[t_1, \ldots, t_{n+1}] &\cong R[t_1, \ldots, t_n]\,[t_{n+1}], \\ R[t_1, \ldots, t_n] &\cong R[t_{\pi(1)}, \ldots, t_{\pi(n)}] \quad \forall \pi \in \mathfrak{S}_n \end{aligned}$$

als direkte Konsequenz der entsprechenden Aussagen über direkte Produkte von (Halb-)Gruppen.

Für Elemente des Monoids in (ii) läßt sich eine Ordnung definieren mittels:

$$\underline{t}^{\underline{\nu}} \geq t^{\underline{\mu}} \quad \Leftrightarrow \quad \underline{\nu} \geq \underline{\mu}$$

(etwa lexikographisch).

49. Definition

Es sei

$$f(\underline{t}) = \sum_{\underline{\nu} \in (\mathbb{Z}^{\geq 0})^n} a_{\underline{\nu}} \, \underline{t}^{\underline{\nu}}$$

ein Element des Polynomrings $R[t_1, \ldots, t_n]$. Hierbei heißen die Summanden $a_{\underline{\nu}} \, \underline{t}^{\underline{\nu}}$ Monome. Unter dem Grad eines Monoms $\neq 0$ versteht man die Summe der Exponenten $\nu_1 + \ldots + \nu_n$. Als Grad von $f \neq 0$ bezeichnet man das Maximum der Grade seiner Monome (Bezeichnung:

$\deg(f)$). Ist auf den Potenzen $\underline{t}^{\underline{\nu}}$ eine Ordnung gegeben, so heißt $a_{\underline{\nu}}$ mit $\underline{\nu}$ maximal Leitkoeffizient von f und $a_{\underline{\nu}}\,\underline{t}^{\underline{\nu}}$ heißt Leitmonom. (I.a. setzt man

$$\underline{\nu} \geq \underline{\mu} \quad \Leftrightarrow \quad \underline{t}^{\underline{\nu}} \geq \underline{t}^{\underline{\mu}} \quad :\Leftrightarrow \quad \sum_{i=1}^{n} \nu_i \geq \sum_{i=1}^{n} \mu_i$$

und im Falle der Gleichheit $\underline{\nu} \geq \underline{\mu}$ lexikographisch.) Ferner setzt man $\deg(0) = -\infty$. Im Fall $l(f) = 1$ heißt f normiert.

Beispiele für Anordnungen auf $(\mathbb{Z}^{\geq 0})^n$:

$\underline{\nu} \geq \underline{\mu} :\Leftrightarrow \left(\sum_{i=1}^{n} \nu_i \geq \sum_{i=1}^{n} \mu_i \text{ und für Gleichheit } \underline{\nu} \geq \underline{\mu} \text{ lexikographisch}\right)$,

$\underline{\nu} \geq \underline{\mu}$ lexikographisch $:\Leftrightarrow\ \nu_i = \mu_i,\ 1 \leq i < i_0$ und $\nu_{i_0} > \mu_{i_0}$ für ein $i_0 \in \{1, \ldots, n\}$.

Bemerkung:

(1) Sind $f, g \in R[\underline{t}]$, so gilt

$$\begin{aligned} \deg(f+g) &\leq \max\{\deg(f), \deg(g)\} \\ \deg(f\,g) &\leq \deg(f) + \deg(g). \end{aligned}$$

Bei der Multiplikation gilt Gleichheit, falls $l(f)$, $l(g)$ keine Nullteiler sind, also etwa für Integritätsringe R.

(2) $R[\underline{t}]$ Integritätsring $\Leftrightarrow$ R Integritätsring.

(3) $f \in R[\underline{t}]$ invertierbar $\Leftrightarrow$ $f \in U(R)$ $(U(R[\underline{t}]) = U(R))$ in Integritätsringen R!

50. Hilbertscher Basissatz

Es sei R ein kommutativer Ring mit 1. Ist R noethersch, dann auch $R[t]$.

Beweis:

Es sei $\mathfrak{Q}$ ein Ideal in $R[t]$. Betrachte hierzu Polynome vom Grad $i \in \mathbb{Z}^{\geq 0}$, setze

$$\mathfrak{a}_i := \{x \in R \mid x = l(f) \text{ für ein } f \in \mathfrak{Q} \text{ mit } \deg(f) = i\} \cup \{0\}.$$

Dann bilden die $\mathfrak{a}_i$ Ideale in R, denn

(1) für $f, g \in \mathfrak{Q}$ mit $\deg(f) = \deg(g) = i \ \Rightarrow$ entweder $l(f \pm g) = l(f) \pm l(g)$ mit $\deg(f \pm g) = \deg(f) = i$ oder $\deg(f \pm g) < i$ mit $l(f) \pm l(g) = 0$;

(2) für $a = l(f) \in \mathfrak{a}_i,\ r \in R \ \Rightarrow\ ra = 0$ oder $rf \in \mathfrak{Q}$ mit $\deg(rf) = i$ und $l(rf) = r\,l(f)$.

Da man Elemente von $\mathfrak{Q}$ mit t multiplizieren kann und dabei in $\mathfrak{Q}$ bleibt, folgt unmittelbar

$$\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \ldots \subseteq \mathfrak{a}_r \subseteq \ldots .$$

Da R noethersch ist, wird diese Kette stationär. Es sei $r \in \mathbb{Z}^{\geq 0}$ minimal mit $\mathfrak{a}_r = \mathfrak{a}_{r+k}\ \forall k \in \mathbb{N}$. Dann existieren erzeugende Elemente

$a_{i1}, \ldots, a_{in_i}$ $(n_i \in \mathbb{N})$ für $\mathfrak{a}_i$ $(0 \leq i \leq r)$. Für $0 \leq i \leq r,\ 1 \leq j \leq n_i$ sei $f_{ij} \in \mathfrak{Q}$ mit $l(f_{ij}) = a_{ij}$.

Wir zeigen nun, daß diese f_{ij} das Ideal $\mathfrak{Q}$ erzeugen.

Es sei $f \in \mathfrak{Q}$ mit $\deg(f) = d$. Wir führen Induktion nach d durch. Der Fall $d = 0$ ist klar, da dann f in $\mathfrak{a}_0$ liegt. Sei also $d > 0$. Für $d > r$ gilt

$$\mathfrak{a}_d =< l(t^{d-r} f_{r1}, \ldots, l(t^{d-r} f_{rn_r}) >,$$

es exitieren daher $\gamma_1, \ldots, \gamma_{n_r} \in R$ mit

$$\deg(f - \gamma_1 t^{d-r} f_{r1} - \ldots - \gamma_{n_r} t^{d-r} f_{rn_r}) < d,$$

und das Differenzpolynom liegt wiederum in $\mathfrak{Q}$. Für $d \leq r$ erhalten wir analog ein Polynom

$$f - \tilde{\gamma}_1 f_{d1} - \ldots - \tilde{\gamma}_{n_d} f_{dn_d}$$

mit Grad $< d$ in $\mathfrak{Q}$. Nach Induktionsannahme liegt das Differenzpolynom im Ideal

$$\mathcal{F} :=< f_{ij} \mid 0 \leq i \leq r,\ 1 \leq j \leq n_i >,$$

also auch f selbst. Damit gilt $\mathfrak{Q} = \mathcal{F}$, jedes Ideal von $R[t]$ ist endlich erzeugt, damit ist $R[t]$ noethersch.

□

51. Hilfssatz

Ist Λ ein unitärer Oberring von R (d.h. $1_\Lambda = 1_R$), so ist für $\underline{x} \in \Lambda^n$ die Abbildung

$$\Phi_{\underline{x}} : R[\underline{t}] \to \Lambda : f(\underline{t}) \mapsto f(\underline{x})$$

ein Ringhomomorphismus mit $\Phi_{\underline{x}}|_R = \mathrm{id}_R$. Dieser läßt die Elemente aus R invariant, ist also ein sogenannter R-Homomorphismus.

Beweis: Durch Nachrechnen!

Bemerkung:
$\underline{x} \in \Lambda^n$ heißt Nullstelle von $f \in R[\underline{t}]$, falls $\Phi_{\underline{x}}(f) = 0$ bzw. $f(\underline{x}) = 0$ ist.

?? und ?? implizieren:
R noethersch $\Leftrightarrow$ $R[\underline{t}]$ noethersch.

Im folgenden betrachten wir hauptsächlich univariate Polynome (= Polynome in 1 Variablen).

