Definition 2.1 Ein Ring besteht aus einem Quintupel $(R, +, 0, \cdot, 1)$ sodass
- $(R, +, 0)$ eine abelsche Gruppe, und
- $(R, \cdot, 1)$ ein Monoid, [illegible] ist, und
- für alle $a, b, c \in R$ gilt $(a+b)c = ac + bc$, $c(a+b) = ca + cb$ (Distributivität).

Ein Ring heißt kommutativ, falls $\cdot$ kommutativ ist.

Bemerkungen
- wir verlangen nicht, dass $0 \neq 1$. Falls $0 = 1$, so folgt aber, dass $R = \{0\}$. (ÜA)
- es gilt zB $(-a)b = -(ab)$ wie wir es von $\mathbb{Z}$ gewohnt sind
- es gilt zB nicht, dass aus $ab = 0$ folgt, dass $a = 0$ oder $b = 0$ siehe Bsp 2.2. e)

Ein Ringhom $f: R \to S$ ist eine Gruppenhomom. $(R,+,0) \to (S,+,0)$ welcher auch ein Monoidhom. $(R,\cdot,1) \to (S,\cdot,1)$ ist. Isomorphismus falls f bijektiv ist ($\Leftrightarrow \exists g: S \to R$ Ringhom s.d. ...)
Eine Teilmenge $S \subseteq R$ heißt Unterring von R falls S bzgl $+$ eine UG und bzgl $\cdot$ ein UM ist (d.h. $0,1 \in S$ und $\forall a,b \in S$ gilt $a+b \in S$, $-a \in S$ und $ab \in S$.).

Ein injektiver Ringhom $f: R \hookrightarrow S$ identifiziert R mit einem Unterring von S (dem Bild von f). Wir nennen dann auch S eine Ringerweiterung von R. (und schreiben dass S/R Erw.)

Wir schreiben $R^\times = (R,\cdot,1)^\times = \{a \in R \mid \exists$ inv. bzgl $\cdot$ von $a\}$.
und nennen $R^\times$ die Gruppe der Einheiten von R
Ein Ring ist ein Schiefkörper falls $R^\times = R \setminus \{0\}$
Ein Schiefkörper heißt Körper, falls er kommutativ ist.

In einem Ring heißt ein Element a (rechts/links) Nullteiler falls es $b \in R$ gibt mit $ab=0$ / $ba=0$. (nur Nullteiler falls R kommutativ)
Ein Ring heißt nullteilerfrei, falls a Nullteiler $\Rightarrow a=0$
Ein komm. nullteilerfreier Ring heißt Integritätsbereich

Beispiele 2.2 a) $(\mathbb{Z},+,0,\cdot,1)$ ist ein Integritätsbereich, $\mathbb{Z}^\times = \{\pm 1\}$.
$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind Körper

b) $\mathbb{H}$ = Quaternionen: $\mathbb{H} = \mathbb{R}$-VR mit basis $\{e,i,j,k\}$
definiere multiplikation durch
- e = neutraler Element
- $i^2 = j^2 = k^2 = -e$
- $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$

Dann ist $\mathbb{H}$ ein Schiefkörper
Satz $\mathbb{R}, \mathbb{C}, \mathbb{H}$ sind die einzigen Schiefkörper / $\mathbb{R}$ (nicht trivial) !

c) K Körper (oder ring), $M_n(K)$ Ring bzgl. $+$ und $\cdot$
$M_n(K)^\times = GL_n(K)$, für $n \geq 2$ ist $M_n(K)$ nicht komm.

d) $V \neq K\text{-VR}$, $\mathrm{End}_K(V) = \{ f : V \to V \mid f \ K\text{-linear} \}$
ist ein Ring bzgl $+$ und $\circ$ = Komposition.
ÜA: $\dim(V) = n$, so ist $\mathrm{End}_K(V) \underset{\text{ring}}{\cong} M_n(K)$

e) R ring, X Menge. $\mathrm{Hom}_{\text{Mengen}}(X, R)$ ist ein Ring durch:
$(f+g)(x) = f(x) + g(x)$, $(f * g)(x) = f(x) * g(x)$, $0(x) = 0$, $1(x) = 1$.

Ist $\mathrm{Hom}^{\text{endl. tr.}}_{\text{Mengen}}(X, R) = \{ f : X \to R \mid f(x) = 0 \text{ fast immer} \}$ ein Ring?

Wir schreiben auch $\prod_{x \in X} R$, für $|X| = 2$ schreiben wir $R \times R$
$R \times R$ ist kein Integritätsbereich: $(0,1) \cdot (1,0) = (0,0)$

f) X Menge, $\forall x \in X$ sei R_x ein Ring. Dann ist $\prod_{x \in X} R_x$ mit komponentenweiser addition + multipl. ein Ring, $\forall y \in X$ ist die projektion $\prod_{x \in X} R_x \to R_y$ ein Ringhom.

g) $p \geq 2$, $\mathbb{Z}/n\mathbb{Z}$ hat multipl. $[n] \cdot [m] = [nm]$, für $n = p$ schreiben wir $\mathbb{F}_p$. (Körper (siehe später))
Sei nun R ein kommutativer Ring. Wir definieren im Folgenden den Polynomring $R[X]$ über R.

Betrachte dazu die Menge $R^{(\mathbb{N})} = \mathrm{Hom}^{\text{endl. tr.}}_{\text{Mengen}}(\mathbb{N}, R)$

dies ist kanonisch eine abelsche Gruppe unter „punktweise addieren in R".
(Bsp 12. f) definiere eine multiplikation wie folgt:
$(f * g)(n) = \sum_{i+j=n} f(i) \cdot g(j)$. Dann gelten

a) $f * g \in R^{(\mathbb{N})}$ b) $e = \begin{cases} n \mapsto 1 & n = 0 \\ n \mapsto 0 & n \neq 0 \end{cases}$ erfüllt
$f * e = f = e * f$. $\forall f \in R^{(\mathbb{N})}$.

