II RINGE (einige Seiten lang recht „trocken" – bitte durchhalten)

§3 GRUNDBEGRIFFE UND POLYNOMRINGE

3.1. Ringe, Nullteiler, Integritätsbereiche

betrachten nun eine Menge R mit zwei inneren Verknüpfungen $+$ und $\cdot$, die durch sogenannte Distributivgesetze gekoppelt sind (z.B. $\mathbb{Z}$ mit $+$ und $\cdot$)

DEF: $(R,+,\cdot)$ ist ein **Ring**, falls

(R1) $(R,+)$ abelsche Gruppe ist,

(R2) $(R,\cdot)$ eine Halbgruppe ist (also $\cdot$ assoziativ),

(R3) die Distributivgesetze gelten: $\forall a,b,c \in R$ ist

$$a\cdot(b+c) = a\cdot b + a\cdot c \quad \text{und} \quad (b+c)\cdot a = b\cdot a + c\cdot a.$$

neutr. El. 0 bzgl. $+$ heißt **Nullelement** von R

wegen (R3) und „um Klammern zu sparen" soll „Punktrechnung vor Strichrechnung" gelten ...., wobei der „Punkt" oft auch nicht geschrieben wird...

R heißt **kommutativer Ring**, falls $(R,\cdot)$ kommutativ ist

ein Element $1 \in R$ heißt Einselement, falls $1 \cdot a = a \cdot 1 = a \quad \forall a \in R$

(↑ beide Gleichungen müssen i.A. verlangt werden)

Mini-Lemma: in einem Ring $(R, +, \cdot)$ gilt:

(i) $0 \cdot a = a \cdot 0 = 0$

(ii) $(-a)b = a(-b) = -(ab)$

(iii) $(-a)(-b) = ab$

(iv) wenn R ein Einselement 1 besitzt:

$1 = 0 \iff R = \{0\}$ ... Nullring

Beweis: UE.

DEF.2: $a \in R$ heißt rechter bzw. linker Nullteiler, wenn $\exists\, b \in R \setminus \{0\}$: $b \cdot a = 0$ bzw. $a \cdot b = 0$.

(Somit ist 0 (beinahe) immer Nullteiler, falls $R \neq \{0\}$; es gibt hier aber auch andere Konventionen, nun Elemente $\neq 0$ überhaupt als Nullteiler zuzulassen ...)

R heißt nullteilerfrei, wenn es keine rechten oder linken Nullteiler außer 0 gibt.

Mini-Lemma 2: Für einen Ring R ist äquivalent:

(i) R ist nullteilerfrei,

(ii) auf $R \setminus \{0\}$ ist $\cdot$ eine innere Verknüpfung,

(iii) es gelten die Kürzungsregeln: für $x \neq 0$ gilt

$$ax = bx \Rightarrow a = b$$

und

$$xa = xb \Rightarrow a = b$$

Beweis: UE

DEF. 3: Ein Ring R heißt Integritätsbereich oder Integritätsring, falls gilt:

(a) R hat ein Einselement $1 \neq 0$,

(b) R ist kommutativ,

(c) R ist nullteilerfrei.

BEISP: 1) $(\mathbb{Z}, +, \cdot)$ ist Integritätsbereich

2) $\bar{2}$ ist Nullteiler in $\mathbb{Z}_6$, denn $\bar{2} \cdot \bar{3} = \bar{6} = \bar{0}$
und $\bar{2} \neq 0$, $\bar{3} \neq 0$

3.2. Einheiten, Körper, Unterringe

DEF: R Ring mit 1; $a \in R$ heißt **Einheit**, falls $\exists\, \tilde{a} \in R: a \cdot \tilde{a} = \tilde{a} \cdot a = 1$.
(↑ beide gl. verlangen, i.A.)

Es ist dann die Menge $R^\times := \{a \in R \mid a \text{ ist Einheit}\}$ eine Gruppe bzgl. $\cdot$; sogenannte **Einheitengruppe** von R: • $a, b \in R^\times \Rightarrow \exists \tilde{a}, \tilde{b} \in R: \tilde{a}a = a\tilde{a} = 1 = b\tilde{b} = \tilde{b}b \Rightarrow$
$(ab)(\tilde{b}\tilde{a}) = a b \tilde{b} \tilde{a} = a\tilde{a} = 1 \Rightarrow ab \in R^\times$
• $1 \in R^\times$ • $\tilde{a}^{-1}$ (in $R^\times$) Inverses zu a □

Beisp: $\mathbb{Z}^\times = \{1, -1\}$
Für $1 \neq 0$ ist also zwingend $R^\times \subseteq R \setminus \{0\}$;
falls sogar $R^\times = R \setminus \{0\}$, also jedes Element $a \neq 0$ besitzt ein multiplikativ Inverses, dann sprechen wir von einem **Schiefkörper**, im kommutativen Fall von einem **Körper**: $(K, +, \cdot)$ heißt **Körper**, falls gilt:

(K1) $(K, +)$ abelsche Gruppe (mit neutr. El. 0)
(K2) $(K \setminus \{0\}, \cdot)$ ist abelsche Gruppe (mit neutr. El. $1 \neq 0$)
(K3) Distr.gesetz: $a \cdot (b + c) = a \cdot b + a \cdot c$

DEF. 2: Sei $(R,+,\cdot)$ ein Ring; $S \subseteq R$ heißt Unterring von R, falls gilt: (a) $\forall a,b \in S$: $a+b \in S$ und $a \cdot b \in S$,
(b) S ist mit den von R geerbten Verknüpfungen $+$ und $\cdot$ ein Ring.

Ist $(K,+,\cdot)$ ein Körper, so heißt $L \subseteq K$ ein Unterkörper, wenn L Unterring und mit diesen geerbten Verknüpfungen selbst ein Körper ist. Komplementär heißt dann K Oberkörper von L oder (häufiger) Körpererweiterung von L.

Ist $M \subseteq R$ so heißt der kleinste Unterring von R, der M enthält, der von M erzeugte Unterring und wird mit $Erz(M)$ bezeichnet; in „Formeln" ist

$$Erz(M) = \bigcap_{\substack{S \text{ Unterring von } R, \\ M \subseteq S}} S$$

[beliebige Durchschnitte von Unterringen ergeben wieder einen Unterring].

Ist $S \subseteq R$ Unterring und $a \in R$, so schreiben wir

$$S[a] := Erz(S \cup \{a\})$$

[kl. Unterring, der S und a enthält.]

und sagen, a werde zu S adjungiert.

BEM: $S \subseteq R$ ist Unterring

$\Leftrightarrow$

(i) $S \neq \emptyset$,

(ii) $\forall a, b \in S$: $a - b \in S$ und $a \cdot b \in S$

[verwende Untergr.charakterisierung in Lemma 1.3 für $(S,+)$ und entsprechende Vererbung von AG für. und DG von R auf S]

3.3. Ringhomomorphismen

DEF: Seien $(R,+,\cdot)$ und $(R',+',\cdot')$ Ringe. Eine Abb. $\varphi: R \to R'$ heißt Ringhomomorphismus, falls $\forall a, b \in R$ gilt:

$$\varphi(a+b) = \varphi(a) +' \varphi(b), \quad \varphi(a \cdot b) = \varphi(a) \cdot' \varphi(b).$$

Bijektiver Homo heißt Isomorphismus, bzw. Automorphismus für $R' = R$.

$\operatorname{Ker} \varphi := \{a \in R \mid \varphi(a) = 0'\}$ heißt Kern von φ,

$\operatorname{Im} \varphi := \{\varphi(a) \mid a \in R\} = \varphi(R)$ heißt Bild von φ.

Eigenschaften:

(a) $\varphi: R \to R'$ Ringhomo. $\Rightarrow$ $\operatorname{Ker}\varphi \subseteq R$ und $\operatorname{Im}\varphi \subseteq R'$ jeweils Unterringe

(b) $\varphi: R' \to R''$ weiterer Ringhomo. $\Rightarrow$ $\varphi \circ \varphi: R \to R''$ ebenfalls Ringhomo.

(c) φ Ringiso. $\Rightarrow$ $\varphi^{-1}: R' \to R$ Ringiso.

(d) φ injektiv $\Leftrightarrow$ $\operatorname{Ker}\varphi = \{0\}$

(e) R Körper, dann gilt: φ injektiv oder $\varphi(a) = 0' \; \forall a \in R$

Beweis: (a)-(d) leichte Routineüberlegungen.