52. Hilfssatz

Es sei R ein Integritätsring mit 1. Ein R-Homomorphismus $\varphi : R[t] \to R[t]$ ist genau dann ein Isomorphismus, wenn

$$\varphi(t) = at + b \quad \text{mit} \quad a \in U(R),\ b \in R$$

gilt.

Beachte:
Für Homomorphismen $\varphi : R[t] \to \Lambda$ ist φ durch $\varphi(t)$ eindeutig festgelegt wegen

$$\begin{aligned} \varphi\left(\sum_{i=0}^{n} a_i\, t^i\right) &= \sum_{i=0}^{n} \varphi(a_i\, t^i) \\ &= \sum_{i=0}^{n} \underbrace{\varphi(a_i)}_{=a_i}\, \varphi(t)^i. \end{aligned}$$

Beweis:
Für $\varphi(t) = at + b$ mit $a \in U(R),\ b \in R$ folgt $\varphi^{-1}(t) = a^{-1}(t - b)$, also $\varphi \circ \varphi^{-1} = \mathrm{id}_{R[t]}$. Ist andererseits φ Isomorphismus, so gilt $\varphi(t) = g(t) \in R[t],\ t = \varphi(f(t))$ mit

$$1 = \deg(t) = \deg(f(g(t)) = \deg(f)\, \deg(g).$$

Also muß $\deg(f) = \deg(g) = 1$ sein, d.h. $g(t) = at + b,\ f(t) = ct + d$ ($a, b, c, d \in R$). Aus

$$\begin{aligned} t &= f(g(t)) \\ &= c(at + b) + d \\ &= cat + bc + d \ \Rightarrow\ 1 = ac \wedge 0 = bc + d \end{aligned}$$

folgt $a \in U(R)$, also die behauptete Form für φ.

□

53. Definition

Es sei Λ ein unitärer Oberring des Ringes R. Ein Element $x \in \Lambda$ heißt algebraisch über R, falls die Abbildung $\varphi_x : R[t] \to \Lambda$ nicht injektiv ist, d.h. es existiert ein Polynom $f(t) \in R[t]$ mit $f(x) = 0$. Andernfalls heißt $x \in \Lambda$ transzendent über R.

Bemerkung:
x algebraisch $\Leftrightarrow$ x Nullstelle eines Polynoms aus $R[t]$.

Beispiele:
$\sqrt{2} \in \mathbb{R}$ ist algebraisch über $\mathbb{Z}$ als Nullstelle von $f(x) = x^2 - 2$.
$e, \pi \in \mathbb{R}$ sind transzendent über $\mathbb{Z}$ bzw. $\mathbb{Q}$ (ohne Beweis).

54. Hilfssatz

Es seien R ein kommutativer Ring mit 1, $f(t) \in R[t]$ mit $\deg(f) \geq 1$ und Λ ein unitärer Oberring von R. $x \in \Lambda$ ist genau dann Nullstelle von $f(t)$, wenn $(t-x)$ das Polynom $f(t)$ in $\Lambda[t]$ teilt.

Beweis:
Division mit Rest ist in $\Lambda[t]$ durchführbar, da $l(t-x)$ Einheit in Λ ist! Also folgt

$$f(t) = Q(f,\, t-x)\,(t-x) + R(f,\, t-x)$$

mit $\deg(R(f,\, t-x)) < \deg(t-x) = 1$, also ist $R(f,\, t-x) \in \Lambda$ konstant.

Nun spezialisieren wir $t \mapsto x$:

$$\begin{aligned} x \text{ Nullstelle} &\Leftrightarrow 0 = f(x) \\ &\Leftrightarrow R(f,\, t-x)\,(x) = 0 \\ &\Leftrightarrow R(f,\, t-x) = 0. \end{aligned}$$

□

Zur Division mit Rest in beliebigen Polynomringen (Pseudodivision) vgl. Übungen, Blatt 9.

Beispiel:
Für $R = \mathbb{Z}$ ist die Division $(t^3-2) \;:\; (2t-1)$ in $R[t]$ nicht durchführbar.

Jedoch gilt:

$$2^3(t^3-2) = (4t^2+2t+1)\,(2t-1) + -15 \text{ in } \mathbb{Z}[t].$$

55. Satz

Der Polynomring $K[t]$ über einem Körper K ist ein euklidischer Ring.

Beweis:
Mittels euklidischem Algorithmus mit $v = \deg$.

□

Speziell ist $K[t]$ also Hauptidealring und ZPE-Ring, und für ein irreduzibles Polynom $f(t)$ aus $K[t]$ ist $K[t]/f(t)K[t]$ wieder ein Körper. In $K[t]$ ist die Anzahl der Wurzeln eines Polynoms — der Vielfachheit entsprechend gezählt — kleiner gleich dem Grad. Dasselbe gilt über Integritätsringen, sonst ist diese Aussage i.a. falsch: t^2-1 hat in $\mathbb{Z}/8\mathbb{Z}[t]$ Nullstellen $\overline{1}$, $\overline{3}$, $\overline{5}$, $\overline{7}$, also $t^2-1 = (t-\overline{1})\,(t-\overline{7}) = (t-\overline{3})\,(t-\overline{5})$.

56. Hilfssatz

Es sei R kommutativer Ring mit 1. Dann gilt:

$$R[t] \text{ Hauptidealring} \quad \Leftrightarrow \quad R \text{ Körper.}$$

Beweis: " $\Leftarrow$" Klar!
" $\Rightarrow$" Betrachte

$$\varphi_0 \,:\, R[t] \to R \,:\, f(t) \mapsto f(0).$$

Es gilt: $R[t]$ Hauptidealring $\Rightarrow$ $R[t]$ Integritätsring $\Rightarrow$ R Integritätsring.

Ferner ist $R \cong R[t]/\ker \varphi_0$, also ist $\ker \varphi_0$ Primideal und damit im Hauptidealring $R[t]$ maximal, also ist $R[t]/\ker \varphi_0$ Körper.

□

Bemerkung:
Polynomringe in mehr als einer Variablen sind folglich keine Hauptidealringe. Dagegen vererben sich die Eigenschaften "noethersch" und "faktoriell" von R auf $R[t]$. Die letzte Aussage ist eine Konsequenz von (2.57).

57. Satz (Gauß)

Für einen ZPE-Ring R ist auch $R[t]$ ein ZPE-Ring.

Der Beweis erfolgt in mehreren Schritten.

58. 1. Hilfssatz

Es sei R ein kommutativer Ring mit 1. Ist $\mathfrak{a}$ ein (Prim-)Ideal von R, so ist $\mathfrak{a}[t]$ (Prim-)Ideal in $R[t]$.

Beweis:
Idealeigenschaft von $\mathfrak{a}[t]$ ist unmittelbar einsichtig. Es sei nun $\mathfrak{a}$ ein Primideal von R. Sind dann $f(t) = \sum_{i=0}^{n} a_i t^i$, $g(t) = \sum_{j=0}^{m} b_j t^j \in R[t]\backslash\mathfrak{a}[t]$, so haben f, g Koeffizienten a_i, $b_j \notin \mathfrak{a}$; hierbei wählen wir Indizes i, j minimal.Für den Koeffizienten von t^{i+j} in $f \cdot g$ erhalten wir dann:

$$c_{i+j} := \sum_{k=0}^{i+j} a_k\, b_{i+j-k} \equiv a_i b_j \bmod \mathfrak{a},$$

also $c_{i+j} \notin \mathfrak{a}$, also $f \cdot g \notin \mathfrak{a}[t]$.

□

59. Definition

Es sei R ein ZPE-Ring und $f(t) \in R[t]$ mit $\deg(f) \geq 0$.

$$I(f) := \mathrm{ggT}(a_0, \ldots, a_n) \quad \text{heißt für} \quad f(t) = \sum_{i=0}^{n} a_i\, t^i$$

Inhalt von f; für $I(f) = 1$ heißt f primitiv.

Bemerkung:
Jedes Polynom $f(t) \in R[t]$ mit $\deg(f) \geq 0$ läßt sich in der Form $f(t) = I(f)\, f_p(t)$ schreiben, wobei $f_p(t) \in R[t]$ primitiv ist.

60. 2. Hilfssatz

Über einem ZPE-Ring R ist das Produkt zweier primitiver Polynome primitiv.