Man rechnet nach, dass $*$ assoziativ ist und mit $+$ das distributivitätsgesetz erfüllt, $(R^{(\mathbb{N})}, +, 0, *, e)$ ist dann ein (kommutativer) Ring welchen wir mit $R[X]$ bezeichnen.

Für $f \in R[X]$ schreiben wir $f = \sum_{i=0} f(i) X^i$
$R \hookrightarrow R[X]$, $a \mapsto a \cdot X^0$ ist ein Unterring.

Bemerkung: (Polynome definieren Funktion durch einsetzen).
Sei $f \in R[X]$ und $c \in R$. Dann schreibt man
$f(c)$ für $\sum_{i \geq 0} f(i) c^i \in R$.

$(f, c) \longmapsto f(c)$
So bekommt man eine Abbildung $R[X] \times R \longrightarrow R$

Beispiel 2.3 (Polynome sind nicht das gleiche wie Funktionen)
sei $R = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ einer $+$ und $\cdot$ (mit Rest) (Bsp 2.2.g))
betrachte $f = X^p - X \neq 0 \in \mathbb{F}_p[X]$.
es gilt aber, dass die von f induz. Funktion $\mathbb{F}_p \to \mathbb{F}_p$ gegeben ist durch $n \mapsto n^p - n$. Aber $n^p \equiv n$ modulo p (EWA)

Ist $f \in R[X]$ so setzen wir den Grad von f als

$$\operatorname{grad}(f) := \sup_{n \geq 0} \{ f(n) \neq 0 \} \qquad (\sup \emptyset = -\infty)$$

schreiben wir $f = \sum_{i \geq 0} a_i X^i$ so ist $a_{\operatorname{grad}(f)}$ der Leitkoeffizient von f. Ist dieser 1, so sagen wir, dass f ein normiertes Polynom ist.
Ist der Leitkoeff. a von f ein element von $R^\times$, so ist $a^{-1} \cdot f$ ein normiertes Polynom.

Lemma 2.4 Sei R kommm. rng, $f \in R[X]$. Dann gelten
1) $\operatorname{grad}(f+g) \leq \max\{\operatorname{grad}(f), \operatorname{grad}(g)\}$
2) $\operatorname{grad}(f \cdot g) \leq \operatorname{grad}(f) + \operatorname{grad}(g)$.
Ist R Integritätsbereich, so gilt in 2) Gleichheit, $R[X]$ ist wieder ein Integritätsbereich und $(R[X])^\times \xrightarrow{\cong} R^\times$

Beweis: 1) schreibe $f = \sum_{i=0}^{n=\operatorname{grad}(f)} a_i X^i$ $g = \sum_{i=0}^{m=\operatorname{grad}(g)} b_i X^i$. Für $i > \max(n,m)$ gilt $a_i + b_i = 0$. $\Rightarrow$ 1) Der Koeff. von $f+g$ bei X^j ist $\sum_{i+k=j} a_i b_k$. Für $j > n+m$ ist $a_i b_k = 0 \Rightarrow$ 2)

nehmen wir an, R ist Integritätsbereich. Dann gilt $fg(n+m) = a_n b_m \neq 0$.

also folgt Gleichheit in 2) und auch, dass $R[X]$ Integritätsbereich ist.
Sei $f \in R[X]^\times$. Sei $g \in R[X]$ mit $fg = 1$. Dann gilt
$\operatorname{grad}(fg) = 0$ und es folgt dass $\operatorname{grad}(f) = 0$ due 2). ∎

Satz 2.5 (Division mit Rest) Sei R ein komm. Ring, $g \in R[X]$ $n = \operatorname{grad}(g)$ $(= \sum b_n x^n)$
mit $b_n \in R^\times$. Für $f \in R[X]$ existieren eindeutige $q, r \in R[X]$
sodass $\operatorname{grad}(r) < n$ und $f = g \cdot q + r$

Beweis: Zunächst: sei $h \in R[X]$ dann gilt $\operatorname{grad}(gh) = \operatorname{grad}(g) + \operatorname{grad}(h)$
den der Leitkoeff. von g ist eine Einheit.
Wir zeigen zuerst die Eindeutigkeit: seien dafür q, r und q', r'
mit $\operatorname{grad}(r), \operatorname{grad}(r') < n$ und $f = gq + r = gq' + r'$.
Dann gilt $r - r' = g(q' - q)$ und somit

$$\underbrace{\operatorname{grad}(r - r')}_{<n} = \underbrace{\operatorname{grad}(g)}_{\geq n} + \operatorname{grad}(q' - q) \quad \Rightarrow \text{ beide Seiten müssen } -\infty \text{ sein}$$
$$\Rightarrow g = g' \text{ und } r = r'.$$

Existenz: Induktion über $\operatorname{grad}(f)$: ist $\operatorname{grad}(f) < 0$ (also $f = 0$ so: $q = r = 0$)
sei nun $m = \operatorname{grad}(f) \geq 0$.
betrachte $h = f - \frac{a_m}{b_n} X^{m-n} g$, $f = h + \frac{a_m}{b_n} X^{m-n} g$

so gilt $\operatorname{grad}(h) < \operatorname{grad}(f)$. Nach Induktion gilt also

$$h = gq + r \quad \text{und somit} \quad f = gq + r + \frac{a_m}{b_n} X^{m-n} g$$
$$= \left(q + \frac{a_m}{b_n} X^{m-n}\right) g + r$$
∎

Definition 2.6 Sei R ein Ring. ein (Links/rechts) Ideal $\mathfrak{a} \subseteq R$ ist eine UG
von $(R, +, 0)$ sodass $\forall a \in \mathfrak{a}$ und $r \in R$ gilt dass $ra \in R$ / $ar \in R$.
Ist R kommutativ so sprechen wir einfach von einem Ideal = Linksideal = Rechtsideal

Beispiele 2.7 a) $\{0\}, R \subseteq R$ sind die trivialen Ideale.
ist $1 \in \mathfrak{a} \Rightarrow \mathfrak{a} = R$ $(r \cdot 1 = r \in \mathfrak{a})$.

b) die UG $m\mathbb{Z} \subseteq \mathbb{Z}$ sind Ideale und jedes Ideal hat diese Form

c) In einem Körper gibt es nur die trivialen Ideale:
Sei $0 \neq \mathfrak{a} \subseteq K$ Ideal, $x \in \mathfrak{a} - \{0\}$. Dann ist $1 \in x \cdot x^{-1} \in \mathfrak{a}$ und damit nach a) $\mathfrak{a} = K$.