(e): falls $\exists\, a \in R^\times$ mit $\varphi(a) = 0'$, dann

$$\varphi(1) = \varphi(a \cdot a^{-1}) = \varphi(a) \cdot \varphi(a^{-1}) = 0' \cdot \varphi(a^{-1}) = 0';$$

daher weiter $\forall\, b \in R$:

$$\varphi(b) = \varphi(b \cdot 1) = \varphi(b) \cdot \varphi(1) = \varphi(b) \cdot 0' = 0' \qquad \square$$

3.4. Beispiele

1) $\mathbb{Z}$ ist Unterring von $\mathbb{Q}$

2) $\mathbb{R}$ ist Körpererweiterung von $\mathbb{Q}$

3) $\mathbb{C}$ ist Körpererweiterung von $\mathbb{R}$

4) $\mathbb{Z} + i\mathbb{Z} := \{m + n \cdot i \mid m, n \in \mathbb{Z}\}$ ist Unterring von $\mathbb{C}$

5) $\mathbb{R}^2$ mit $(a,b)+(c,d) := (a+c, b+d)$ und
$(a,b)\cdot(c,d) := (ac, bd)$ ist ein Ring
mit Nullteilern, z.B.: $(1,0)\cdot(0,1) = (0,0)$

6) Sei M eine Menge, dann ist $\mathcal{F}(M,\mathbb{R}) :=$
$\{f: M \to \mathbb{R}\}$ ein Ring mit punktweise
definierten $(f+g)(x) := f(x)+g(x)$, $(f\cdot g)(x) := f(x)\cdot g(x)$
(geht analog mit beliebigem Ring R statt $\mathbb{R}$)

Bem: für $M=\mathbb{N}$ erhalten wir gerade die reellen
Folgen mit komponentenweiser Add. und Mult.
(erinnere, dass eine Folge eine Abb $a: \mathbb{N} \to \mathbb{R}$ mit
vereinbarter Schreibweise $a_n := a(n)$; $(a_n)_{n\in\mathbb{N}}$)

7) $M=[0,1]$ in 6) und $S := C([0,1],\mathbb{R}) = \{f: [0,1] \to \mathbb{R} |$
f ist stetig$\}$, dann ist S ein Unterring von $\mathcal{F}([0,1],\mathbb{R})$
(Summe und Differenz stetiger Funktionen ist
stetig; ebenso Produkte)

8) $M(n,\mathbb{R})$ und $M(n,\mathbb{C})$ sind Ringe mit
Matrixadd. und -mult.; Einselement I_n
Einheiten $GL(n,\mathbb{R})$ bzw. $GL(n,\mathbb{C})$

3.5. Polynomringe

„weiv" bzw. „praktisch" gesehen ist ein Polynom ein Ausdruck der Art

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$$

mit Koeffizienten a_j, die einer Addition und Multiplikation unterworfen werden können müssen...,

also Elemente eines Ringes sein sollen;

und einer „Unbekannten" X.... aber was ist das formal korrekt?

Das X müsste so wie andere Ringelemente mit den Koeff. multipliziert und auch potenziert werden können; aber festgelegt ist ein Polynom eigentlich durch seine Koeff.,

und mit diesen wird hauptsächlich gerechnet:

$$(a_3 X^3 + a_2 X^2 + a_1 X + a_0) + (b_1 X + b_0) =$$

$$= (a_3 + 0) X^3 + (a_2 + 0) X^2 + (a_1 + b_1) X + (a_0 + b_0)$$

$$(a_3 X^3 + \dots + a_0) \cdot (b_1 X + b_0) = (a_3 b_1) X^4 + (a_2 b_1 + a_3 b_0) X^3 + \dots$$

Indexsumme = 4 — Indexsumme = 3

Der Trick fürs Formale ist also, nur die Koeffizienten mit ihren Positionen zu notieren: nun besser links mit „kleinen Potenzen von X" anfangen:

$$(a_0, a_1, a_2, a_3) + (b_0, b_1, 0, 0) = (a_0 + b_0, \dots)$$

$$(a_0, a_1, a_2, a_3) \cdot (b_0, b_1, 0, 0) = (a_0 b_0, a_1 b_0 + a_0 b_1, \dots)$$

die Koeff.-folgen sind endlich, aber beliebig lang, daher können wir sagen es sind Folgen $(a_j)_{j \in \mathbb{N}}$, wo $a_j = 0$ für fast alle j ist.

DEF: Sei R ein kommutativer Ring mit 1.

$$R[X] := \{ (a_0, a_1, a_2, \dots) \in R^{\mathbb{N}} \mid a_j = 0 \text{ für fast alle } j \in \mathbb{N} \}$$

$R^{\mathbb{N}}$: Folgen in R

„fast alle" d.h. nur für endlich viele j ist $a_j \neq 0$

mit komponentenweiser Addition

$$(a_j)_{j \in \mathbb{N}} + (b_j)_{j \in \mathbb{N}} := (a_j + b_j)_{j \in \mathbb{N}}$$

und dem sogenannten Cauchy-Produkt

$$(a_0, a_1, a_2, \dots) \cdot (b_0, b_1, b_2, \dots) := (c_0, c_1, c_2, \dots),$$

wobei $$c_k := \sum_{\ell=0}^{k} a_\ell \cdot b_{k-\ell} = a_0 b_k + a_1 b_{k-1} + \dots + a_k b_0$$

[Indexsumme $= k$]

der ergibt einen kommutativen Ring [leicht und fad]
mit Einselement $(1,0,0,\ldots)$:

$(1,0,\ldots)\cdot(a_0,a_1,\ldots) = (c_0,c_1,\ldots)$ mit

$$c_0 = 1\cdot a_0,\quad c_1 = 1\cdot a_1 + 0\cdot a_0 = a_1 \text{ etc.}\ldots$$

wir schreiben nieder 1 statt $(1,0,\ldots)$.

Mittels $a \longmapsto (a,0,\ldots)$, $R \to R[X]$
ist R in $R[X]$ eingebettet, d.h. diese Abb. ist ein injektiver Ringhomo., der die Einselemente aufeinander abbildet; daher fassen wir R gleich als Unterring von $R[X]$ auf.

Wir können nun auch $X := (0,1,0,\ldots)$ setzen; dann ist

$$X^k = (0,\ldots,0,\underset{\uparrow}{1},0,\ldots)$$
$$(k+1)\text{-te Stelle}$$

und

$$R[X] \ni (a_0,a_1,a_2,\ldots) = a_0\cdot 1 + a_1 X + a_2 X^2 + \ldots$$
(endliche Summe!)

↝ also „alles in Butter." [Details lesen in UE]

$(R[X],+,\cdot)$ heißt der <u>Polynomring über R</u>.

Einsetzen für X geht nun so:

Ist R' ein Ring mit $R' \supseteq R$, $\alpha \in R'$ und $f = a_0 + a_1 X + \dots + a_n X^n \in R[X]$, so setzen wir $f(\alpha) := a_0 + a_1 \alpha + \dots + a_n \alpha^n \in R'$

Durch $f \mapsto f(\alpha)$ erhalten wir eine Abbildung $R[X] \to R'$.

Bem: R' statt R ist praktisch, weil dann z.B. kompl. Zahlen in reelle Pol. eingesetzt werden können; aber auch $R' = R[X]$ möglich, insbesondere für $\alpha = X$ erhalten wir also $id : R[X] \to R[X]$.
(Jetzt ist alles formal wieder einseinander = erhalten, aber dennoch eine einfache Notation möglich !)

Polynom versus Polynomfunktion:

Ist $f = a_0 + a_1 X + \dots + a_n X^n \in R[X]$, so erhalten wir daraus die zugeordnete Polynomfunktion

$\tilde{f} : R \to R$, $x \mapsto a_0 + a_1 x + \dots + a_n x^n$ [hier $x \in R$]

Achtung: Polynome sind durch ihre Koeff. immer eindeutig bestimmt, für Pol.funkt. gilt das über allg. Ringen aber nicht immer!

Beisp: $R = \mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$, $f = X^2 + X \in \mathbb{Z}_2[X]$, dann ist

$\bar{f}(\bar{0}) = \bar{0}$ und $\bar{f}(\bar{1}) = \bar{1}^2 + \bar{1} = \bar{1} + \bar{1} = \bar{2} = \bar{0}$,

somit $\bar{f}$ die Nullfunktion, aber dem Nullpolynom $(0,0,\dots) = 0 + 0\cdot X + \dots$ entspricht, obwohl $f \neq$ Nullpolynom. $[f = (0,1,1,0,\dots)]$

Bem: Wenn R ein Integritätsbereich mit ∞ vielen Elementen ist, dann ist $f \mapsto \bar{f}$ injektiv, weil es in diesem Fall für $f \neq 0$ nicht ∞ viele Nullstellen geben kann (später).

3.6. Grad eines Polynoms und Division mit Rest

Sei R komm. Ring mit 1

Für $f = a_n X^n + \dots + a_1 X + a_0$ mit $a_n \neq 0$ nennen wir die höchste auftretende Potenz n den Grad von f, wir schreiben $\deg f = n$ und nennen a_n den Leitkoeffizienten, $a_n X^n$ den Leitterm von f.

Für $f=0$ (Nullpolynom) setzen wir künstlich $\deg 0 := -\infty$[, damit es sich gut von allen Polynomen absetzt und so, dass spätere Gradformeln auch in diesem Fall noch sinnvoll lesbar sind.]

Ein konstantes Polynom $f \neq 0$ hat dennoch $\deg f = 0$, weil $f = a_0$ mit $a_0 \in R \setminus \{0\}$;
$\deg(aX+b) = 1$, falls $a \neq 0$ usw. ....

<u>Gradformel:</u> $\forall f, g \in R[X]$ gilt

$$\deg(f \cdot g) \leq \deg(f) + \deg(g).$$

Gleichheit gilt, falls der Leitkoeffizient von f oder g kein Nullteiler ist.