Beweis:
Es seien $f(t)$, $g(t) \in R[t]$ primitiv und $h = f\,g$. Für $I(h) \notin U(R)$ existiert ein Primelement $\pi \in R$, welches sämtliche Koeffizienten von h teilt. Hierfür ist $R\pi$ ein Primideal (wegen (2.41)), also auch $R\pi[t]$ gemäß (2.57). Wegen $f\,g \in R\pi[t]$ ist entweder $f(t)$ oder $g(t)$ in $R\pi[t]$ enthalten, d.h. sämtliche Koeffizienten von f oder g sind durch π teilbar im Widerspruch zu $I(f) = I(g) = 1$.

□

Bemerkung:
Für beliebige Polynome f, g über einem ZPE-Ring R ist der Inhalt ihres Produkts gleich dem Produkt von $I(f)$ und $I(g)$, d.h. $I(fg) = I(f)\, I(g)$. Dies folgt unmittelbar aus dem letzten Hilfssat und der Bermerkung davor.

61. Lemma (Gauß)

Es sei R ein ZPE-Ring mit Quotientenkörper $K = \mathfrak{Q}(R)$. Gilt dann für $h(t) \in R[t]$, $\deg(h) \geq 0$, in $K[t]$ die Zerlegung $h = f_1 f_2$, so existiert in $R[t]$ eine Zerlegung $h = c g_1 g_2$ mit primitiven Polynomen g_1, g_2, $c \in R$, und es existieren $\alpha_i \in K$ mit $\alpha_i f_i = g_i$ $(i = 1, 2)$.

Beweis:
Es sei λ_i kgV der Nenner der Koeffizienten von f_i $(i = 1, 2)$, sowie $\mu_i := I(\lambda_i f_i)$. Also erhalten wir für die primitiven Anteile $g_i := (\lambda_i f_i)_p$

$$\lambda_1 \lambda_2\, h = \mu_1 \mu_2\, g_1 g_2.$$

Es folgt $\lambda_1 \lambda_2\, I(h) = \mu_1 \mu_2$, also $\mu_1 \mu_2 = (\lambda_1 \lambda_2)\, c$ $(c \in R)$ und damit die Behauptung.

□

Bemerkung:

(1) Ist $f \in R[t]\backslash R$ irreduzibel, so ist f auch in $\mathfrak{Q}(R)[t]$ irreduzibel.
Beispiel: $t^2 - n$ ist irreduzibel über $\mathbb{Z}$ für $n \notin \{x^2 \mid x \in \mathbb{Z}\}$. Dies bedingt $\sqrt{n} \notin \mathbb{Q}$.
Die Umkehrung lautet: Ist $f(t) \in R[t]\backslash R$ reduzibel in $K[t]$, dann auch in $R[t]$.
(2) Sind $f,\ g \in R[t],\ f \neq 0,\ g$ primitiv mit $g|f$ in $K[t]$, so gilt $g|f$ bereits in $R[t]$. ($f = h \cdot g$ in $K[t] \overset{(2.60)}{\Rightarrow} f = c \cdot h,\ c \in R,\ h \in R[t] \Rightarrow$ Behauptung.)
(3) Zwei primitive Polynome $f,\ g \in R[t]$ sind genau dann in $K[t]$ assoziiert, falls sie es in $R[t]$ sind. ($f = c \cdot g \Leftrightarrow f = \tilde{c}\hat{c}\, g,\ \tilde{c}\hat{c} \in U(R)$.)

Beweis zu (2.57):
Die irreduziblen Elemente von $R[t]$ sind von zweierlei Gestalt:
(1) irreduzible Elemente aus R,
(2) irreduzible Polynome $f(t) \in R[t]$ mit $\deg(f) \geq 1$.

$R[t]$ ist Integritätsring mit 1, da R es ist. Sei nun $f(t) \in R[t]$ vorgelegt. O.B.d.A. können wir $\deg(f) > 0$ annehmen. Dann existiert im ZPE-Ring $K[t]$ mit $K = \mathfrak{Q}(R)$ eine Faktorisierung von f in irreduzible Elemente: $f = \tilde{q}_1 \cdot \ldots \cdot \tilde{q}_r$ mit $\tilde{q}_i \in K[t]$. Mittels (2.61) erhalten wir hieraus eine Faktorisierung

$$f = c\, q_1 \cdot \ldots \cdot q_r \text{ mit } q_i = \alpha_i \tilde{q}_i \ (1 \leq i \leq r)$$

aus $R[t]$ primitiv und irreduzibel, $c \in R$. c besitzt jedoch nach Voraussetzung eine Zerlegung in irreduzible Elemente in R.
Hat f in $R[t]$ nun zwei solche Zerlegungen

$$f = \tilde{c}\, q_1 \cdot \ldots \cdot q_r = tc\, p_1 \cdot \ldots p_s \ \ (\deg(q_i) > 0,\ \deg(p_j) > 0),$$

dann sind q_i, p_j auch in $K[t]$ irreduzibel, also gilt $r = s$ und — bei passender Numerierung — $q_i = \alpha_i p_i$ ($\alpha_i \in K,\ 1 \leq i \leq r$). Damit sind die q_i und p_i in $R[t]$ assoziiert, und es folgt $c \sim \tilde{c}$ und — wegen R ZPE-Ring — die Behauptung.

□

Bemerkung: Ist R ZPE-Ring, so auch $R[t_1, \ldots, t_n]$.

Als Bausteine sind die irreduziblen Polynome in ZPE-Ringen $R[t]$ von Interesse.

Bemerkung: $(at + b) \mid \left(\sum_{i=0}^{n} a_i\, t^{n-i} \right) \Rightarrow a|a_0,\ b|a_n.$

Beispiel:
Für welche $a \in \mathbb{Z}$ ist $f(t) = t^5 + at + 1$ in $\mathbb{Q}[t]$ irreduzibel?
Die Entscheidung fällt bereits in $\mathbb{Z}[t]$! f ist primitiv!
Existenz von Nullstellen: $f(\pm 1) = \left\{ \begin{smallmatrix} 2+a \\ -a \end{smallmatrix} \right\}$, also ist f reduzibel für $a \in \{0, -2\}$.

Quadratische Faktoren:

$$t^5 + at + 1 = (t^2 + \alpha\, t + \beta)\,(t^3 + \gamma\, t^2 + \delta\, t + \varepsilon)$$

$\Rightarrow \quad \alpha + \gamma = 0,\ \delta + \alpha\,\gamma + \beta = 0,\ \varepsilon + \alpha\,\delta + \beta\,\gamma = 0,\ \alpha\,\varepsilon + \beta\,\delta = a,\ \beta\,\varepsilon = 1$

$\Rightarrow \quad \gamma = -\alpha,\ \delta = \alpha^2 - \beta,\ \varepsilon = \alpha\,(2\beta - \alpha^2),$

Damit: $\beta = \varepsilon = 1 \quad \Rightarrow \quad a = 1\ (\alpha = 1,\ \gamma = -1, \delta = 0)$

$\beta = \varepsilon = -1 \quad \Rightarrow$ keine Lösung ($-1 = -\alpha\,(2 + \alpha^2) \ \Rightarrow\ 1 = \alpha\,(2 + \alpha^2)$ Widerspruc

62. Satz (Irreduzibilitätskriterium von Eisenstein)

Es sei R ein ZPE-Ring und

$$f(t) = \sum_{i=0}^{n} a_i\, t^i \ \in R[t]$$

mit $\deg(f) \geq 1$. Gibt es dann ein Primelement $\pi \in R$ mit $\pi | a_i$ $(0 \leq i < n)$, $\pi^2 \nmid a_0$ und $\pi \nmid a_n$, so ist $f(t)$ in $\mathfrak{Q}(R)[t]$ irreduzibel.

Beweis: Indirekt!

Ist $f(t)$ in $\mathfrak{Q}(R)[t]$ echt zerlegbar, dann auch nach (2.60) in $R[t]$. Wir nehmen daher in $R[t]$ an: $f(t) = g(t)\,h(t)$ mit $\deg(g) \cdot \deg(h) > 0$, etwa

$$g(t) = \sum_{i=0}^{d} b_i\, t^i, \quad h(t) = \sum_{j=0}^{m} c_j\, t^j.$$

Speziell gilt dann:

$$a_i := \sum_{\substack{k=0 \\ k \leq d \\ i-k \leq m}}^{i} b_k\, c_{i-k}.$$

Aus $a_0 = b_0 c_0$ und $\pi | a_0,\ \pi^2 \nmid a_0$ folgt o.B.d.A. $p | b_0,\ p \nmid c_0$.