Sind $\mathfrak{a}, \mathfrak{b} \subseteq R$ Ideale so gibt es folgende neue Ideale:

$$\mathfrak{a} + \mathfrak{b} = \{a + b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}$$

$$\mathfrak{a}\mathfrak{b} = \left\{\sum_{i=1}^{n} a_i b_i \mid a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\right\}$$

$$\mathfrak{a} \cap \mathfrak{b} = \{x \mid x \in \mathfrak{a} \text{ und } x \in \mathfrak{b}\}$$

Induktiv lassen sich Summen, Produkte und Schnitte von endlich vielen Idealen definieren, geschrieben $\sum_{i \in I} \mathfrak{a}_i$, $\prod_{i \in I} \mathfrak{a}_i$ und $\bigcap_{i \in I} \mathfrak{a}_i$.

Ist $a \in R$, so ist $(a) \subseteq R$ das von a erzeugte Ideal:

$$(a) = Ra = \{r \cdot a \mid a \cdot r \in R\}$$

Sind $a_1, \dots, a_n \in R$ so ist $(a_1, \dots, a_n) = (a_1) + \dots + (a_n)$ dies sind jeweils die kleinsten Ideale von R, welche a_i bzw. $a_1, \dots, a_n$ enthalten.

Definition 2.8 R komm. Ring $\mathfrak{a} \subseteq R$ Ideal. Eine Teilmenge $\{a_i\}_{i \in I} \subseteq R$ heißt Erzeugendensystem von $\mathfrak{a}$ falls $\mathfrak{a} = \sum_{i \in I} (a_i)$. $\mathfrak{a}$ heißt endlich erzeugt, falls es ein endliches Erzeugendensystem gibt. $\mathfrak{a}$ heißt Hauptideal, falls es von einem Element erzeugt wird. Ein Hauptidealring ist ein Integritätsbereich indem jedes Ideal ein Hauptideal ist.

Beispiele 2.9 a) $\mathbb{Z}$ ist ein Hauptidealring (Jedes Ideal ist $m\mathbb{Z} = (m)$ für ein m)

b) $K[X]$ für K ein Körper ist ein Hauptidealring:
Sei $0 \neq \mathfrak{a} \subseteq K[X]$ Ideal. Sei $f \in \mathfrak{a} - \{0\}$ mit minimalem Grad
Beh: $(f) = \mathfrak{a}$. Klar ist, dass $(f) \subseteq \mathfrak{a}$. Sei also $g \in \mathfrak{a}$.
Nach Satz 2.5 gilt $g = fq + r$ mit $\operatorname{grad}(r) < \operatorname{grad}(f)$
$\Rightarrow r = g - fq \in \mathfrak{a} \Rightarrow r = 0$ und damit $g \in (f)$.

c) R Hauptidealring, $\mathfrak{a} = (a)$ und $\mathfrak{b} = (b)$ Ideale in R so gilt
$\mathfrak{a} = \mathfrak{b} \iff a = cb$ für $c \in R^\times$ (das gilt allg. in Integritätsbereichen)

d) $R = \mathbb{Z}[X]$. Betrachte das Ideal welches von $\{2, X\}$ aufgespannt wird.
dies ist kein Hauptideal. (ÜA)

Bemerkung: $R \xrightarrow{\varphi} R'$ Ringhomom. zw. komm. Ringen.
Dann ist $\mathrm{Im}(\varphi) \subseteq R'$ ein Unterring und
$\ker(\varphi) \subseteq R$ ein Ideal

Insbesondere: Ein Ringhom $K \xrightarrow{\varphi} R$ mit K Körper ist injektiv (oder $R = 0$)
denn: $\ker(\varphi) \subseteq K$ Ideal, also $\{0\}$ oder K. Ist $\ker(\varphi) = K$ so gilt
$1 = \varphi(1) = 0$ in R und somit dass $R = 0$.

Beispiele 2.1: a) $\mathrm{Hom}_{\mathrm{Ring}}(\mathbb{Z}, R) \cong \{*\}$: $1 \overset{\varphi}{\mapsto} 1$ und Bsp 6.a)

b) $R \to R'$ Ringhom und $c \in R'$. Dann ist $R[X] \to R'$, $f \mapsto f(c)$
ein Ringhomom.

c) $\mathbb{C} \to \mathbb{C}$, $x \mapsto \overline{x}$ ist ein Ringhomom.

d) für $n \geq 1$ gibt es keinen Ringhom. $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}$.

Konstruktion: R komm. Ring, $\mathfrak{a} \subseteq R$ ideal. Dann ist $\mathfrak{a} \subseteq R$ ein
NT bzgl $+$ [$(R, +, 0)$ ist abelsch] und somit $R/\mathfrak{a}$ eine abelsche
Gruppe. Wir definieren eine Multiplikation auf $R/\mathfrak{a}$ sd. die
Projektion $R \xrightarrow{\pi} R/\mathfrak{a}$ multiplikativ ist durch:
$[r] \cdot [r'] = [r \cdot r']$. dies ist wohldefiniert:
ist $[r] = [s]$ so gilt $r = s + a$ für $a \in \mathfrak{a}$.
dann gilt $r \cdot r' = (s+a) r' = sr' + ar'$ und $ar' \in \mathfrak{a}$ sd.
$[rr'] = [sr']$.
π ist dann ein surjektiver Ringhomom. mit $\ker(\pi) = \mathfrak{a}$.