<u>Bem:</u> $\deg(f+g) \leq \max(\deg(f), \deg(g))$ [Leitkoeff. könnten einander auslöschen]

Beweis der Gradformel: falls $f=0$ oder $g=0$, dann $f \cdot g = 0$ und Ungl. gilt im Sinne $-\infty \leq -\infty$;
seien also $f \neq 0$ und $g \neq 0$ mit Darstellungen

$f = a_m X^m + \ldots + a_0$, $a_m \neq 0$ und $g = b_n X^n + \ldots + b_0$, $b_n \neq 0$.

Wir haben also $\deg f = m$, $\deg g = n$;
in $f \cdot g$ ist der Koeffizient mit dem größtmöglichen Index $c_{m+n} = a_m \cdot b_n$, daher
$\deg(f \cdot g) \leq m+n$.

Falls a_m oder b_n kein Nullteiler, dann ist sicher $c_{m+n} \neq 0$, also $\deg(f \cdot g) = m+n$ □

Ein Polynom mit Leitkoeffizienten 1 heißt normiert. Ist $f = a_n X^n + \dots + a_0$ und $a_n \in R^\times$, also eine Einheit, so können wir $\tilde{f} := a_n^{-1} \cdot f$ bilden und erhalten ein normiertes Polynom.

„Sätzchen": (i) $R[X]$ nullteilerfrei $\Leftrightarrow$ R nullteilerfrei
(ii) R nullteilerfrei $\Rightarrow$ $(R[X])^\times = R^\times$
[insbes. alle Einheiten $\deg = 0$]

„Beweischen": (i): $\Rightarrow$: wegen $R \subseteq R[X]$ klar;
$\Leftarrow$: es gilt $\deg(f \cdot g) = \deg(f) + \deg(g)$; falls $f \cdot g = 0$,
muss entweder $\deg(f) = -\infty$ oder $\deg(g) = -\infty$ gelten,
also $f = 0$ oder $g = 0$.

(ii): $R^\times \subseteq (R[X])^\times$ klar $\left[a_0 \in R^\times,\ f = a_0;\ g := a_0^{-1} \Rightarrow g \cdot f = 1 \right]$

wir zeigen $(R[X])^\times \subseteq R^\times$: $f \in (R[X])^\times \Rightarrow$

$\exists\, g \in R[X] : f \cdot g = 1$; somit

$$0 \leq \underbrace{\deg(f)}_{\geq 0} + \underbrace{\deg(g)}_{\geq 0} = \deg(f \cdot g) = \deg(1) = 0$$

[$\deg(f) \geq 0$ und $\deg(g) \geq 0$ möglich, wenn $f \cdot g = 1$]

$\Rightarrow \deg(f) = 0 = \deg(g)$; daher f und g „konstante" Polynome, also $f = a_0$ mit $a_0 \in R^\times$ □

SATZ ÜBER DIE DIVISION MIT REST

Sei K ein Körper und $f, g \in K[X]$ mit $g \neq 0$.

Dann $\exists!\, q \in K[X]$ und $\exists!\, r \in K[X]$, sodass

$$f = q \cdot g + r \quad \text{und} \quad \deg(r) < \deg(g).$$

Beweis:

Eindeutigkeit: Wenn $qg + r = \tilde{q} g + \tilde{r}$ mit $\deg(r) < \deg(g)$ und $\deg(\tilde{r}) < \deg(g)$,

dann folgt $\underbrace{r - \tilde{r}}_{\deg < \deg(g)} = \underbrace{(\tilde{q} - q) \cdot g}_{\deg = \deg(\tilde{q}-q) + \deg(g)}$ Gradformel:

$\Rightarrow \tilde{q} - q = 0 \Rightarrow \tilde{q} = q$ und $\tilde{r} = r$

Existenz: sei $f = a_n X^n + \dots + a_0$, $g = b_m X^m + \dots + b_0$,

$n = \deg(f)$, $m = \deg(g) \geq 0$ [$g \neq 0$; $b_m \neq 0$]

- falls $n < m$, dann fertig mit $q = 0$ und $r = f$
- falls $n \geq m$, dann konstruieren wir sukzessive $q_1, \dots, q_k \in K[X]$ mit $k \leq n - m + 1$ derart, dass

$$q := q_1 + \dots + q_k$$ zusammen mit $r := f - qg$ eine Lösung ergibt.

1. Schritt: setze $f_0 := f$, $q_1 := \frac{a_n}{b_m} \cdot X^{n-m}$ [in Körpern Schreibweise $\frac{a_n}{b_m}$ statt $a_n b_m^{-1}$]

$f_1 := f_0 - q_1 g$, $\deg(f_1) < \deg(f_0)$ [$q_1 \cdot g = a_n X^n + \dots$]

- falls $\deg(f_1) < \deg(g)$, dann fertig mit $q = q_1$, $r = f_1$.
- falls $\deg(f_1) \geq \deg(g)$: mit f_1 wie oben mit f_0 verfahren, also $q_2 := c \cdot X^{\deg(f_1) - m}$: $q_2 \cdot g$ gleichen Leitterm wie f_1 hat,

$$f_2 := f_1 - q_2 g, \quad \deg(f_2) < \deg(f_1).$$

- Verfahren fortsetzen, bis

$f_k := f_{k-1} - q_k g$ die Bedingung $\boxed{\deg(f_k) < \deg(g)}$ erfüllt

- das ist spätestens bei $k = n-m+1$ der Fall, weil $\deg(f_k) < \deg(f_{k-1}) < \ldots < \deg(f_1) < n$ und $\deg(g) = m \leq n$ ist.

insgesamt $f = q_1 g + f_1 = q_1 g + q_2 g + f_2 = \ldots =$

$$= \underbrace{(q_1 + \ldots + q_k)}_{=:q} g + \underbrace{f_k}_{=:r}$$

□

Variante des Divisionssatzes für Integritätsbereich R statt K:

Sei R ein Integritätsbereich und $f, g \in R[X]$ mit $g \neq 0$. Ist $b_m \in R$ der Leitkoeffizient von g, dann $\exists\, q, r \in R[X]$ und $k \in \mathbb{N}$, so dass

$$b_m^k \cdot f = q \cdot g + r \quad \text{und} \quad \deg(r) < \deg(g).$$

Bem: q und r sind bis auf eine Potenz von b_m eindeutig

Begründung für die Gültigkeit der Variante: im obigen Bew. im 1. Schritt mit $b_m f$ und $q_1 \cdot b_m = a_n X^{n-m}$ arbeiten [durch b_m kann i.A. nicht dividiert werden, denn $f_1 = b_m f_0 - \tilde{q}_1 g_1$ b_m ist jedenfalls kein Nullteiler]

denn $f_2 = b f_1 - \tilde{q}_2 \cdot g$ etc.; bzw. $bf = f_1 + \tilde{q}_1 g_1$, $b^2 f = f_2 + \tilde{q}_2 g_1$ usw.

BEISP: 1) $f = X^2 - 1$, $g = 2X$ in $\mathbb{Z}[X]$

$2 \cdot f = 2X^2 - 2 = \underbrace{X}_{q} \cdot \underbrace{2X}_{g} - 2$ und $r = -2$

$f = q \cdot g + r$ würde $q = \frac{1}{2} X$ erfordern, geht nicht in $\mathbb{Z}[X]$

2) in $\mathbb{R}[X]$: Verfahren eig. aus der Schule bekannt

$\overbrace{(X^3 - X + 1)}^{f} : \overbrace{(X+1)}^{g} = \underbrace{X^2 - X}_{q}$

$-X^3 \pm X^2$

$-X^2 - X + 1$

$\mp X^2 \mp X$

$1 = r$

$X^3 - X + 1 = (X^2 - X) \cdot (X+1) + 1$

3.7. Nullstellen von Polynomen

SATZ: Ist R ein Integritätsbereich und $f \in R[X]$ mit $\deg(f) \geq 1$ und $a \in R$ mit $f(a) = 0$, dann

$\exists!\, q \in R[X]$: $f = (X - a) \cdot q$ und $\deg(q) = \deg(f) - 1$.

Insbesondere hat ein Polynom vom Grad $n \geq 1$ höchstens n verschiedene Nullstellen in R.

Beweis: Division von f durch $g = X - a$ mit Rest ergibt

$$f = q \cdot (X-a) + r, \quad \deg(r) < 1 = \deg(g)$$

wegen $0 = f(a) = r(a)$ folgt $r = 0$, also $f = q \cdot (X-a)$;

daher $\deg(f) = \deg(q \cdot (X-a)) = \deg(q) + 1$.

Sind $a_1, \dots, a_m \in R$ (paarweise) verschiedene Nullst., d.h. $f(a_j) = 0$ $(j = 1, \dots, m)$ und $a_i \neq a_j$ $(i \neq j)$, dann ergibt sich durch sukzessive Anwendung des Obigen: $f = (X-a_1) \cdot \sim (X-a_m) \cdot h$ mit

$0 \leq \deg(h) = \deg(f) - m = n - m \Rightarrow m \leq n$

$[h \neq 0$, sonst $f = 0]$ □

KOR: Sind $a_1, \dots, a_m \in R$ (paarweise) verschiedene Nullstellen von $f \in R[X]$, $\deg(f) \geq 1$, dann $\exists! \, h \in R[X]$:

$$f = (X-a_1) \dots (X-a_m) \cdot h, \quad \deg(h) = \deg(f) - m \geq 0.$$

BEISP: $f = (X-1)(X-2)(2X-1)$ $[= 2X^3 - 7X^2 + 7X - 2]$

in $\mathbb{R}[X]$: $f = (X-1)(X-2)\left(X - \frac{1}{2}\right) \cdot 2$

in $\mathbb{Z}[X]$: $f = (X-1)(X-2) \cdot (2X-1)$

„minimaler h-Anteil"

3.8. Komplexe Einheitswurzeln

$n \in \mathbb{N}, n \geq 1$:

$\zeta \in \mathbb{C}$ wird eine <u>n-te Einheitswurzel</u> genannt, wenn $\zeta^n = 1$ gilt; äquivalent dazu ist, dass ζ eine Nullstelle des Polynoms $X^n - 1$ ist.