Wir zeigen induktiv: $p | b_j$ $(1 \leq j \leq d)$. Für $d \geq i > 0$ gilt ja:

$$a_i = \sum_{\substack{k=0 \\ i-k \leq m}}^{i} b_k\, c_{i-k} = \sum_{\substack{k=0 \\ i-k \leq m}}^{i-1} b_k\, c_{i-k} + b_i\, c_0 \equiv 0 \bmod \pi$$

nach Induktionsannahme, also $\pi | b_i c_0$ und wegen $\pi \nmid c_0$ folglich $\pi | b_i$. Für $i = d$ folgt $\pi | b_d c_n = a_n$. Widerspruch!

□

Beispiel:

(1) $t^n - a$ ($a \in \mathbb{Z}$, $\exists$ Primzahl p mit $p | a,\ p^2 \nmid a$) ist in $\mathbb{Q}[t]$ (und $\mathbb{Z}[t]$) irreduzibel. ($\sqrt[n]{a}$ ist in diesem Fall irrational!)

(2) In $\mathbb{Q}[t]$ sind gemäß (2.61) irreduzibel:

$$\begin{aligned} f_1(t) &= 3\,t^5 - 15 \quad (p = 5), \\ f_2(t) &= 2\,t^{10} - 21 \quad (p = 3,\ 7), \\ f_3(t) &= 5\,t^5 - 12\,t^4 + 24\,t^3 + 2\,t^2 - 4\,t + 34 \quad (p = 2). \end{aligned}$$

Hierbei sind allerdings nur die beiden letzten Polynome $f_2,\ f_3$ auch in $\mathbb{Z}[t]$ irreduzibel ($f_1(t) = 3\,(t^5 - 5),\ 3 \notin U(\mathbb{Z})$).

(3) p-te Einheitswurzeln sind Nullstellen von $t^p - 1$, sie bilden eine zyklische Gruppe der Ordnung p. $t^p - 1$ ist reduzibel $(t-1) \mid (t^p - 1)$.

$$\frac{t^p - 1}{t - 1} = \sum_{i=0}^{p-1} t^i =: \Phi_p(t)$$

heißt <u>p-tes Kreisteilungspolynom</u>.

$\Phi_p(t)$ irreduzibel $\Leftrightarrow$ $\Phi_p(t+1)$ irreduzibel; dies gilt, weil $\varphi : R[t] \to R[t] : t \mapsto t+1$ Ringisomorphismus ist.

Es gilt

$$\begin{aligned}\Phi_p(t+1) &= \frac{(t+1)^p - 1}{t} \\ &= \frac{\sum_{i=0}^{p} \binom{p}{i} t^i - 1}{t} \\ &= t^{p-1} + \sum_{i=1}^{p-1} \binom{p}{i} t^{i-1},\end{aligned}$$

und für $a_{i-1} := \binom{p}{i},\ a_0 = p$ erhalten wir $p | a_0,\ p^2 \nmid a_0$,

$\binom{p}{i} = \frac{p \cdot (p-1) \cdot \ldots \cdot (p-i+1)}{i \cdot \ldots \cdot i} \equiv 0 \bmod p \quad (1 \le i \le p-1)$, also folgt

$p \left| \binom{p}{i} \right. = a_{i-1}\ (1 \le i \le p-1),\ p \nmid a_{p-1} = 1 \ \Rightarrow\ \Phi_p(t)$ irreduzibel.

63. Satz (Reduktion)

Es seien R, S zwei Integritätsringe mit 1 und $\varphi : R \to S$ ein Ringhomomorphismus mit $\varphi(1_R) = 1_S$. Dann läßt sich φ kanonisch zu einem Ringhomomorphismus $\Phi : R[t] \to S[t]$ mit $\Phi|_R = \varphi$ fortsetzen. Es sei $f(t) \in R[t]$ mit $\deg(\Phi(f)) = \deg(f) > 0$. Ist dann $\Phi(f)$ in $S[t]$ irreduzibel, so ist f in $R[t]$ nicht als Produkt $f = g\,h$ mit $\deg(g)\ \deg(h) > 0$ darstellbar.

<u>Beweis:</u>

(1)

$$\Phi : R[t] \to S[t] : \sum_{i=0}^{n} a_i\, t^i \mapsto \sum_{i=0}^{n} \varphi(a_i)\, t^i$$

hat $\ker \Phi = \ker(\varphi)[t]$ wegen $\Phi|_R = \varphi$.

(2) Ist $f = g\,h$ eine echte Zerlegung, d.h. $(\deg(g)\,\deg(h) > 0)$ in $R[t]$, so ist $\Phi(f) = \Phi(g)\,\Phi(h)$ und $\deg(\Phi(g)) \leq \deg(g),\ \deg(\Phi(h)) \leq \deg(h)$. Wegen $\deg(\Phi(f)) = \deg(f)$ und S Integritätsring liefert ein Gradvergleich, daß $\Phi(g)\,\Phi(h)$ echte Zerlegung von $\Phi(f)$ ist. Widerspruch.

□

Anwendung:
Bei Irreduzibilitätstests in $\mathbb{Z}[t]$!
$R = \mathbb{Z},\ S = \mathbb{Z}/p\mathbb{Z},\ p$ Primzahl mit $p \nmid l(f)$.

Beispiele:

(1) $f(t) = t^3 + 39t^2 - 4t + 8 \in \mathbb{Z}[t]$,
$p = 3\ :\ \Phi(f) = t^3 - t - 1$ ist in $\mathbb{Z}/3\mathbb{Z}$ irreduzibel, da es dort keine Nullstelle besitzt.

(2) $f(t) = t^2 + (10^{170} + 1)t + (10^{54821} + 343) \in \mathbb{Z}[t]$,
$p = 2\ :\ \Phi(f) = t^2 + t + 1$ ist in $\mathbb{Z}/2\mathbb{Z}$ irreduzibel.
(Dagegen ist eine Bestimmung der Teiler von $f(0)$ praktisch unmöglich.)

Lösen von Gleichungen:
Gegeben sei ein Polynom $f(t) \in R[t],\ R$ kommutativer Ring mit 1,

$$f(t) = \sum_{i=0}^{n} a_i\, t^{n-i}.$$

Problem:

Bestimme $x \in R$ oder aus einem unitären Oberring Λ von R mit $f(x) = 0$. Ist a_0 kein Nullteiler, dann liefert Multiplikation mit a_o^{n-1}:

$$(a_0x)^n + a_1\,(a_0x)^{n-1} + \ldots + a_n a_0^{n-1} = 0,$$

und jede Lösung $y \in R$ von

$$y^n + a_1 y^{n-1} + \ldots + a_n a_0^{n-1} = 0$$

liefert eine Lösung $x = \dfrac{y}{a_0}$ in $\mathfrak{Q}(R)$.

Also genügt es, $f(t)$ als normiert $a_n = 1$) anzunehmen. Ein unitärer Oberring Λ von R, in dem f ein Nullstelle besitzt, heißt Lösungsring der Gleichung $f(x) = 0$.

64. Lemma

Es sei R ein kommutativer Ring mit 1 und $f(t) \in R[t]$ normiert mit $\deg(f) \geq 1$. Dann ist $\Lambda := R[t]/(f)$ ein Ring, in dem f eine Nullstelle besitzt. Außerdem läßt sich R in Λ einbetten.

Beweis:

Λ besitzt über R eine Basis $t^\nu/(f)$ $(0 \leq \nu < \deg(f))$, da sich jedes Polynom $g \in R[t]$ in der From

$$g = Q(g,\, f)\, f + R(g,\, f) \quad \text{mit} \quad \deg(R(g,\, f)) < \deg(f)$$

schreiben läßt. Also existiert in Λ ein Repräsentantensystem, das aus jeder Restklasse ein Polynom vom Grad $< \deg(f)$ enthält, was sich also aus den t^ν $(0 \leq \nu < \deg(f))$ linear (mit Koeffizienten aus R) kombinieren läßt. Eine solche Darstellung ist überdies eindeutig, da die Differenz zweier ungleicher Polynome vom Grad $< \deg(f)$ ein Polynom vom Grad ≥ 0 und $< \deg(f)$ ergibt, welches folglich nicht die Nullrestklasse repräsentiert. Überdies gilt offenbar $f(x) = 0$ für $x = t/(f)$. Eine Einbettung von R in Λ erfolgt mittels

$$\tau \,:\, R \to \Lambda \;:\mapsto a + (f).$$

□

Bemerkung:
Der Ring $\Lambda = R[t]/(f)$ hat die folgenden 3 Eigenschaften:

(1) Λ ist unitärer Oberring von R.
(2) Λ wird über R durch eine Wurzel $x = t/(f)$ (d.h. $x \in \Lambda$) von f generiert.
(3) Für jeden Lösungsring S mit Nullstelle y von f in S existiert ein Ringhomomorphimus

$$\varphi \,:\, \Lambda \to S \;:\; x \mapsto y \quad (\varphi(x) = y,\ \varphi(1) = 1).$$

Ein Ring mit diesen drei Eigenschaften wird Ring der Gleichung $f(x) = 0$ genannt.