Es gilt das Analogon von Satz 1.12:

Satz 2.12 Sei $\varphi: R \to R'$ ein Ringhomom., $\mathfrak{a} \subseteq R$ Ideal mit $\mathfrak{a} \subseteq \ker(\varphi)$. Dann existiert ein eind. Ringhom $\bar{\varphi}: R/\mathfrak{a} \to R'$ sd. $R \xrightarrow{\varphi} R'$ kommutiert. Es gelten

$\pi \downarrow \nearrow \bar{\varphi}$ mit $R/\mathfrak{a}$

- $\mathrm{Im}(\varphi) = \mathrm{Im}(\bar{\varphi})$
- $\ker(\bar{\varphi}) = \pi(\ker(\varphi))$ und $\ker(\varphi) = \pi^{-1}(\ker(\bar{\varphi}))$

$\bar{\varphi}$ ist genau dann injektiv wenn $\mathfrak{a} = \ker(\varphi)$.

Beweis: 1.12 gibt einen eind. Gruppenhom $\bar{\varphi}$ mit obigen Eigenschaften. per Konstruktion ist dieses $\bar{\varphi}$ ein Ringhomom: $\bar{\varphi}([r]\cdot[s]) = \bar{\varphi}([rs]) = \varphi(rs) = \varphi(r)\cdot\varphi(s) = \bar{\varphi}([r])\cdot\bar{\varphi}([s])$. ∎

Korollar 2.13 Ist $\varphi: R \to R'$ ein surjektiver Ringhom, so induziert φ einen Isomorphismus $R/\ker(\varphi) \xrightarrow{\cong} R'$. ∎

Beispiel 2.14 sei $m \geq 0$, $m\mathbb{Z} \subseteq \mathbb{Z}$ das entspr. Ideal.

$m=0$: $\mathbb{Z} \xrightarrow{\mathrm{id}} \mathbb{Z}$ induz. $\mathbb{Z}/(0) \xrightarrow{\cong} \mathbb{Z}$

$m=1$: $\mathbb{Z}/(1) \xrightarrow{\cong} 0$

$m \geq 2$: $\mathbb{Z}/m\mathbb{Z}$ ring; man kann nachrechnen (siehe aber auch 2.16)

m prim $\Leftrightarrow$ $\mathbb{Z}/m\mathbb{Z}$ Integritätsbereich $\Leftrightarrow$ $\mathbb{Z}/m\mathbb{Z}$ Körper.

Definition 2.15 R ein komm. Ring

1) $\mathfrak{p} \subsetneq R$ Ideal heißt Primideal (prim) falls für $a, b \in R$ mit $ab \in \mathfrak{p}$ gilt, dass $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$.
2) $\mathfrak{m} \subsetneq R$ heißt maximales Ideal falls für jedes Ideal $\mathfrak{a} \subseteq R$ mit $\mathfrak{m} \subseteq \mathfrak{a}$ folgt dann $\mathfrak{m} = \mathfrak{a}$.

Lemma 2.16 Ein R komm. ring.

a) Ein Ideal $\mathfrak{p} \subsetneq R$ ist prim $\Leftrightarrow$ $R/\mathfrak{p}$ ist ein Integritätsbereich

b) Ein Ideal $\mathfrak{m} \subsetneq R$ ist maximal $\Leftrightarrow$ $R/\mathfrak{m}$ ist ein Körper.

Insbesondere sind max. ideale prim (direktes Argument auch möglich)

Für den Beweis bemerken wir zunächst:

- $\varphi: R \to S$ Ringhom., $\mathfrak{a} \subseteq S$ Ideal. $\Rightarrow \varphi^{-1}(\mathfrak{a}) \subseteq R$ Ideal
- $\varphi: R \to S$ surj. Ringhom, $\mathfrak{a} \subseteq R$ Ideal $\Rightarrow \varphi(\mathfrak{a}) \subseteq S$ Ideal.

Beweis (2.16) a) klar nach Definitionen und der Tatsache dass

$\ker(R \to R/\mathfrak{p}) = \mathfrak{p}$.

b) obige Bemerkung zeigt:

$$\left\{\begin{array}{l}\text{Ideale } \mathfrak{b} \subseteq R \\ \text{mit } \mathfrak{a} \subseteq \mathfrak{b}\end{array}\right\} \xrightarrow[\cong]{\pi} \left\{\text{Ideale in } R/\mathfrak{a}\right\} \quad \text{kompatibel mit } "\subseteq"$$

Insbesondere: $\mathfrak{m} \subsetneq R$ max $\Leftrightarrow \{0\} \subseteq R/\mathfrak{m}$ maximal.

ggz: R Körper $\Leftrightarrow \{0\} \subseteq R$ maximal.

"$\Rightarrow$" ✓ "$\Leftarrow$" sei $r \in R \setminus \{0\}$. dann gilt $\{0\} \subsetneq (r)$ und somit aus max. $(r) = R$. Insbesondere $1 \in (r)$ und $r \in R^\times$. ∎

Satz 2.17 (chinesischer Restsatz) Sei R ein komm. ring $\mathfrak{a}_1, \dots, \mathfrak{a}_n \subseteq R$ Ideale: paarweise koprime Ideale (dh. für $i \neq j$ gilt $\mathfrak{a}_i + \mathfrak{a}_j = R$). Die Abbildung

$\varphi: R \longrightarrow R/\mathfrak{a}_1 \times \dots \times R/\mathfrak{a}_n$, $x \mapsto (\pi_1(x), \dots, \pi_n(x))$ ist surjektiv

und $\ker(\varphi) = \bigcap_{i=1}^n \mathfrak{a}_i$. Insbesondere gilt

$$R/\bigcap_{i=1}^n \mathfrak{a}_i \xrightarrow{\cong} \prod_{i=1}^n R/\mathfrak{a}_i.$$