Es gibt nach 3.7 höchstens n verschiedene n-te Einheitswurzeln und für $\zeta_n := e^{\frac{2\pi i}{n}}$ ist jede der Zahlen ζ_n^k $(k = 0, 1, \dots, n-1)$ eine solche.

Es ist $\zeta_n^{k+l\cdot n} = e^{\frac{2\pi i k}{n} + 2\pi i l} = e^{\frac{2\pi i k}{n}} = \zeta_n^k$, somit ist

$C_n = \{\zeta_n^k \mid k \in \mathbb{Z}\} = \{1, \zeta_n, \dots, \zeta_n^{n-1}\} \subseteq S^1$

gerade die Menge der n-ten Einheitswurzeln.

Weiters gilt gemäß 3.7:

$$X^n - 1 = (X-1)(X-\zeta_n)\cdots(X-\zeta_n^{n-1}).$$

In früheren Beisp. und UE-Aufgaben haben wir gesehen:

$\varphi: \mathbb{Z} \to C_n$, $k \mapsto \zeta_n^k$ ist Gruppenhomo. und faktorisiert wegen $\ker \varphi = n\mathbb{Z}$ zu einem Iso.

$\bar{\varphi}: \mathbb{Z}_n \to C_n$, $\bar{k} \mapsto \zeta_n^k$; C_n ist also endliche zyklische Gruppe

Es ist $(X^n - 1) = (X-1)\cdot(X^{n-1} + \dots + X + 1)$,

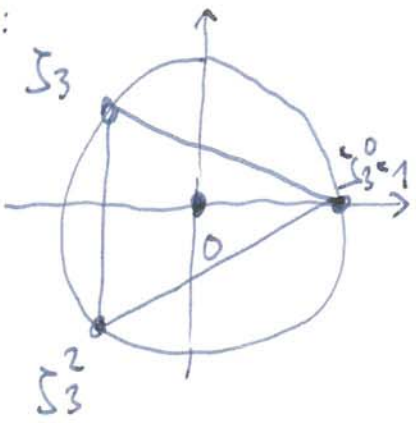
↑ hat einzige Nullstelle $\zeta_n^0 = 1$ bzw. $\zeta_1 = 1$

daher ist für $n \geq 2$ sicherlich ζ_n eine Nst. des zweiten Faktors, also

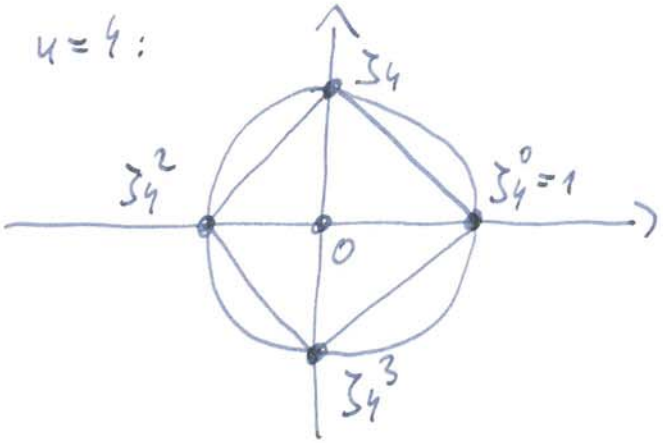
$$\zeta_n^{n-1} + \zeta_n^{n-2} + \dots + \zeta_n + 1 = 0$$

als Vektorsumme in $\mathbb{R}^2$ interpretiert sagt dies, dass 0 der „Schwerpunkt" des regelmäßigen n-Ecks C_n ist

$n=3$:



$n=4$:



<u>Bem:</u> $C_m \cap C_n = C_{ggT(m,n)}$ (o.B.; siehe Fischer II, 1.9)

3.9. Vom Integritätsbereich zum Quotientenkörper

Es ist ein häufiges mathematisches Ziel, „unfertige" Strukturen zu „vervollständigen" – oft als formale Nachbildung von historisch mühevoll gewachsenen Erweiterungen; z.B. kann die Halbgruppe $(\mathbb{N},+)$ zur Gruppe $(\mathbb{Z},+)$ erweitert werden, indem Differenzen wie z.B. $3-7$ durch Äquivalenzklassen von Paaren $(3,7) \sim (4,8) \sim (5,9) \ldots$ hergestellt werden; somit muss nicht gesagt werden, was negative Zahlen sind, und es kann mit diesen (Klassen von) Paaren einfach gerechnet werden: $(k,l)+(r,s)=(k+r,l+s)$; damit wird $\mathbb{N}\times\mathbb{N}/\sim$ zur Gruppe mit neutr. El. = die Klasse von $(0,0)$ $[\sim(1,1)$ etc.$]$ und zur Klasse von (k,l) ist die Klasse von (l,k) invers, weil $(k,l)+(l,k)=(k+l,l+k)\sim(0,0)$.

[Allg. Hintergrund für diese Konstr. ↝ Fischer II, 1.12]

Ähnlich kann ein Integritätsbereich R zu einem Körper $Q(R)$ erweitert werden, indem man die multiplikative Halbgruppe $(R\setminus\{0\},\cdot)$ auf ähnliche Art und die nötigen „Brüche" erweitert wird: statt „$\frac{a}{b}$" führen wir das Paar $(a,b) \in R \times R\setminus\{0\}$ ein und erinnern uns an „$\frac{a}{b} = \frac{a'}{b'} \iff ab' = a'b$",

wes wir durch

$$(a,b) \sim (a',b') :\iff a\cdot b' = a'\cdot b \text{ in } R$$

modellieren; Mult. von „Brüchen" ist leicht: $(a,b)\cdot(c,d) := (ac, bd)$,

Addition von „Brüchen" erfolgt nach dem Muster „$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$": $(a,b)+(c,d) := (ad+bc, bd)$.

$0 \mathrel{\hat{=}} (0,1)$, $1 \mathrel{\hat{=}} (1,1)$ [bzw. deren Klassen]

Die Menge $Q(R)$ dieser Klassen von „Brüchen" wird so ein Körper [Fischer II, 1.13] und

Das Standardbeispiel ist $Q(\mathbb{Z}) = \mathbb{Q}$, wo denn die Paare $(m,n) \in \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ als Brüche $\frac{m}{n}$ notiert werden.

Ein weiteres wichtiges Beispiel ist für ein Körper K

$Q(K[X]) =: K(X)$ ..... Körper der rationalen Funktionen, also Brüche von Polynomen $\frac{f}{g}$ $f \in K[X]$, $g \in K[X]$, $g \neq 0$

↑ Polynomring, ist Integritätsbereich, weil K Körper

Achtung: $\frac{f}{g}$ ergibt die zugehörige rationale Funktion, die in den endlich vielen Nullstellen von g nicht definiert ist ($g \neq 0$ heißt ja nur „ungleich dem Nullpolynom");

- hier hat die formale Einführung der Polynome seine Vorteile gegenüber der konkreten Modellierung als Funktionen.

§4 IDEALE UND RESTKLASSENRINGE

4.1. Ideale

Wenn $\varphi: R \to R'$ Ringhomo., dann ist gemäß 3.3 $I := \ker\varphi \subseteq R$ ein Unterring; I hat hier aber sogar eine weitere starke Eigenschaft: sei $x \in R$ und $a \in I$, dann gilt $\varphi(ax) = \underbrace{\varphi(a)}_{0} \cdot \varphi(x) = 0$, $\varphi(xa) = \varphi(x) \underbrace{\varphi(a)}_{0} = 0$,

also $x \cdot a \in I$ und $a \cdot x \in I$ (für Unterring ist nun $b \cdot a \in I \wedge a \cdot b \in I$ für $b \in I$ nötig)

allgemeiner führen wir nun einen denen modellierten Begriff für Unterringe ein:

DEF: Ist R ein Ring und $I \subseteq R$, dann heißt I Ideal, falls gilt:

(I1) I ist bzgl. $+$ eine Untergruppe von R,

(I2) $a \in I, x \in R \Rightarrow x \cdot a \in I \wedge a \cdot x \in I$.

Insbesondere ist ein Ideal daher ein Unterring.