Beispiele:

(1) Es seien $R = \mathbb{Z}/8\mathbb{Z} = \{0, \ldots, 7\}$ und $f(t) = t^2 - 1 \in R[t]$. $\Lambda = R[t]/(f)$ besitzt als R-Basis $1/(f)$, $t/(f) =: x$. Anderseits ist $S = \mathbb{Z}/8\mathbb{Z}$ selbst Lösungsring, folglich existiert ein Ringhomomorphismus $\varphi \,:\, \Lambda \to R$ mittels $t/(f) \mapsto \alpha$, $\alpha \in \{1, 3, 5, 7\}$

$$\begin{array}{ccc}
a\,1/(f) + b\,t(f) & \mapsto & a + \alpha\, b \\
(a\,1(f) + b\,t/(f))\,(c\,1/(f) + d\,t/(f)) & \mapsto & (a + \alpha\, b)\,(c + \alpha\, d) \\
\| & & \| \\
(ac + bd)\,1/(f) + (ad + bc)\,t/(f) & & (ac + \alpha^2 bd) + \alpha\,(ad + bc) \\
\| & & \| \\
(ac + bd)\,1/(f) + (ad + bc)\,t/(f) & & (ac + bd) + \alpha\,(ad + bc).
\end{array}$$

(2) $f(t) = t^3 + pt^2 + qt + r$ zerfalle in $\Lambda[t]$ gemäß

$$\begin{aligned}
f(t) &= (t - x)\,(t^2 + at + b), \text{ also} \\
f(t) &= (t - x)\,(t^2 + (p + x)\,t + q + x\,(x + p)) \\
&\Rightarrow\ r = -x\,(x\,(x + p) + q) \text{ in } R[t]/(f).
\end{aligned}$$

(3) $t^2 + m$ sei irreduzibel über R (etwa $m = 1$, $R = \mathbb{R}$ oder $m = -2$, $R = \mathbb{Z}/5\mathbb{Z}$). $R[t]/(f)$ hat Basis 1, t. Es ist

$$R[t]/(f) \cong R \times R.$$

Wie sieht die Ringstruktur auf $R \times R$ aus?

$$\begin{aligned}(a + tb) \cdot (c + td) &= ac - mbd + t\,(bc + da),\\ (a,\, b) \cdot (c,\, d) &= (ac - mbd,\, bc + da),\end{aligned}$$

$$f((0,\, 1)) = (0,\, 1)^2 + (m,\, 0) = (-m + m,\, 0) = 0.$$

65. Korollar

Durch iterierte Anwendung der Konstruktion aus (2.63) erhält man $S(f,\, R)$, den sogenannten Zerfällungsring von f über R, mit $n!$ Basiselementen über R, $n = \deg(f)$.

66. Hilfssatz

Es sei K ein Körper und $f \in K[t]$, $\deg(f) > 0$. Dann exitiert ein Erweiterungskörper L von K, besitzt. Auin dem f eine Nullstelle besitzt.

Beweis:
Es sei $g \in K[t]$ ein irreduzibler Faktor von f mit $\deg(g) \geq 1$, d.h. $f = p \cdot g$, $p \in K[t]$. Da $K[t]$ Hauptidealring ist, ist g Primideal und (g) maximales Ideal. Folglich ist $L := K[t]/(g)$ ein Körper, in dem g (und damit f) eine Nullstelle besitzt, d.h. die Restklasse von t, $t + (g)$, ist Nullstelle von f in L wegen $f = p \cdot g \in (g)$.

□

67. Satz

Es seien K ein Körper und $f(t) \in K[t]$ mit $\deg(f) = n > 0$. Dann exitiert ein Erweiterungskörper L von K, in dem f Produkt von $l(f)$ und n normierten Polynomen ersten Grades ist:

$$f(t) = l(t) \prod_{i=1}^{n} (t - x_i) \text{ in } L[t],\ x_i \in L.$$

Speziell enthält L alle Nullstellen von f.

Beweis: Per Induktion über $n = \deg(f)$!
$n = 0$: $f = l(f)$, das Produkt über normierte Polynome ersten Grades ist hier leer.

$n \Rightarrow n + 1$:
Gemäß (2.65) exitiert ein Erweiterungskörper L_1 von K, in dem f eine Nullstelle hat.

$$f(t) = (t - x_1)\, g(t) \text{ in } L_1[t],\ \deg(f) = n + 1,\ x_1 \in L_1,\ \deg(g) = n.$$

Nach Induktionsvoraussetzung gibt es einen Erweiterungkörper L von L_1, in dem g zerfällt:

$$g = l(g) \prod_{i=2}^{n+1} (t - x_i) \ \in L[t],\ x_2, \ldots, x_{n+1} \in L,$$

und es folgt

$$f = (t - x_1) \cdot l(g) \cdot \prod_{i=2}^{n+1} (t - x_i) = l(f) \cdot \prod_{i=1}^{n+1} (t - x_i) \ \in L[t].$$

□

Beispiel:
Es sei $f \in K[t],\ f$ normiert, f zerfällt in L mit $x_i \in L$ wie folgt:

$$\begin{aligned} f &= \prod_{i=1}^{n} (t - x_i) \\ &= (t - x_1)\,(t - x_2)\,\ldots\,(t - x_n) \\ &= t^n - t^{n-1} \sum_{i=1}^{n} x_i + t^{n-2} \sum_{i<j} x_i\, x_j \\ &\quad + \ldots + (-1)^{n-k} t^k \sum_{1 \le i_1 < i_2 < \ldots < i_k \le n} x_{i_1} \cdot \ldots \cdot x_{i_{n-k}} + \ldots + (-1)^n\, x_1 \cdot \ldots \cdot x_n. \end{aligned}$$

68. Definition

Es sei R ein kommutativer Ring mit 1. Ein Polynom

$$f(\underline{t}) \in R[\underline{t}] \quad (\underline{t} = (t_1, \ldots, t_n))$$

heißt symmetrisch, falls

$$f(t_1, \ldots, t_n) = f(t_{\pi(1)}, \ldots, t_{\pi(n)})$$

für alle $\pi \in \mathfrak{S}_n$ gilt. Speziell heißen

$$\begin{aligned} \sigma_0(\underline{t}) &:= 1 \\ \sigma_j(\underline{t}) &:= \sum_{1 \le i_1 < i_2 < \ldots < i_j \le n} t_{i_1} \cdot \ldots \cdot t_{i_j} \quad (1 \le j \le n) \end{aligned}$$

elementarsymmetrische Funktionen in $t_1, \ldots, t_n$ ($\sigma_j = \sigma_j^{(n)}$).

Beispiele:

(1)

$$\begin{aligned} \sigma_1 = t_1 + \ldots + t_n, \\ \sigma_2(t_1, t_2, t_3) &= t_1 t_2 + t_1 t_3 + t_2 t_3, \\ \sigma_n(t_1, \ldots, t_n) &= t_1 \ldots t_n. \end{aligned}$$

(2) Potenzsummen:

$$\begin{aligned} S_k(\underline{t}) &:= \sum_{j=1}^{n} t_j^k \quad (\underline{\text{Potenzsummen}}),\ (k \in \mathbb{Z}^{\geq 0}), \\ S_2(\underline{t}) &= t_1^2 + \ldots + t_n^2 \\ &= (t_1 + \ldots + t_n)^2 - 2\sum_{i<j} t_i\, t_j. \end{aligned}$$

(3) Zusammenhang:

$$\begin{aligned} S_2 &= \sigma_1^2 - 2\sigma_2 \\ &= \sigma_1\, S_1 - 2\sigma_2, \end{aligned}$$

also für $n = 2$:

$$\begin{aligned} \sigma_2(\underline{t}) &= t_1^2 + t_2^2 \\ &= (t_1 + t_2)^2 - 2t_1t_2 \\ &= \sigma_1(\underline{t})^2 - 2\,\sigma_2(\underline{t}). \end{aligned}$$