Beweis: die letzten Aussagen sind klar, nur surjektivität ist zu zeigen (klar falls $n=1$.)

seien dafür $x_1, \dots, x_n$ Repräsentanten von Elementen in $R/\mathfrak{a}_1, \dots, R/\mathfrak{a}_n$, $n \geq 2$

da die $\mathfrak{a}_i$'s pw koprim finden wir elemente $a_1^i \in \mathfrak{a}_1$ und $a_i \in \mathfrak{a}_i$ $i \neq 2, \dots, n$ sd. $a_1^i + a_i = 1$. Dann gilt auch

$$1 = \prod_{i=1}^n (a_1^i + a_i) \in \mathfrak{a}_1 + \prod_{i=2}^n \mathfrak{a}_i \Rightarrow \mathfrak{a}_1 \text{ und } \prod_{i=2}^n \mathfrak{a}_i \text{ sind koprim}$$

schreibe also $1 = a + b_1$ mit $a \in \mathfrak{a}_1$, $b \in \prod_{i=2}^n \mathfrak{a}_i \subseteq \mathfrak{a}_j$ für alle $j = 2, \dots, n$, $b \equiv 1 \ (\mathfrak{a}_1)$

mit gleichem argument angewendet auf $\mathfrak{a}_2, \mathfrak{a}_1, \dots, \mathfrak{a}_n$ findet man ein $b_2 \in \prod_{i \neq 2}^n \mathfrak{a}_i$

allgemein b_i mit $b_i \in \prod_{j \neq i} \mathfrak{a}_j$ und $b_i \equiv 1 \bmod \mathfrak{a}_i$. dann betrachte $\sum b_i x_i$. ∎

Primfaktorzerlegungen: $\mathbb{Z}$ hat folgende fundamentale Eigenschaften

a) es gibt Division mit Rest

b) $\mathbb{Z}$ ist Hauptidealring

c) jedes Element ist Produkt von Primzahlen

Gibt es.

Definition 2.18 R Integritätsring. Eine Abbildung $\delta: R \setminus \{0\} \to \mathbb{N}$ sodass gilt: für $f, g \in R$, $g \neq 0$ existieren $q, r \in R$ mit

$$f = q \cdot g + r \quad \text{und} \quad \delta(r) < \delta(g) \text{ oder } r = 0$$

so nennen wir (R, δ) einen euklidischen Ring, δ die Normabb. von R.

Beispiele 2.19 a) K Körper ist euklidischer Ring ($\delta(x) = 1$ für $x \neq 0$)

b) $\mathbb{Z}$ mit $\delta(n) = |n|$.

c) $K[X]$ mit K Körper, $\delta = \text{grad}$ (Satz 2.5)

d) $\mathbb{Z}[i] \subseteq \mathbb{C}$, also $\{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$. $|\cdot| = \sqrt{a^2 + b^2}^2 \in \mathbb{N}$ (ÜA)

Satz 2.20 euklidische Ringe sind Hauptidealringe

Beweis: siehe Bsp. 2.9. b), ersetze grad durch δ. ∎

Definition 2.21 R Integritätsbereich, $0 \neq p \in R \setminus R^\times$.

1) p heißt irreduzibel falls aus $p = xy$ folgt, dass $x \in R^\times$ oder $y \in R^\times$
ist p nicht irreduzibel, so ist es reduzibel

2) p heißt prim falls aus $p \mid xy$ folgt dass $p \mid x$ oder $p \mid y$.
(p ist prim $\Leftrightarrow$ (p) ist ein Primideal).

Bemerkung: in $\mathbb{Z}$ (allgem. in faktoriellen Ringen, siehe Def. 2.25) ist p irreduzibel $\Leftrightarrow$ p prim. Allgemein ist dies aber nicht der Fall

Lemma 2.22 R Integritätsbereich, $0 \neq p \in R \setminus R^\times$.

(a) ist (p) max. ideal $\Rightarrow$ p prim

(b) ist p prim $\Rightarrow$ p ist irreduzibel

(c) ist R Hauptidealring, $p \in R$ irreduzibel $\Rightarrow$ (p) max.
Insbesondere gilt p irred $\Leftrightarrow$ p prim $\Leftrightarrow$ (p) max.

Beweis: a) (p) max $\Rightarrow$ (p) prim (2.16)

b) sei $p = xy$. Da $p \mid xy$ und p prim gilt (oBdA) $p \mid x$.

d.h. $x = pc$ für $c \in R$. $\Rightarrow p = xy = pcy \Rightarrow p(1-cy) = 0$

da $p \neq 0 \Rightarrow 1 - cy = 0$ und damit $y \in R^\times$ $(y^{-1} = c)$.

c) sei sei p irreduzibel. ist $(a) \subseteq R$ Ideal mit $(p) \subseteq (a) \Rightarrow$

$p = ca$ für $c \in R$. da p irreduzibel. ist $c \in R^\times$ $(\Rightarrow (p) = (a))$

oder $a \in R^\times$ (also $(a) = R$). es folgt, dass (p) maximal ist. ∎

Bemerkung

Korollar 2.3 a) primideale in Hauptidealringen sind maximal

b) $\mathbb{Z}/m\mathbb{Z}$ ist Körper $\Leftrightarrow$ m prim

c) R komm. ring sodass $R[X]$ Hauptidealring $\Rightarrow$ R Körper.

Beweis: a), b) ✓

c) $R[X]$ Hauptidealring $\Rightarrow$ R Integritätsbereich. $\Rightarrow (X)$ prim

(denn $R[X]/(X) \cong R$) $\Rightarrow (X)$ maximal $\Rightarrow R$ Körper.