Falls R kommutativ (mit 1) ist, ist (I1+I2) äquivalent mit

(I) $0 \in I$ und $\forall n \in \mathbb{N}\ \forall a_1, \dots, a_n \in I\ \forall x_1, \dots, x_n \in R$:

$x_1 a_1 + \dots + x_n a_n \in I$ [Beweis als UE]

weiters definieren wir im kommutativen Fall für $a \in R$ das <u>von a erzeugte Hauptideal</u> durch

$$(a) := R \cdot a := \{ x \cdot a \mid x \in R \}$$

(dies ist ein Ideal, denn für $\tilde{x}, \tilde{y} \in (a)$ mit $\tilde{x} = xa$, $\tilde{y} = ya$ ist $\tilde{x} - \tilde{y} = xa - ya = (x-y)a \in (a)$ und für $z \in R$ ist $z \cdot \tilde{x} = z(x \cdot a) = (zx)a \in R$)

<u>Beisp:</u> 1) oben gesehen: Kern eines Ringhomo. ist Ideal

2) die <u>trivialen Ideale</u> $\{0\}$ und R gibt es immer

3) $m\mathbb{Z}$ ist Ideal in $\mathbb{Z}$ (entweder direkt oder als Kern von $k \mapsto \bar{k}$, $\mathbb{Z} \to \mathbb{Z}_m$)

<u>BEM:</u> Sei $\varphi: R \to R'$ Ringhomo., dann gilt:

(i) $I' \subseteq R'$ Ideal $\Rightarrow \varphi^{-1}(I')$ Ideal in R,

(ii) $I \subseteq R$ Ideal und φ surjektiv $\Rightarrow \varphi(I) \subseteq R'$ Ideal

[Beweise als UE]

<u>SATZ:</u> (i) R Ring mit 1, $I \subseteq R$ Ideal mit $I \cap R^\times \neq \emptyset$

$\Rightarrow I = R$,

(ii) ein Körper K besitzt nur die trivialen Ideale,

(iii) R kommutativen Ring mit $1 \neq 0$ und besitzt nur die trivialen Ideale $\{0\}$ und R, dann ist R ein Körper.

Beweis: (i) $a \in I \cap R^\times \Rightarrow \exists b \in R^\times : \underbrace{ab}_{\in I} = ba = 1$

$\Rightarrow 1 \in I \Rightarrow \forall x \in R : \underbrace{x \cdot 1}_{x} \in I \Rightarrow I = R$;

(ii) es ist $K^\times = K \setminus \{0\}$; ist I Ideal in K und $I \neq \{0\}$, so muss $I \cap K^\times \neq \emptyset$ sein, also $I = K$ nach (i);

(iii) wir müssen $R^\times = R \setminus \{0\}$ zeigen, dann fertig;
$c \in R \setminus \{0\} \Rightarrow \{0\} \neq (c) = Rc$ und $Rc = R$, weil
$[1 \neq 0]$
keine nichttrivialen Ideale in R existieren;
daher $\exists b \in R : bc = 1$ (weil $1 \in R = Rc$),
somit $c \in R^\times$; also $R^\times = R \setminus \{0\}$ gezeigt,
weil $R^\times \subseteq R \setminus \{0\}$ immer gilt □

Kegelsatz

KOR: $R^\times = \bigcap_{\substack{I \text{ echtes} \\ \text{Ideal in } R}} R \setminus I$ [„echtes Ideal" ... nichttriviales Ideal]

Bew: aus Satz (i) folgt $R^\times \cap I = \emptyset$ für jedes echte Ideal I; somit $R^\times \subseteq R \setminus I$ für jedes echte Ideal, d.h. $R^\times \subseteq$ rechter Seite.

Ist andererseits $a \in R \setminus (R^\times \cup \{0\})$, dann ist $1 \notin (a)$ und somit $I = (a)$ ein echtes Ideal, das a enthält, daher $a \notin$ rechter Seite; somit $R^\times \supseteq$ rechter Seite. □

4.2. Restklassenringe

nun Verallgemeinerung der Konstruktion $\mathbb{Z}/m\mathbb{Z}$ bzgl. Ringstruktur ($m\mathbb{Z}$ ist Ideal in $\mathbb{Z}$):

sei $\underline{I}$ Ideal in R, dann als Untergr. der abelschen Gruppe $(R,+)$ stets Normalteiler, also Faktorgruppe

$$R/\underline{I} = \{x+\underline{I} \mid x \in R\}$$

mit Addition $(x+\underline{I})+(y+\underline{I}) := (x+y)+\underline{I}$ wieder eine abelsche Gruppe; sei $\varrho: R \to R/\underline{I}, x \mapsto x+\underline{I}$ der kanonische surjektive Gruppenhomo.; wir wollen nun $R/\underline{I}$ durch die Multiplikation

$$(x+\underline{I})\cdot(y+\underline{I}) := (x\cdot y)+\underline{I}$$

zu einem Ring machen — dies ist die einzige Mult. auf $R/\underline{I}$, die ϱ zu einem Ringhomo. machen kann:

- Mult. ist wohldefiniert: $x+\underline{I}=x'+\underline{I}$, $y+\underline{I}=y'+\underline{I}$
$\Rightarrow x-x' \in \underline{I} \wedge y-y' \in \underline{I} \Rightarrow$

$$xy - x'y' = \underbrace{(x-x')}_{\in \underline{I}}y' + x\underbrace{(y-y')}_{\in \underline{I}} \in \underline{I} \Rightarrow (xy)+\underline{I} = (x'y')+\underline{I}$$

- AG und DG vererben sich von R auf R/I, weil sie für die Repräsentanten $x, y \ldots$ den Klassen gelten
- $\ker \rho = I$ nach Konstruktion von ρ
- wenn R kommutativ, dann auch R/I
- wenn R Einselement 1 besitzt, dann $1+I$ Einselement in R/I

BEM: somit kann jedes Ideal als Kern eines Ringhomo. aufgefasst werden, weil immer $I = \ker \rho$ für $\rho: R \to R/I$ kanonische Surjektion

Wir nennen R/I den Restklassenring von R modulo I und schreiben Kongruenten modulo I in R auch so:

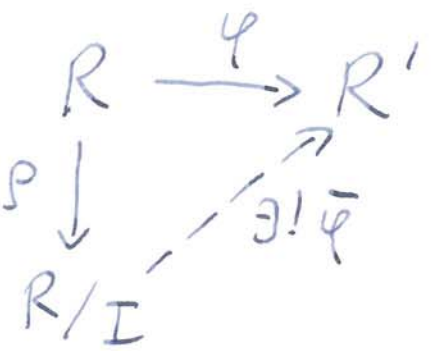
$$x \equiv x' \pmod{I} :\Leftrightarrow x+I = x'+I \Leftrightarrow x-x' \in I$$

(vgl. $x \equiv x' \pmod{m} \Leftrightarrow x-x' \in m\mathbb{Z}$ $[\mathbb{Z}_m]$)

Eig: $\left.\begin{array}{l} x \equiv x' \pmod{I} \\ y \equiv y' \pmod{I} \end{array}\right\} \Rightarrow x \cdot y \equiv x' \cdot y' \pmod{I},\ x+y \equiv x'+y' \pmod{I}$

Eigenschaften: analog zu Gruppen gelten (o. Bew.)

(i) Faktorisierungssatz: Sei $\varphi: R \to R'$ Ringhomo., $I \subseteq R$ Ideal mit $I \subseteq \ker(\varphi)$ und $\rho: R \to R/I$ die kanonische Surjektion. Dann $\exists!$ Ringhomo. $\bar{\varphi}: R/I \to R'$, sodass $\varphi = \bar{\varphi} \circ \rho$ gilt, d.h.



ist kommutativer Diagramm

Weiters gilt $\bar{\varphi}(R/I) = \varphi(R)$, $\ker(\bar{\varphi}) = \ker(\varphi)/I$.

(ii) erster Isomorphiesatz: $\varphi: R \to R'$ Ringhomo. $\Rightarrow$ $\bar{\varphi}$ bijektiv als Abb. $R/\ker\varphi \to \varphi(R)$,

$$x + \ker\varphi \mapsto \varphi(x)$$

also Isomorphismus $\boxed{\varphi(R) \cong R/\ker\varphi}$ (via $\bar{\varphi}$).

Ist zudem φ surjektiv, dann $R' \cong R/\ker\varphi$.

4.3. Beispiele

1) Jedes Ideal in $\mathbb{Z}$ ist eine additive Untergruppe, also von der Form $n\mathbb{Z}$ [frühere UE-Aufg.]; und jedes $n\mathbb{Z}$ ($n \in \mathbb{N}$) ist ein (Haupt-)Ideal in $\mathbb{Z}$; entsprechende Restklassenringe $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ sind die „Prototypen" für 4.2. gewesen;
es ist $\mathbb{Z}$ nullteilerfrei; und für $n \geq 2$: $\mathbb{Z}_n$ nullteilerfrei genau dann, wenn n Primzahl [ebenfalls UE bzw. via Zahlentheorie],
für die Einheiten in $\mathbb{Z}_n$ gilt

$$\mathbb{Z}_n^\times = \{ \bar{k} \mid ggT(k,n) = 1 \}$$

$$\left(\exists \substack{l \in \mathbb{Z} \\ x \in \mathbb{Z}} \; \underbrace{1}_{ggT(k,n)} = kl + nx, \text{ d.h. } \bar{k} \cdot \bar{l} = \bar{1} \right)$$

2) betrachte $\varphi : \mathbb{R}[X] \to \mathbb{C}$, $f \mapsto f(i)$ Ringhomo. [sonst. [UE]]

Beh.: $\ker(\varphi) = (X^2+1) = \mathbb{R}[X] \cdot (X^2+1)$ Hauptideal

„$\supseteq$": klar, weil $i^2+1 = 0$, d.h. $\varphi(X^2+1) = 0$ und somit $\varphi(f \cdot (X^2+1)) = \varphi(f) \cdot \underbrace{\varphi(X^2+1)}_{0} = 0$

„$\subseteq$" wird in UE besprochen (bzw. in 4.5, Beisp. 3) anders) $\square$

Isomorphiesatz: $\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}$

$\bar{\varphi}: f+(X^2+1) \longmapsto f(i)$

- für $a \in \mathbb{R}$ ist $\bar{\varphi}(a+(X^2+1)) = a \in \mathbb{R}$ $[f=a]$
- für $X \in \mathbb{R}[X]$ erhalten wir $\bar{\varphi}(X+(X^2+1)) = i$ $[f=X]$

d.h. $\bar{\varphi}(\underbrace{a+bX}_{f}+(X^2+1)) = a+bi$

Also ist Rechnen mit komplexen Zahlen wie Rechnen in $\mathbb{R}[X]$ modulo (X^2+1)

4.4. Hauptidealringe und euklidische Ringe

DEF: Sei R ein Integritätsbereich.