(4)

$$\begin{aligned} f(t_1, \ldots, t_n, t) &:= \prod_{i=1}^{n}(t - t_i) \\ &= \sum_{j=0}^{n}(-1)^{n-j}\,\sigma_{n-j}(\underline{t})\,t^j, \end{aligned}$$

$$\sum_{i=0}^{n}(-1)^i\,\sigma_i(\underline{t})\,t^{n-i}.$$

(5) Es sei $A \in M_n(\mathbb{C})$ und

$$J_c = \begin{pmatrix} \lambda_1 & *_1 & & \\ & \ddots & \ddots & \\ & & \ddots & *_{n-1} \\ & & & \lambda_n \end{pmatrix}$$

mit λ_i Eigenwert zu A $(1 \leq i \leq n)$ und $*_j \in \{0, 1\}$ $(1 \leq j \leq n-1)$.

$$\begin{aligned} f_A &= \det(t - J_c) \\ &= \prod_{i=1}^{n} t - \lambda_i) \\ &= \sum_{j=0}^{n}(-1)^j\,\sigma_j(\lambda_1 \ldots \lambda_n)\,t^{n-j} \end{aligned}$$

$$\sigma_1(\lambda_1 \ldots \lambda_n) = \mathrm{Sp}(A), \quad \sigma_n(\lambda_1 \ldots \lambda_n) = \det A.$$

(6)

$$\sigma_k^{(n)}(t_1 \ldots t_n) = \sigma_k^{n+m)}(t_1 \ldots t_n, \underbrace{0 \ldots 0}_{m}).$$

Bemerkung:
Die symmetrischen Polynome bilden einen Unterring von $R[t_1 \dots t_n]$. Der Einsetzungshomomorphismus

$$\Phi_{(\sigma_1 \dots \sigma_n)} \; : \; R[t_1 \; \dots \; t_n] \to R[t_1 \; \dots \; t_n]$$

$\Phi(f) = f(\sigma_1, \dots, \sigma_n)$ ist symmetrisch.

69. Satz (Hauptsatz über elementarsymmetrische Funktionen)

Es sei R ein kommutativer Ring mit 1. Dann ist jedes symmetrische Polynom $f(\underline{t}) \in R[\underline{t}]$ gleich $g(\sigma_1, \dots, \sigma_n)$ für ein eindeutig bestimmtes Polynom $g \in R[\underline{t}]$.

Beweis:
Wir definieren das Gewicht eines Monoms

$$g(\underline{t}) = a\, t_1^{m_1} \cdot \dots \cdot t_n^{m_n} \text{ als } w(t_k) = k, \; w(g) := \sum_{i=1}^{n} i\, m_i.$$

Das Gewicht eines Polynoms $f \in R[\underline{t}]$ wird dann als Maximum der Gewichte seiner Monome festgelegt, d.h.

$$f = \sum a_{i_1 \dots i_n}\, t_1^{i_1} \dots t_n^{i_n}, \quad w(f) = \max\{w(t_1^{i_1} \dots t_n^{i_n}).$$

(1) Wir zeigen: Zu $f \in R[\underline{t}]$ symmetrisch vom Grad d existiert $g \in R[t]$ mit $w(g) \le d$ und $f(t_1, \dots, t_n) = g(\sigma_1, \dots, \sigma_n)$.

Der Beweis erfolgt mittels Induktion nach n.
Für $n = 1$ ist $f = g$ und $\sigma_1 = t_1$.
$n - 1 \Rightarrow n$: Beweis per Induktion nach $d = \deg(f)$.
Für $d \le 0$ ist f konstant und $g = f$ tut's.
Sei also $d > 0$.
$d - 1 \Rightarrow d$: Dann ist

$$f^{(n-1)}(t_1, \dots, t_{n-1}) := f(t_1, \dots, t_{n-1}, 0)$$

vom Grad $\deg(f^{(n-1)}) \le d$ symmetrisch in $t_1, \dots, t_{n-1}$. Nach Induktionsvoraussetzung über n existiert also ein Polynom $g_1(t_1, \dots, t_{n-1}) \in R[t_1, \dots, t_{n-1}]$ vom Gewicht $\le d$ mit

$$f^{(n-1)}(t_1, \dots, t_{n-1}) = g_1(\sigma_1^{(n-1)}, \dots, \sigma_{n-1}^{(n-1)}),$$

wobei $\sigma_i^{(n-1)} = \sigma_i(t_1, \dots, t_{n-1}, 0)$ gesetzt wurde.
Hiernach ist

$$h(\underline{t}) := f(\underline{t}) - g_1(\sigma_1, \dots, \sigma_{n-1})$$

ebenfalls symmetrisch vom Grad $\le d$. Wegen $h(\underline{t})$ symmetrisch und $h(t_1, \dots, t_{n-1}, 0) = 0$ folgt $\sigma_n | h$, bzw. $h = \sigma_n h_1$, $\deg(h_1) = \deg(h) - n$. Wiederum ist h_1 symmetrisch vom Grad $d - n < d$.

Nach Induktionsannahme existiert daher $g_2 \in R[t_1, \ldots, t_n]$ vom Gewicht $\leq d - n$ mit

$$h_1(t_1, \ldots, t_n) = g_2(\sigma_1, \ldots, \sigma_n),$$

und insgesamt leistet

$$g(\sigma_1, \ldots, \sigma_n) = g_1(\sigma_1, \ldots, \sigma_{n-1}) + \sigma_n \, g_2(\sigma_1, \ldots, \sigma_n)$$

das Verlangte.

(2) Eindeutigkeit:

Dazu zeigen wir: Für $f \in R[t_1, \ldots, t_n]$ mit $f(\sigma_1, \ldots, \sigma_n) = 0$ gilt $f = 0$.

Der Beweis erfolgt per Induktion über n.

Für $n = 1$ ist die Aussage wegen $\sigma_1 = t_1$ trivial.

Sei also $n > 1$ und $f \neq 0$ von minimalem Grad > 0 mit $f(\sigma_1, \ldots, \sigma_n) = 0$. Aus dem Ansatz

$$f(t_1, \ldots, t_n) = \sum_{i=0}^{l} f_i(t_1, \ldots, t_{n-1}) \, t_n^i$$

folgt zunächst $f_0(t_1, \ldots, t_{n-1}) \neq 0$, da sonst f durch t_n teilbar wäre, d.h.

$$f(\underline{t}) = t_n \, \tilde{f}(\underline{t}) \quad \text{mit} \quad 0 = f(\underline{\sigma}) = \sigma_n \, \tilde{f}(\underline{\sigma}),$$

im Widerspruch zur Minimalität des Grades. Daher gilt:

$$0 = f(\sigma_1, \ldots, \sigma_n) = \sum_{i=0}^{l} f_i(\sigma_1, \ldots, \sigma_{n-1}) \, \sigma_n^i.$$

Setzen wir hierin $t_n = 0$, so erhalten wir

$$0 = f(\sigma_1^{(n-1)}, \ldots, \sigma_{n-1}^{(n-1)}, 0) = f_0(\sigma_1^{(n-1)}, \ldots, \sigma_{n-1}^{(n-1)})$$

im Widerspruch zur Induktionsannahme!

□

Beispiel:

Für

$$f(t_1, t_2, t_3) = (t_1 - t_2)^2 \, (t_1 - t_3)^2 \, (t_2 - t_3)^2$$

ist

$$\begin{aligned} f(t_1, t_2, 0) &= (t_1 - t_2)^2 \, (t_1 t_2)^2 \\ &= (\sigma_1^{(2)^2} - 4 \, \sigma_2^{(2)}) \, \sigma_2^{(2)^2}; \end{aligned}$$

folglich gilt $h(\underline{t}) = \sigma_3 \, h_1(\underline{t})$ mit

$$\begin{aligned} h_1(t_1, t_2, 0) &= 18 \, \sigma_1^{(2)} \, \sigma_2^{(2)} - 4 \, \sigma_1^{(2)^3} \\ h_2(\underline{t}) &= h_1(\underline{t}) - 18 \, \sigma_1^{(3)} \, \sigma_2^{(3)} + 4 \, \sigma_1^{(3)} \\ &= -27 \, t_1 t_2 t_3 \\ &= -27 \, \sigma_3 \end{aligned}$$

$\Rightarrow$

$$f(t_1,t_2,t_3)=\sigma_1^2\,\sigma_2^2-4\,\sigma_2^3+\sigma_3\,(18\,\sigma_1\,\sigma_2-4\,\sigma_1^3-27\,\sigma_3).$$

Zusammenhang zwischen Potenzsummen und elementarsymmetrischen Funktionen:

70. Satz

Für die Potenzsummen $S_k(\underline{t})$ und die elementarsymmetrischen Funktionen $\sigma_j(\underline{t})$ gelten die "Newtonschen Relationen":

(1)

$$\sum_{i=0}^{k-1}(-1)^i\,\sigma_i(\underline{t})\,S_{k-i}(\underline{t})+k\,(-1)^k\,\sigma_k(\underline{t})=0\quad(0\le k\le n),$$

(2)

$$\sum_{i=0}^{n}(-1)^i\,\sigma_i(\underline{t})\,S_{k-i}(\underline{t})=0\quad(k\ge n).$$

Beweis:
Für

$$f(t_1,\ldots,t_n,t)=\sum_{j=0}^{n}(-1)^j\,\sigma_j(\underline{t})\,t^{n-j}=\prod_{j=1}^{n}(t-t_j)$$

gilt:

$$0=\sum_{j=0}^{n}(-1)^j\,\sigma_j(\underline{t})\,t_i^{n-j}\quad(1\le i\le n)$$

bzw.

$$0=\sum_{j=0}^{n}(-1)^j\,\sigma_j(\underline{t})\,t_i^{k-j}\quad(1\le i\le n,\ k\ge n).$$

Summation dieser n Gleichungen liefert

$$\sum_{j=0}^{n}(-1)^j\,\sigma_j(\underline{t})\,S_{k-j}(\underline{t})=0,$$

also (ii) bzw. (i) für $k=n$. Der Rest von (i) wird bei festem k mittels Induktion nach n bewiesen:

Induktionanfang: $n=k$ ist bereits gezeigt.
$n-1\Rightarrow n$:
Wir setzen

$$F(t_1,\ldots,t_n):=\sum_{i=0}^{k-1}(-1)^i\,\sigma_i(\underline{t})\,S_{k-i}(\underline{t})+k\,(-1)^j\,\sigma_k(\underline{t}).$$

Dies ist eine symmetrische Funktion vom Grad $\le k<n$. Ferner gilt

$$F(t_1,\ldots,t_n,0)=0$$

nach Induktionsannahme. Also ist $F(\underline{t})$ durch t_n — wegen der Symmetrie durch $\sigma_n(\underline{t})$ — teilbar. Wegen $\deg(F) < n$ muß F folglich identisch verschinden.

□

Beispiel:

$$\begin{aligned} S_1(\underline{t}) &= \sigma_1(\underline{t}), \\ S_2(\underline{t}) &= \sigma_1(\underline{t})\, S_1(\underline{t}) - 2\,\sigma_2(\underline{t}) \\ &= \sigma_1^2(\underline{t}) - 2\,\sigma_2(\underline{t}), \\ S_3(\underline{t}) &= \sigma_1(\underline{t})\, S_2(\underline{t}) - \sigma_2(\underline{t})\, S_1(\underline{t}) + 2\,\sigma_3(\underline{t}) \\ &= \sigma_1^3(\underline{t}) - 3\,\sigma_1(\underline{t})\,\sigma_2(\underline{t}) + 3\,\sigma_3(\underline{t}), \end{aligned}$$

usw. Sind die natürlichen Zahlen in R keine Nullteiler, so gilt in $\mathfrak{Q}(R)$ auch:

$$\begin{aligned} \sigma_1(\underline{t}) &= S_1(\underline{t}), \\ \sigma_2(\underline{t}) &= \frac{1}{2}\,(S_1(\underline{t})^2 - S_2(\underline{t})), \\ \sigma_3(\underline{t}) &= \frac{1}{3}\left(S_2(\underline{t}) - S_1(\underline{t})^3 + 3\,S_1(\underline{t})\,\frac{1}{2}\,(S_1(\underline{t})^2 - S_2(\underline{t}))\right) \\ &= \frac{1}{6}\,(2\,S_3(\underline{t}) + S_1(\underline{t})^3 - 3\,S_1(\underline{t})\,S_2(\underline{t})), \end{aligned}$$

usw.

71. Definition

In $R[\underline{t}]$ heißt

$$D(\underline{t}) = \prod_{1 \le i < j \le n} (t_i - t_j)^2$$

Diskriminante von $\underline{t}$.

Beispiel:

$t^2 + at + b,\ x_{1,2} = -\frac{a}{2} \pm \sqrt{\frac{a^2 - 4b}{4}},\ \frac{a^2 - 4b}{4} = (x_1 - x_2)^2.$

72. Hifssatz

In $R[\underline{t}]$ gilt:

$$D(\underline{t}) = \det\left((S_{i+j-2}(\underline{t})_{1 \le i,j \le n}\right).$$

Beweis in den Übungen.

73. Satz (Fundamentalsatz der Algebra)

Jedes Polynom $f \in \mathbb{C}[t]$ mit $\deg(f) \geq 1$ besitzt eine Nullstelle in $\mathbb{C}$, d.h. über $\mathbb{C}$ zerfällt f in Linearfaktoren:

$$f(t) = l(f) \prod_{j=1}^{\deg(f)} (t - x_j) \quad x_j \in \mathbb{C}).$$

"$\mathbb{C}$ ist algebraisch abgeschlossen."

Beweis:

(1) Wir führen den Beweis auf die gleiche Aussage für Polynome aus $\mathbb{R}[t]$ zurück.

Für $f \in \mathbb{C}$ bilden wir

$$g(t) := f(t)\,\overline{f}(t) \ \in \mathbb{R}[t].$$

Wir erhalten dann

$$g(t) := |l(f)|^2 \prod_{j=1}^{2\deg(f)} (t - c_j).$$

Hier ist mit c_j auch $\overline{c}_j$ Nullstelle von g (!) und wir bekommen

$$f(t) = l(f) \prod_{i=1}^{\deg(f)} (t - c_{j_i}) \quad (1 \leq j_1 < j_2 < \ldots < j_{\deg(f)} \leq 2\deg(f)).$$

(2) Wir zeigen: Jedes Polynom

$$f(t) = t^n - a_1 t^{n-1} + a_2 t^{n-2} - + \ldots + (-1)^n a_n \ \in \mathbb{R}[t]$$

mit $n \geq 1$ besitzt in $\mathbb{C}$ ein Nullstelle.

Für n ungerade folgt dies aus dem Zwischenwertsatz der Analysis.

Sei also n von der Form $2^k q$ mit $k \in \mathbb{Z}^{\geq 0}$, q ungerade, $q \in \mathbb{N}$.

Wir führen den Beweis mittels Induktion nach k.

Induktionsanfang: $k = 0$ ist bereits geklärt.

Sei nun $k \geq 1$ und die Behauptung für $1, \ldots, k-1$ bereits bewiesen.

Nach (2.66) existiert ein Erweiterungskörper K von $\mathbb{R}$ mit

$$f(t) = l(f) \prod_{j=1}^{n} (t - x_j)$$

in $K[t]$. Wir bilden nun für jede reelle Zahl r das Polynom

$$L_r(t) := \prod_{1 \leq \mu < \nu \leq n} (t - x_\mu - x_\nu - r\, x_\mu x_\nu) \ \in K[t]$$

(Laplace) (Koeffizenten von $L_r(t)$ sind symmetrisch in den Wurzeln). Hierbei ist L_r eine symmetrische Funktion in $x_1, \ldots, x_n$,

also sind die Koeffizienten reelle Polynome in den elementarsymmetrischen Funktionen $\sigma_j(\underline{x}) = (-1)^j a_j$, d.h. es gilt $L_r(t) \in \mathbb{R}[t]$. Wegen

$$\deg(L_r) = \frac{n}{2}(n-1) = 2^{k-1}q(2^k q - 1) = 2^{k-1}\tilde{q},$$

$\tilde{q}$ ungerade, besitzt L_r für jedes $r \in \mathbb{R}$ eine Nullstelle in $\mathbb{C}$. Für jedes $r \in \mathbb{R}$ existieren also Indizes μ, ν mit

$$z_r := x_\mu + x_\nu + r\, x_\mu x_\nu \ \in \mathbb{C}.$$

Da die Anzahl der Indexpaare μ, ν endlich, die der $r \in \mathbb{R}$ unendlich ist, existieren $r \neq \tilde{r}$ in $\mathbb{R}$, $1 \leq \mu < \nu \leq n$ mit

$$x_\mu + x_\nu + r\, x_\mu x_\nu,\ x_\mu + x_\nu + \tilde{r}\, x_\mu x_\nu \ \in \mathbb{C}.$$

Hieraus folgt $x_\mu + x_\nu \in \mathbb{C}$, $x_\mu x_\nu \in \mathbb{C}$, d.h. x_μ, x_ν sind Nullstellen von

$$t^2 - (x_\mu + x_\nu)\, t + x_\mu x_\nu \ \in \mathbb{C}[t],$$

also x_μ, $x_\nu \in \mathbb{C}$.