Satz 2.24 R Hauptidealring, $0 \neq a \in R \setminus R^\times$. Dann existieren Primelemente $p_1, \dots, p_n$ sodass $a = p_1 \cdots p_n$. Diese Darstellung ist eindeutig bis auf Reihenfolge und Einheiten.

Beweis: zunächst: sei $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \dots$ eine aufsteigende Kette von Idealen

Dann ist $\mathfrak{a} = \bigcup \mathfrak{a}_i$ wieder ein Ideal. Sei $\mathfrak{a} = (a)$.

da $\mathfrak{a} = \bigcup \mathfrak{a}_i$ gibt es ein $i \geq 1$ sodass $a \in \mathfrak{a}_i$. $\Rightarrow$

$(a) \subseteq \mathfrak{a}_i \subseteq \mathfrak{a} = (a)$ und somit folgt $\mathfrak{a} = \mathfrak{a}_i = \mathfrak{a}_{i+1} = \dots$

(Ringe in denen jede aufsteigende Kette von Idealen stationär wird heißen Noethersch. wir haben gezeigt: Hauptidealringe sind Noethersch.)

Betrachte nun die Menge $S = \{ \mathfrak{a} \subseteq R \text{ Ideal} \mid \mathfrak{a} = (a) \text{ für } a \in R \setminus R^\times$ und a kann nicht als Produkt von Primelementen geschrieben werden $\}$

wir zeigen dass $S = \emptyset$.

angenommen $S \neq \emptyset$. Dann gibt es in S ein maximales Element

(falls $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \dots$ mit $\mathfrak{a}_i \in S \Rightarrow \bigcup \mathfrak{a}_i \in S$)

Sei $0 \neq a \in S$ maximal, $a = (a)$. Es folgt dass a nicht prim und daher nicht irreduzibel (2.22). Wir haben also $a = xy$ mit $0 \neq x, y \in R \setminus R^\times$.

Behauptung (ÜA): $(a) \subsetneq (x)$ analog $(a) \subsetneq (y)$.

also sind $(x), (y) \notin S$ (Maximalität von a)

daher sind x und y produkte von Primelementen daher auch $a = x \cdot y$.

Zur Eindeutigkeit: Sei $p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s$, p_i, q_j prim.

$p_1 \mid q_1 \cdot \ldots \cdot q_s$ und daher (oBdA) $p_1 \mid q_1$. dh. $q_1 = p_1 \cdot b_1$

da q_1 prim $\Rightarrow$ irreduzibel folgt, dass $b_1 \in R^\times$.

$\Rightarrow p_1 \cdot (p_2 \cdot \ldots \cdot p_r) = p_1 \cdot (b_1 q_2 \cdot \ldots \cdot q_s) \Rightarrow p_2 \cdot \ldots \cdot p_r = b_1 q_2 \cdot \ldots \cdot q_s$

Iterativ folgt $r = s$ und die behauptete Eindeutigkeit ∎

Bemerkung: R Hauptidealring, $0 \neq a \in R$. Dann existieren $b \in R^\times$ und $p_1, \ldots, p_n$ prim sodass $a = b p_1 \cdot \ldots \cdot p_n$: ist $a \in R^\times$ so wähle $n = 0$, $b = a$. ist $a \in R \setminus R^\times$ so greift 2.24.

Lemma 2.25: Für einen Integritätsring R sind folgende Bedingungen äquivalent:

a) jedes $0 \neq a \in R \setminus R^\times$ lässt sich als Produkt von Primelementen schreiben

b) jedes $0 \neq a \in R \setminus R^\times$ lässt sich eindeutig bis auf Reihenfolge und Einheiten als Produkt von Primelementen schreiben

c) jedes $0 \neq a \in R \setminus R^\times$ lässt sich eindeutig bis auf Reihenfolge und Einheiten als Produkt von irreduziblen elementen schreiben

Beweis: Der Eindeutigkeitsteil des Beweises von 2.24 zeigt a) $\Rightarrow$ b) und b) $\Rightarrow$ a) ist offenbar. Gilt b) so zeigen wir, dass irreduzible Elemente prim sind, es gilt daher c). Sei also q irreduz. nach b) gilt $q = p_1 \cdot \ldots \cdot p_n$ mit $p_1, \ldots, p_n$ prim. q irreduzibel sagt, dass $n = 1$ gelten muss (Primelemente sind keine Einheiten).

Gilt c) so zeigen wir wieder, dass irreduzible Elemente prim sind, es gilt daher b) sei also q irreduzibel und $q \mid xy$ mit $x, y \in R$

wir müssen zeigen dass $q \mid x$ oder $q \mid y$ gilt. Falls x oder $y \in R^\times$ ist dies klar. nehmen wir also an dass $xy \in R - R^\times$.

nach c) können wir schreiben $x = x_1 \cdots x_n$, $y = y_1 \cdots y_m$ mit x_i, y_j irred.

Dann gilt $q \mid x_1 \cdots x_n \cdot y_1 \cdots y_m$.

Wegen der Eindeutigkeit der Zerlegung von $x \cdot y$ in irred. Elemente (bis auf Reihenfolge und Einheiten) folgt, dass $q = \varepsilon x_i$ oder $q = \varepsilon y_j$ für $\varepsilon \in R^\times$ und $i \in \{1, \dots, n\}$, $j \in \{1, \dots, m\}$. Daher teilt q x oder y ∎

Definition 2.26 Ein Integritätsbereich der eine der äquiv. Bedingungen von 2.25 erfüllt heißt **faktoriell**.

wir haben also

$$R \text{ euklidisch} \overset{2.20}{\Longrightarrow} R \text{ Hauptidealring} \overset{2.24}{\Longrightarrow} R \text{ faktoriell}$$

Beispiele 2.27 a) wir zeigen später: R faktoriell $\iff R[X]$ faktoriell

also ist $\mathbb{Z}[X]$ faktoriell aber kein Hauptidealring. (2.23 c)).

b) sei $0,1 \neq d \in \mathbb{Z}$ quadratfrei ($\forall n \geq 1 : n^2 \nmid d$).