(i) R heißt Hauptidealring, wenn jedes Ideal I in R ein Hauptideal ist, also $I = (a) = Ra$ für ein $a \in R$.

(ii) R heißt euklidischer Ring, wenn es eine Abbildung $\delta: R\setminus\{0\} \to \mathbb{N}$ gibt mit folgender Eig.: $\forall a,b \in R\setminus\{0\}$ $\exists q,r \in R$: $a = q\cdot b + r$ und $\delta(r) < \delta(b)$, falls $r \neq 0$.

(Division mit Rest)

BEISP: 1) $\mathbb{Z}$ ist Hauptidealring, denn wie in 4.3 bemerkt ist jedes Ideal in $\mathbb{Z}$ von der Form $m\mathbb{Z}$ mit $m \in \mathbb{N}$; $m\mathbb{Z} = (m)$;
in $\mathbb{Z}$ kann $\delta(k) = |k|$ verwendet werden und Division mit Rest gilt, also ist $\mathbb{Z}$ auch ein euklidischer Ring

2) K Körper, dann ist (nach 3.6) $K[X]$ ein euklidischer Ring mit $\delta(f) = \deg(f)$ für $f \neq 0$

3) $\mathbb{Z}[X]$ ist kein Hauptidealring (und gemäß folgendem Satz auch kein euklidischer Ring):
$I := \{ 2 \cdot f_1 + X \cdot f_2 \mid f_1, f_2 \in \mathbb{Z}[X] \}$ ist ein Ideal in $\mathbb{Z}[X]$ und $I \neq \{0\}$; es ist $1 \notin I$, somit auch $I \neq \mathbb{Z}[X]$;
wäre $\mathbb{Z}[X]$ ein Hauptidealring, so müsste es ein $f \in \mathbb{Z}[X]$ mit $I = (f) = \mathbb{Z}[X] \cdot f$ geben:
wegen $2, X \in I$ gibt es

$g, h \in \mathbb{Z}[X]$, sodass $\underbrace{2 = g \cdot f}, \underbrace{X = h \cdot f}_{(*)}$

$\Rightarrow \deg(g) = 0 = \deg(f)$

also $f = a_0$, $g = b_0$ mit $a_0, b_0 \in \mathbb{Z}$ und $a_0 b_0 = 2$,

in $(*)$: $X = h \cdot a_0 \Rightarrow h = a_1 \cdot X$ und $a_0 a_1 = 1$

$\Rightarrow a_0 = \pm 1$, d.h. $f = \pm 1 \Rightarrow \underbrace{(f)}_{\parallel I} = \mathbb{Z}[X]$ ↯

SATZ: Ein euklidischer Ring ist ein Hauptidealring.

Beweis: sei R euklid. und $I \subseteq R$ ein Ideal;

im Falle $I = \{0\} = (0)$ fertig; also nun

$I \neq \{0\}$ annehmen:

setze $M := \{n \in \mathbb{N} \mid \exists a \in I \setminus \{0\} : n = \delta(a)\}$

$I \neq \{0\} \Rightarrow M \neq \emptyset$; sei $k = \min M$ und $a \in I \setminus \{0\}$

mit $k = \delta(a)$

Behauptung: $I = (a)$

$I \supseteq (a)$ ist klar, bleibt z.z. $I \subseteq (a)$

wäre $b \in I \setminus (a)$, dann Division mit Rest:

$$b = qa + r \quad \text{mit } \delta(r) < \delta(a) = k, \text{ falls } r \neq 0$$

- für $r = 0$ wäre $b = qa \in (a)$ ↯
- für $r \neq 0$ ist $\delta(r) < k$ und

$$r = \underbrace{b}_{\in I} - \underbrace{qa}_{\in I} \in I \quad \Rightarrow \delta(r) \in M$$

↯ zur Minimalität von k

□

KOR: K Körper $\Rightarrow K[x]$ Hauptidealring

BEM: für einen Integritätsbereich R ist äquivalent:

(i) R ist Körper

(ii) $R[x]$ euklidisch

(iii) $R[x]$ Hauptidealring [Kowal-Mitrich, Kap. II, Satz 6.4.]

4.5. Primideale und maximale Ideale

Problem: Nullteiler in Restklassenring können entstehen, wenn $\underbrace{(x+I)(y+I)}_{xy+I} = I$ } d.h. $xy \in I$ ohne, dass $x \in I$ oder $y \in I$ gilt

DEF. 1: Ein Ideal $P \subseteq R$ heißt **Primideal**, wenn

(a) $P \neq R$,

(b) $a, b \in R$ und $ab \in P \Rightarrow a \in P$ oder $b \in P$

BEM: $\{0\}$ Primideal $\Leftrightarrow$ R nullteilerfrei

SATZ 1: R kommutativer Ring mit $1 \neq 0$, $P \subseteq R$ Ideal:

P Primideal $\Leftrightarrow$ R/P Integritätsbereich.

Beweis: ($\Rightarrow$) $a+P$ Nullteiler in $R/P \Rightarrow \exists\, b \in R \setminus P$:

$$\underbrace{(a+P)\cdot(b+P)}_{ab+P} = P \Rightarrow ab \in P \overset{b \notin P}{\Longrightarrow} a \in P$$

$$\Rightarrow a+P = P \quad [\text{Nullklasse}]$$

($\Leftarrow$) $a \cdot b \in P \Rightarrow (a+P)(b+P) = ab+P = 0+P$

$\Rightarrow a+P = P$ oder $b+P = P \Rightarrow a \in P$ oder $b \in P$

□

DEF. 2: Ein Ideal $M \subseteq R$ heißt **maximales Ideal**, wenn

(a) $M \neq R$,

(b) $\nexists$ Ideal $I \subseteq R$ mit $M \subsetneq I \subsetneq R$.

[(b) $\Leftrightarrow$ $\forall$ Ideal $I \subseteq R$ mit $I \supseteq M \Rightarrow I = R$ oder $I = M$]

[es kann verschiedene max. Ideale geben]

SATZ 2: R komm. Ring mit $1 \neq 0$, $M \subseteq R$ Ideal:

M maximales Ideal $\Leftrightarrow$ R/M Körper.

Beweisskizze: • falls $1 \in M$, dann $M = R$ und $R/M = \{0+M\}$ kein Körper und M nicht max. Ideal

• $1 \notin M \Rightarrow R/M$ Ring mit $1+M \neq 0+M$;
nach Satz (ii) und (iii) in 4.1 ist [bzw. UE]

R/M Körper $\Leftrightarrow$ R/M besitzt keine nichttrivialen Ideale

$\Updownarrow$ (leicht zu zeigen*)

$\nexists\, I \subseteq R$ Ideal mit $M \subsetneq I \subsetneq R$ □

*Entweder Korrespondenzsatz [Fischer II.2.2] oder direkt: • I Ideal, $M \subsetneq I \subsetneq R$, dann $\tilde{I} := \{a+M \mid a \in I\}$ Ideal in R/M; $\tilde{I} \neq \{M\}$ und $\tilde{I} \neq R/M$

• $\tilde{J}$ Ideal in R/M, $\{0\} \neq \tilde{J} \subsetneq R/M$, dann setze $J := \{a \in R \mid a+M \in \tilde{J}\}$; J Ideal in R: $a \in J, y \in R \Rightarrow ay+M = \underbrace{(a+M)}_{\in \tilde{J}}\underbrace{(y+M)}_{\in \tilde{J}}$

$\Rightarrow ay \in J$; $J \neq M$, weil $\exists\, a+M \in \tilde{J} \setminus \{M\}$; $J \supseteq M$;
$J \neq R$, weil $\tilde{J} \subsetneq R/M$

KOR: R komm. Ring mit $1 \neq 0$, dann ist jedes maximale Ideal auch Primideal.