$\Rightarrow$ alle zugehörigen Wurzeln in $\mathbb{C}$ (in $\mathbb{C}$ lassen sich Wurzeln ziehen).

□

74. Korollar

Jedes Polynom $f \in \mathbb{R}[t]$ mit $\deg(f) \geq 1$ besitzt eine — bis auf Reihenfolge der Faktoren — eindeutige Darstellung

$$f(t) = l(f) \prod_{i=1}^{k} (t - c_i) \prod_{j=1}^{l} q_j(t)$$

($c_i \in \mathbb{R}$, $q_j(t) = t^2 + u_j t + v_j \in \mathbb{R}[t]$ irreduzibel $(1 \leq j \leq l)$).

Beweis:

Es seien $c_1, \ldots, c_k$ alle reellen Nullstellen von f, und es sei g durch

$$f(t) = l(f) \prod_{i=1}^{k} (t - c_i)\, g(t)$$

eindeutig bestimmt. Da für jede Nullstelle x von g wegen

$$0 = \sum_{\nu=0}^{m} g_\nu\, x^\nu = \sum_{\nu=0}^{m} \overline{g}_\nu\, \overline{x}^\nu = \sum_{\nu=0}^{m} g_\nu\, \overline{x}^\nu$$

für

$$g(t) = \sum_{\nu=0}^{m} g_\nu\, t^\nu$$

auch $\overline{x}$ Nullstelle ist, ist $\deg(g)$ gerade! Es seien $z_1, \ldots, z_l$, $\overline{z}_1, \ldots, \overline{z}_l$ alle Nullstellen von g in $\mathbb{C}$. Dann setzen wir

$$q_j(t) = t^2 - (z_j + \overline{z}_j)\, t + z_j\, \overline{z}_j \ \in \mathbb{R}[t]\ (1 \leq j \leq l).$$

Eindeutigkeit:

Ist $x_j \in \mathbb{R}$ Nullstelle von f so gilt $(t - x_j) \mid f(t)$. Ist $z_j \in \mathbb{C}\backslash\mathbb{R}$ Nullstelle von f, dann auch $\overline{z}_j$, und es gilt

$$\mathbb{R}[t] \ni \ (t^2 - (z_j + \overline{z}_j)\, t + z_j\, \overline{z}_j) \mid f(t).$$

□

75. Korollar

Die irreduziblen Elemente von $\mathbb{C}[t]$ sind die Polynome ersten Grades aus $\mathbb{C}[t]$. Die irreduziblen Elemente von $\mathbb{R}[t]$ sind die Polynome ersten Grades und diejenigen Polynome $c\,(t^2 + ut + v)$ zweiten Grades mit $u^2 - 4v < 0$.

76. Satz

Es sei K ein unitärer nullteilerfreier kommutativer Oberring von $\mathbb{R}$, in dem jedes Element algebraisch über $\mathbb{R}$ ist. Dann ist K isomorph zu $\mathbb{R}$ oder $\mathbb{C}$.

Beweis:

Es sei $K \neq \mathbb{R}$. Für $x \in K\backslash\mathbb{R}$ ist $V := \mathbb{R}1 + \mathbb{R}x$ ein zweidimensionaler $\mathbb{R}$-Vektorraum. Ferner existiert $0 \neq f \in \mathbb{R}[t],\ \deg(f) \geq 1$, mit $f(x) = 0$. Da K nullteilerfrei ist, folgt bereits, daß x Nullstelle eines normierten Polynoms zweiten Grades ist: $g(x) = 0$ für

$$g(t) = t^2 + ut + v \ \in \mathbb{R}[t] \ \ (u^2 - 4v < 0).$$

Also gilt: $x^2 = -ux - v$ in K. Damit läßt sich V zu einem Ring machen mittels

$$\begin{aligned} (a + bx)\,(c + dx) &= ac + (ad + bc)\, x + (-ux - v)\, bd \\ &= (ac - vbd) + (ad + bc - ubd)\, x \ \in V. \end{aligned}$$

Also ist V ein kommutativer nullteilerfreier unitärer Oberring von $\mathbb{R}$ mit 2-elementiger Basis. V ist zu $\mathbb{C}$ isomorph durch dem $\mathbb{R}$-Isomorphismus

$$a + bx \mapsto a + \frac{b}{2}\,(-u + iD) \quad \text{für} \quad D = \sqrt{4v - u^2}.$$

Dies ist zunächst eine surjektive und injektive Abbildung. Zur Homomorphie:

$$\begin{array}{ccc} (a + bx)\,(c + dx) & \mapsto & \left(a + \frac{b}{2}\,(-u + iD)\right)\left(c + \frac{d}{2}\,(-u + iD\right. \\ \| & & \| \\ (ac - bdv) + x\,(bc + ad - ubd) & & ac + \frac{ad}{2}\,(-u + iD) + \frac{bc}{2}\,(-u + iD) + \frac{bd}{4}\,(u^2 + \\ \updownarrow & & \| \\ ac - bdv + (bc + ad - ubd)\,\frac{1}{2}\,(-u + iD) & \stackrel{!}{=} & ac - \frac{u}{2}\,(ad + bc - bdu) - bdv + \frac{i}{2}\,D\,(ad + b \end{array}$$

Es bleibt $K = V$ zu zeigen. Es seien dazu $y \in K \backslash \mathbb{R}$ beliebig, $f \in \mathbb{R}[t]$ mit $f(y) = 0$. Über $V \cong \mathbb{C}$ zerfällt f in Linearfaktoren $t - \lambda$ ($\lambda \in V$), also folgt $y = \lambda$ für passende Wahl von λ.

□

77. Satz

Jede endliche Untergruppe G der multiplikativen Gruppe $K^\times$ eines Körpers K ist zyklisch.

Beweis:

Es sei $|G| = n$ und $m \in \mathbb{N}$ minimal mit $x^m = 1 \; \forall x \in G$. Dann existiert hierzu ein Element $a \in G$ mit $\mathrm{ord}(a) = m$ (vergleiche Übungen, Blatt 3, Aufgabe 1). Wegen $m|n$ ist sicherlich $m \leq n$. Andererseits sind alle $x \in G$ Nullstellen von $t^m - 1$, woraus $m \geq n$ folgt. Insgesamt gilt daher $m = n$ und $G =< a >$.

□

78. Definition

Es sei R (kommutativer) Ring mit 1. $D : R \to R$ heißt Derivation, falls

$$D(a + b) = D(a) + D(b), \quad D(ab) = D(a)\, b + a\, D(b) \quad \forall a, b \in R$$

gilt.

Beispiel: $D : R[t] \to R[t] : f \mapsto f'$.

Bibliography

[1] Bewersdorff, Jörg, *Algebra für Einsteiger*,Vieweg, 2002.
[2] Birkhoff, Bartee, *Modern Applied Algebra.*
[3] S. Bosch, *Algebra*, Springer, 1993.
[4] N. Bourbaki, *Algebre*, Hermann, Paris 1962.
[5] J. H. Davenport, Y. Siret, E. Tournier, *Computer algebra*, Acad. Press, 1989.
[6] I. N. Herstein, *Topics in Algebra*, Xerox Coll. Pub., 1964.
[7] Th. W. Hungerford, *Algebra*, 1974.
[8] N. Jacobson, *Lectures in Abstract Algebra*, Springer GTM, 1974.
[9] R. Kochendörffer, *Einführung in die Algebra*, Dt.Verl.d. Wissenschaften, 1974.
[10] S. Lang, *Algebra*, Addison-Wesley, 1971.
[11] A. Leutbecher, *Zahlentheorie*, Springer, 1996.
[12] F. Lorenz, *Algebra I, II*, BI Wissenschaftsverlag, 1987/90.
[13] K. Meyberg, *Algebra I, II*, Carl Hanser Verlag, 1975.
[14] Mignotte, *Mathematics for Computer Algebra*, Springer, 1992.
[15] E. Scholz, *Geschichte der Algebra*, BI Wissenschaftsverlag, 1990.
[16] G. Stroth, *Algebra*, de Gruyter, 1998.
[17] B. L. van der Waerden, *Algebra I, II*, Springer, 1966/87.
[18] Weber, *Lehrbuch der Algebra*, Vieweg, 1895.