$R_d = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ Unterring

- für $d = -1$ ist $R_d = \mathbb{Z}[i]$ euklidisch (2.19 d))
- für $d = \pm 5$ ist R_d Integritätsbereich, aber nicht faktoriell:

  man zeigt dass $2, 3, 1+\sqrt{-5}$ und $1-\sqrt{-5}$ irreduzibel sind.

  aber $2 \cdot 3 = 6 = (1+\sqrt{-5})(1-\sqrt{-5})$ es gibt also keine eindeutige Zerlegung in irreduzible Elemente

c) (Fakt) $\theta = \frac{1+\sqrt{-19}}{2} \in \mathbb{C} \rightsquigarrow \{a + b\theta \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ ist Hauptidealring aber nicht euklidisch.

Notation: R faktoriell. $P \subseteq R$ Vertretersystem der Primelemente (betrachte alle Primideale, welche Hauptideale sind, und wähle für jeden ein Primelement welches das Ideal erzeugt).

für $0 \neq a \in R$ gilt dann $a = \varepsilon \cdot \prod_{p \in P} p^{v_p(a)}$ für eindeutige $\varepsilon \in R^\times$ und $v_p(a) \in \mathbb{N}$

es gelten dann $v_p(a \cdot b) = v_p(a) + v_p(b)$ und $v_p(a) = 0 \ \forall p \in P \Leftrightarrow a \in R^\times$.

Sei nun R Integritätsbereich, $\{x_1, \dots, x_n\} \subseteq R$ endl. Teilmenge.
Wir nennen $d \in R$ einen größten gemeinsamen Teiler (schreiben $d \in ggT(x_i)$)
falls gilt: a) $d \mid x_i \ \forall i = 1, \dots, n$
b) ist $e \in R$ mit $e \mid x_i \ \forall i = 1, \dots, n \Rightarrow e \mid d$.

Wir nennen $v \in R$ ein kleinstes gemeinsames Vielfaches ($v \in kgV(x_1, \dots, x_n)$)
falls gilt: a) $x_i \mid v \quad \forall i = 1, \dots, n$
b) ist $w \in R$ mit $x_i \mid w \ \forall i = 1, \dots, n \Rightarrow v \mid w$

Falls sie existieren sind ggT's und kgV's eindeutig bis auf Einheiten.

Bemerkungen • ist $(x_1, \dots, x_n) = (d) \Rightarrow d \in ggT$, analog
ist $(x_1) \cap \dots \cap (x_n) = (v) \Rightarrow v \in kgV$.
es gilt aber nicht, dass $d \in ggT(x_1, \dots, x_n) \Rightarrow (x_1, \dots, x_n) = (d)$.

• ist R faktoriell, $x_i \in R$ mit $x_i = \varepsilon_i \cdot \prod_{p \in P} p^{v_p(x_i)}$, $i = 1, \dots, n$

so gilt $\prod_{p \in P} p^{\min\{v_p(x_1), \dots, v_p(x_n)\}} \in ggT(x_1, \dots, x_n)$ und

$\prod_{p \in P} p^{\max\{v_p(x_1), \dots, v_p(x_n)\}} \in kgV(x_1, \dots, x_n)$.

Nullstellen von Polynomen

Ist $K \subseteq L$ eine Körpererweiterung (Ringerw. mit K, L Körper) so haben wir $K[X] \subseteq L[X]$ der Unterring der Polynome deren Koeff in K liegen.
Für $f \in K[X]$ sagen wir dass $\alpha \in L$ eine Nullstelle von f in L ist
falls $g \in L[X]$ existiert sodass $f = (X - \alpha) g$ ($(X-\alpha) \mid f$).
Wir sagen, dass α Vielfachheit $r \geq 1$ hat, falls
$f = (X-\alpha)^r \cdot g$ und $(X-\alpha) \nmid g$.
Ist α Nullstelle von f, so schreiben wir auch $f(\alpha) = 0$.

Lemma 2.28 Sei K Körper, $f \in K[X]$ mit $\operatorname{grad}(f) = n \geq 0$.
Dann hat f höchstens n Nullstellen (mit Vielfachheiten gezählt)
und genau n Nullstellen gelte f in $K[X]$ in Linearfaktoren
zerfällt, d.h. wenn $f = \prod_{i=1}^{n} (X - \alpha_i)$ $\alpha_i \in K$ gilt.

Beweis: ist α ein Nullstelle von f, so gilt $f = (X-\alpha) \cdot g$
und daher $\operatorname{grad}(g) = \operatorname{grad}(f) - 1$. (siehe 2.4, da K Integritätsbereich)
f hat also höchstens n Nullstellen. Hat es n NS so zerfällt
f wie angedeutet ($\prod_{i=1}^{n}(X-\alpha_i)$ teilt f und beide Seiten haben den
gleichen grad). Offenbar hat $\prod_{i=1}^{n}(X-\alpha_i)$ auch n Nullstellen ∎

Sei K Körper, $f = \sum_{i=0}^{n} a_i X^i \in K[X]$. Wir schreiben

$$df = f' = \sum_{i=0}^{n} i a_i X^{i-1} \in K[X]$$ für die formale Ableitung

von f. Dann ist $d: K[X] \to K[X]$ K-linear und
$d(f \cdot g) = df \cdot g + f \cdot dg$

Lemma 2.29 Sei $0 \neq f \in K[X]$. $\alpha \in K$ ist eine mehrfache
Nullstelle von $f \Leftrightarrow f(\alpha) = 0 = f'(\alpha)$