BEISP: 1) in $\mathbb{Z}$ ist jedes Ideal von der Form $m\mathbb{Z}$;
$0 \cdot \mathbb{Z} = \{0\}$ und $1 \cdot \mathbb{Z} = \mathbb{Z}$ keine max. Ideale; also $m \geq 2$:

$\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ Integr.bereich $\overset{\mathbb{Z}_m \text{ endl.}}{\Leftrightarrow}$ $\mathbb{Z}_m$ Körper

$[\Leftrightarrow m\mathbb{Z}$ Primideal$]$ $[\Leftrightarrow m\mathbb{Z}$ max. Ideal$]$

$\Leftrightarrow m$ Primzahl

also: $m\mathbb{Z}$ Primideal $\Leftrightarrow m\mathbb{Z}$ max. Ideal $\Leftrightarrow m$ Primzahl;

weiters: $m\mathbb{Z} \subseteq n\mathbb{Z} \Leftrightarrow m = nk$ mit $k \in \mathbb{Z} \Leftrightarrow n \mid m$;

somit: $m\mathbb{Z}$ enthalten im max. Ideal $p\mathbb{Z}$, wenn p Primteiler von m.

2) $K[X]$ mit Körper K (Hauptidealring)

sei $a \in K$ und $\varphi: K[X] \to K,\ f \mapsto f(a)$ ... Auswertung bei a

- φ Ringhomo
- $f \in \ker\varphi \Leftrightarrow f(a) = 0 \Rightarrow f = (X-a)q,\ q \in K[X]$

$\Rightarrow \ker\varphi \subseteq (X-a)\cdot K[X]$; weil $\ker\varphi$ Ideal und $K[X]$ Hauptidealring, muss $\ker\varphi = (X-a)\cdot K[X] = (X-a)$ gelten

- φ surjektiv, weil $\forall b \in K: \varphi(b) = b$;

Isomorphiesatz $\Rightarrow K[X]/(X-a) \cong K$ ... Körper $\Rightarrow$

$(X-a) = \ker\varphi$ ist max. Ideal in $K[X]$

3) betrachte nun $\varphi: \mathbb{R}[X] \to \mathbb{C},\ f \mapsto f(i)$ [Variante von 2), $i \notin \mathbb{R}$]

- φ Ringhomo [vgl. 4.3.2) bzw. UE] (evtl. wegfallen)
- $\varphi(X^2+1) = i^2+1 = 0 \Rightarrow X^2+1 \in \ker\varphi$

$\Rightarrow (X^2+1) \subseteq \ker\varphi$ [es könnte im Prinzip noch $(X^2+1) \subsetneq \ker\varphi = (f)$ mit $f \neq X^2+1$ geben]

- ist $f \in \ker\varphi \Rightarrow f(i) = 0$;

f aufgefasst als Polynom in $\mathbb{C}[X]$ mit reellen Koeffizienten; daher auch $-i$ Nullstelle von f;

$$\left[\overline{f(X)} = \overline{a_0 + a_1 X + \dots + a_n X^n} = \overline{a_0} + \overline{a_1}\cdot\overline{X} + \dots + \overline{a_n}\,\overline{X}^n = a_0 + a_1\overline{X} + \dots + a_n\overline{X}^n = f(\overline{X}),\ \text{wenn } \overline{a_j} = a_j\right]$$

als Polynom in $\mathbb{C}[X]$ kann f durch $(X-i)$ und $(X+i)$ dividiert werden $\Rightarrow \exists\, q \in \mathbb{C}[X]$:

$$f = (X-i)(X+i)\,q = \underbrace{(X^2+1)}_{\text{reelle Koeff.}}\cdot q \Rightarrow \text{auch } q \text{ reelle Koeff.}$$

$\Rightarrow f = (X^2+1)\cdot q$ mit $q \in \mathbb{R}[X]$

- somit $\ker\varphi = (X^2+1)$

- φ surjektiv, weil $\varphi(a) = a \quad \forall a \in \mathbb{R}$
  und $\varphi(X) = i$, also $\varphi(a+bX) = a+ib$

Isomorphiesatz $\Rightarrow \mathbb{R}[X]/(X^2+1) \cong \mathbb{C}$ ... Körper

$\Rightarrow (X^2+1)$ max. Ideal in $\mathbb{R}[X]$

BEM.(o.B): (i) in $\mathbb{C}[X]$ sind max. Ideale von der Form $(X-\lambda)$, $\lambda \in \mathbb{C}$

(ii) jedes Ideal in einem kommut. Ring mit $1 \neq 0$ ist in einem maximalen Ideal enthalten (Auswahlaxiom)

(iii) R kommut. Ring mit $1 \neq 0 \Rightarrow R^\times = \bigcap_{\substack{M \text{ max.} \\ \text{Ideal in } R}} R \setminus M$

(weggelassen)

§5 TEILBARKEIT UND IRREDUZIBILITÄT IN INTEGRITÄTSBEREICHEN

5.1. Irreduzible Elemente

nun immer R ein Integritätsbereich, also kommutativ, mit 1 und nullteilerfrei, $1 \neq 0$

DEF: $q \in R$ heißt **irreduzibel**, wenn:

(a) $q \neq 0$ und $q \notin R^\times$,

(b) falls $q = a \cdot b$ mit $a, b \in R$, dann $a \in R^\times$ oder $b \in R^\times$.

Andernfalls nennen wir q **reduzibel**; also sind reduzibel: 0, Einheiten, Produkte von Nichteinheiten.

Beisp: $\mathbb{Z}^\times = \{-1, +1\}$ und die irreduziblen Elemente in $\mathbb{Z}$ sind genau die Primzahlen und ihre negativ gespiegelten Zahlen

SATZ: R Hauptidealring und $a \in R$ irreduzibel

$\Rightarrow R/(a)$ Körper

(Verallgemeinerung von p Primzahl $\Rightarrow \mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ Körper)

Beweis: $R/(a)$ ist komm. Ring mit Einselement $\neq (a)$

noch z.z.: jedes $b + (a) \neq 0 + (a)$ ist invertierbar:

$b + (a) \neq (a) \Rightarrow b \notin (a) \Rightarrow I := \{xa + yb \mid x, y \in R\} \supsetneq (a)$

(wir schreiben: $I = (a, b)$)

I ist (das von a und b erzeugte) Ideal:

- $I \neq \emptyset$; $(x_1 a + y_1 b) - (x_2 a + y_2 b) = (x_1 - x_2) a + (y_1 - y_2) b \in I$
- $z \in R$, $xa + yb \in I \Rightarrow z \cdot (xa + yb) = (zx) a + (zy) b \in I$

R Hauptideal $\Rightarrow \exists c \in R: I = (c)$, $\left[(c) \supsetneq (a)\right]$

wegen $a \in I$ $\exists d \in R: a = d \cdot c$;

wäre $d \in R^\times$, denn $c = d^{-1} a \in (a)$, also $(c) \subseteq (a)$ ↯

somit $d \notin R^\times$; a irreduzibel $\Rightarrow c \in R^\times$;

daher $R = (c) = I \Rightarrow 1 \in I \Rightarrow \exists x, y \in R:$

$1 = xa + yb$, d.h. $yb - 1 \in (a)$;

also $(y + (a)) \cdot (b + (a)) = yb + (a) = 1 + (a)$,

d.h. $b + (a)$ invertierbar □

BEM: $p \neq 0$, $p \notin R^\times$, dann gilt:

p irreduzibel $\Leftrightarrow$ (p) maximal als Hauptideal

[d.h. $\nexists a \in R: (p) \subsetneq (a) \subsetneq R$]

(Beweis als UE)

5.2. Teiler und Primelemente

$a \in R$ heißt <u>Teiler</u> von $b \in R$, wir schreiben $a \mid b$, wenn $\exists\, c \in R$ mit $b = c \cdot a$.

<u>einfache Eigenschaften</u>: (i) $a \mid b \iff (b) \subseteq (a)$

(ii) $a \mid 0$, $1 \mid a$, $a \mid a$; $0 \mid a \iff a = 0$

(iii) $a \mid b$ und $b \mid c \Rightarrow a \mid c$; $a \mid b$ und $c \mid d \Rightarrow ac \mid bd$

(iv) $a \mid b_1$ und $a \mid b_2 \Rightarrow a \mid (x_1 b_1 + x_2 b_2)$ $\forall x_1, x_2 \in R$

(v) $a \mid 1 \iff a \in R^\times$

(vi) $a \mid b \Rightarrow (ax) \mid b$ $\forall x \in R^\times$

[alle Beweise unmittelbar klar; (vi): $b = ca \Rightarrow b = c(x^{-1}x)a = (cx^{-1})(xa)$]

- dieses bekannt aus Zahlentheorie für $R = \mathbb{Z}$, mit der Spezialsituation, dass $\mathbb{Z}^\times = \{-1, 1\}$ besonders einfach ist, sodass in $\mathbb{Z}$: $a \mid b \iff a \mid (-b)$;

allgemeiner: $a \sim b :\iff a \mid b$ und $b \mid a$,
a und b heißen dann assoziiert;

- $a \sim b \iff \exists\, x \in R^\times : b = x \cdot a \iff (a) = (b)$

(Beweis als UE)

DEF: $p \in R$ heißt **Primelement** oder **prim**, wenn:

(a) $p \neq 0$ und $p \notin R^\times$,

(b) falls $p \mid (ab)$ mit $a, b \in R$, dann $p \mid a$ oder $p \mid b$.

LEMMA: Jedes Primelement ist irreduzibel.

Beweis: Sei $p = a \cdot b$; dann muss also $p \mid a$ oder $p \mid b$ gelten; o.B.d.A. $p \mid a$; somit $\exists\, c \in R: a = cp$

$$\Rightarrow p = ab = (cp)b = (cb)p \overset{\text{[Kürzen erlaubt]}}{\Rightarrow} cb = 1$$

$$\Rightarrow b \in R^\times$$

□

Beisp: in $\mathbb{Z}$ sind genau die Primzahlen und deren Negative die Primelemente; werden gleich sehen, dass die Begriffe irreduzibel und prim in Hauptidealringen immer zusammenfallen

BEM: $p \neq 0$, $p \notin R^\times$, dann gilt:

p prim $\Leftrightarrow$ (p) Primideal

(Beweis als UE)

SATZ: In einem Hauptidealring stimmen die Begriffe Primelement und irreduzibles Element überein; weiters ist ein Ideal ein Primideal genau dann, wenn es ein maximales Ideal ist.

Beweis: wir wissen bereits „prim ⇒ irreduzibel" [obiges Lemma] und „maximales Ideal ⇒ Primideal" [Kor. in 4.5];

- ist p irreduzibel $\overset{[5.1,\text{Satz}]}{\Rightarrow}$ $R/(p)$ Körper $\overset{[4.5,\text{Satz 2}]}{\Rightarrow}$ (p) maximales Ideal $\Rightarrow$ (p) Primideal $\overset{[\text{obige Bem.}]}{\Rightarrow}$ p prim;
- ist I Primideal $\overset{[\text{Hauptidealring}]}{\Rightarrow}$ $\exists\, p \in R: I=(p)$ $\overset{[\text{obige Bem.}]}{\Rightarrow}$ p prim $\Rightarrow$ p irreduzibel $\overset{[5.1,\text{Satz}]}{\Rightarrow}$ $R/(p)$ Körper $\overset{[4.5,\text{Satz 2}]}{\Rightarrow}$ (p) maximales Ideal $\overset{[(p)=I]}{\Rightarrow}$ I max. Ideal

□

BEISP: $\mathbb{Z}[X]$ kein Hauptidealring [4.4, Beisp. 3)].

$X \in \mathbb{Z}[X]$ Primelement: $X \mid f\cdot g \Rightarrow X \mid f$ oder $X \mid g$ / aber

(X) Primideal, aber kein Hauptideal maximal: $(X) \subsetneq (2,X) \subsetneq \mathbb{Z}[X]$ [siehe 4.4, Beisp. 3)]

5.3. Eindeutige Primfaktorzerlegung

Ohne Beweise (vgl. Fischer, Kap. II, 3.5 und 3.7) erwähnen wir, dass jeder Hauptidealring – also speziell $\mathbb{Z}$ und $K[X]$ für einen Körper K – sowie auch $\mathbb{Z}[X]$ (kein Hauptidealring) die folgende Eigenschaft besitzen: Für jedes $a \in R$, $a \neq 0$ und $a \notin R^\times$ gibt irreduzible (oder gleichwertig prime) Elemente $q_1, \dots, q_r \in R$ mit $a = q_1 \cdots q_r$ und diese Darstellung ist eindeutig bis auf die Reihenfolge und Einheiten als Faktoren.

Solche Integritätsbereiche heißen <u>faktorielle Ringe</u> (oder Gauß'sche Ringe oder ZPE-Ringe).

Es kann dann eine Teilmenge $P \subseteq R$ von Primelementen (bzw. irreduziblen Elementen) ausgewählt werden (je ein Vertreter für alle assoziierten Elemente), sodass wir schreiben können (mit „endlichem" Produkt):

$$a = \varepsilon(a) \cdot \prod_{p \in P} p^{\nu_p(a)} \quad \text{mit } \varepsilon(a) \in R^\times, \begin{cases} \nu_p(a) \in \mathbb{N}, \text{ nur} \\ \text{endl. viele} \neq 0 \end{cases}$$

5.4. Irreduzibilität von Polynomen

erinnere: $R[X]^\times = R^\times$ für Integr.bereich R (Sätzchen in 3.6)

also: $f \in R[X]^\times \Leftrightarrow f = a_0$ mit $a_0 \in R^\times$

Beispiele für Änderung der Irreduzibilität beim Übergang zu anderem Grundring:

1) $f = 2X$ irreduzibel in $\mathbb{Q}[X]$, reduzibel in $\mathbb{Z}[X]$:

- in $\mathbb{Z}[X]$: $f = 2 \cdot X$ und weder 2 noch X Einheiten
- in $\mathbb{Q}[X]$: $2X = g \cdot h \Rightarrow \operatorname{grad}(g) + \operatorname{grad}(h) = 1$;
  OBdA $\operatorname{grad}(g) = 0$, $\operatorname{grad}(h) = 1$, d.h.
  $g = a_0$, $h = b_0 + b_1 X$; somit
  $2X = a_0 \cdot (b_0 + b_1 X) = a_0 b_0 + a_0 b_1 X \Rightarrow$
  $a_0 b_0 = 0$, $a_0 b_1 = 2 \Rightarrow \underbrace{a_0 \neq 0}, b_0 = 0$
  $\Rightarrow g$ Einheit

2) $f = 2$ reduzibel in $\mathbb{Q}[X]$, irreduzibel in $\mathbb{Z}[X]$:

- in $\mathbb{Q}[X]$: 2 invertierbar, also Einheit
- in $\mathbb{Z}[X]$: $2 = g \cdot h \Rightarrow \operatorname{grad}(g) = \operatorname{grad}(h) = 0$;
  $2 = a_0 \cdot b_0 \Rightarrow (a_0 = 2 \wedge b_0 = 1)$ (Einh.) oder $(a_0 = 1 \wedge b_0 = 2)$ (Einh.) $\Rightarrow$ gerade Einh.

3) X^2+1 irreduzibel in $\mathbb{R}[X]$, reduzibel in $\mathbb{C}[X]$

- in $\mathbb{C}[X]$: $X^2+1 = (X-i)(X+i)$

  ↑ beides keine Einheiten, weil $\text{grad} > 0$

- in $\mathbb{R}[X]$: wissen aus 4.5, Beisp. 3), dass (X^2+1) max. Ideal ist, weil $\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}$ Körper; somit X^2+1 irreduzibel nach 5.1;

  <u>aber direkt z.B. so:</u> $X^2+1 = g \cdot h \Rightarrow$

  $\text{grad}(g) + \text{grad}(h) = 2$; $\text{grad}(g)=0$ oder $\text{grad}(h)=0$ ergibt, dass g oder h Einheit ist, weil $\mathbb{R}$ Körper;

  bleibt $\text{grad}(g) = \text{grad}(h) = 1$ zu betrachten, d.h. $g = a_0 + a_1 X$, $h = b_0 + b_1 X$ $[a_1, b_1 \neq 0]$ $\Rightarrow$

  $$X^2+1 = a_1 b_1 \left(X + \frac{a_0}{a_1}\right)\left(X + \frac{b_0}{b_1}\right) \Rightarrow$$

  X^2+1 hat reelle Nullstellen $-\frac{a_0}{a_1}, -\frac{b_0}{b_1}$;

  aber $X^2+1 \geq 1$ hat keine reellen Nst. ↯

4) $a \in R \Rightarrow X-a$ irreduzibel in $R'[X]$ für jeden Oberring R' von R (mit demselben Einselement):

$X - a = f \cdot g \Rightarrow \begin{matrix} f = a_0, \\ g = b_0 + b_1 X \end{matrix} \Rightarrow a_0 \cdot b_0 = 1 \Rightarrow a_0 \in R^\times \subseteq (R')^\times \Rightarrow f$ Einheit

BEM: Beisp. 2) (2 red. in $\mathbb{Q}[X]$ und irred. in $\mathbb{Z}[X]$)

ist ein Ausnahmefall, denn für $f \in \mathbb{Z}[X]$ mit $\deg(f) \geq 1$ gilt der Irreduzibilitätssatz [Fischer, Kap. II, 3.7]:

f irreduzibel in $\mathbb{Z}[X] \Rightarrow f$ irreduzibel in $\mathbb{Q}[X]$.

Irreduzibilität in $K[X]$ für K Körper:

wegen $K^\times = K \setminus \{0\}$ sind alle Polynome vom Grad 0 Einheiten in $K[X]$, und dies sind alle Einheiten, also

$$K[X]^\times = \{ f = a_0 \mid a_0 \in K \setminus \{0\} \} = \{ f \mid \deg(f) = 0 \},$$

ist $f = g \cdot h$ und g oder h eine Einheit in $K[X]$, dann folgt also $f = a_0 \cdot q$ mit $a_0 \in K \setminus \{0\}$, $q \in K[X]$, d.h. irreduzible Polynome $f \in K[X]$ erfüllen $\deg(f) \geq 1$ (sonst $f = 0$ oder $f = a_0$ mit $a_0 \neq 0$ f Einheit) und lassen sich nun durch Herausheben eines konstanten Faktors $\neq 0$ als Produkt von Polynomen aus $K[X]$ zerlegen.

Insbesondere haben irreduzible Polynome vom Grad ≥ 2 keine Nullstellen in K. (Umkehrung davon gilt nicht: $(X^2+1)(X^2+1)$ ist reduzibel und hat keine Nst. in $\mathbb{R}$)