Beweis: α ist Nullstelle $\Leftrightarrow f(\alpha) = 0$. ist α eine Nullstelle, so ist
sie ist r-fach
mehrfach $\Leftrightarrow f = (X-\alpha)^r \cdot g$ mit $r \geq 2$ und $(X-\alpha) \nmid g$. (d.h. $g(\alpha) \neq 0$)
$f' = r \cdot (X-\alpha)^{r-1} \cdot g + (X-\alpha)^r dg$ zeigt, dass $f'(\alpha) = 0 \Leftrightarrow r \geq 2$. ∎

Konstruktion (der Quotientenkörper) Sei R ein Integritätsbereich.
Betrachte $M = R \times (R \setminus \{0\})$ und die Äquivalenzrelation

$$(a,b) \sim (a',b') \Leftrightarrow ab' = ba'$$

die Menge der Äquivalenzklassen schreiben wir $Q(R)$ oder $\operatorname{Frac}(R)$
und $\frac{a}{b}$ für $[(a,b)]$. Die üblichen "Bruchrechenregeln"

$$\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'} \quad \text{und} \quad \frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'}$$

definieren eine Ringstruktur auf $Q(R)$ sodass $R \to Q(R), a \mapsto \frac{a}{1}$ eine Ringhom. ist. Außerdem ist $Q(R)$ ein Körper.

Bemerkung Sei R ein komm. ring, $S \subseteq R$ eine Teilmenge.
$R \to S^{-1}R$ ist eine Ringabb. mit folgender univ. Eigenschaft:
Sei $f: R \to R'$ ein Ringhom. sodass $\forall s \in S$ gilt, dass $f(s) \in R'^{\times}$.
Dann existiert eine eindeutige Ringabbildung $\overline{f}: S^{-1}R \to R'$ sodass

$$\begin{array}{ccc} R & \xrightarrow{f} & R' \\ \downarrow & \nearrow_{\overline{f}} & \\ S^{-1}R & & \end{array}$$

kommutiert.

ÜA: 1) Zeigen Sie, dass $S^{-1}R \leftarrow R$ exakt

Hinweis: Zeigen Sie, dass man annehmen kann, dass $S \subseteq R$ ein Untermonoid von $(R, \cdot, 1)$ ist und adaptieren Sie die obige Konstruktion auf $R \times S$ geeignet

2) Zeigen Sie, dass $Q(R) = (R \setminus \{0\})^{-1}R$.

3) Zeigen Sie, dass für eine Integritätsbereich R, $R \to Q(R)$ injektiv ist, aber allgemein $R \to S^{-1}R$ nicht injektiv sein muss.

4) Ist $p \subseteq R$ prim, so ist $R \setminus p \subseteq R$ ein Untermonoid von $(R, \cdot, 1)$

Beispiele 2.30 a) $R = \mathbb{Z} \rightsquigarrow Q(R) \cong \mathbb{Q}$, $\{n\}^{-1}\mathbb{Z} = \mathbb{Z}[\frac{1}{n}] \subseteq \mathbb{Q}$.

b) $R = \mathbb{Z}[i] \rightsquigarrow Q(R) \cong \mathbb{Q}[i]$

c) [Notation] $R = K[X]$, $Q(R) = K(X)$ "Ring der rationalen Funktionen".

Lemma 2.31 Sei R ein faktorieller Ring und P ein Vertretersystem der Primelemente in R. Jedes $0 \neq x = \frac{a}{b} \in Q(R)$ hat eine bis auf Reihenfolge eindeutige Darstellung als Produkt

$$x = \varepsilon \cdot \prod_{p \in P} p^{v_p(x)} \quad \text{mit } \varepsilon \in R^{\times},\ v_p(x) \in \mathbb{Z} \text{ und } v_p(x) = 0 \text{ für fast alle } p \in P$$

außerdem gilt $x \in R \Leftrightarrow v_p(x) \geq 0 \ \forall p \in P$

und wir setzen $\forall p \in P \ v_p(0) = \infty$.

Beweis: Schreibe $0 \neq x = \frac{a}{b}$, $a,b \in R \setminus \{0\}$, nach Notation nach 2.27 können wir schreiben $a = \varepsilon_a \prod_{p \in P} p^{\nu_p(a)}$ (eindeutig bis auf ...)

und $b = \varepsilon_b \prod_{p \in P} p^{\nu_p(b)}$. Dann gilt $x = \frac{\varepsilon_a}{\varepsilon_b} \cdot \prod_{p \in P} p^{\nu_p(a) - \nu_p(b)}$

die Eindeutigkeit folgt aus den Eigenschaften der Primzerlegung von a und b. ∎

Sei nun R faktoriell, P ein Vertretersystem der Primelemente in R und $f \in Q(R)[X]$ ein Polynom. Die nicht-trivialen Koeff. von f sind von der Form $0 \neq c = \frac{a}{b} \in Q(R)$, $a,b \in R \setminus \{0\}$.

Wir haben dann $\nu_p(c) = \nu_p(a) - \nu_p(b) \in \mathbb{Z}$ für jedes $p \in P$. (und $\nu_p(0) = \infty$). Betrachte

$$\nu_p(f) = \min \{ \nu_p(f(i)) \mid i \geq 0 \}$$

Erinnerung: $f = \sum_{i \geq 0} f(i) X^i$, $f(i) \in Q(R)$

Es gelten daher:

1) $f = 0 \iff \nu_p(f) = \infty \quad \forall p \in P$
2) $f \in R[X] \iff \nu_p(f) \geq 0 \quad \forall p \in P$

Ein Polynom $f \in R[X]$ heißt primitiv falls der größte gemeinsame Teiler aller Koeffizienten 1 ist ($\iff$ falls $\nu_p(f) = 0 \ \forall p \in P$)

zum Beispiel sind normierte Polynome, oder Polynome mit 1 als irgendeinem Koeffizienten primitiv.

Bemerkung: Sei $0 \neq f \in Q(R)[X]$ so ist $f = a \cdot \bar{f}$ mit $a \in Q(R)^\times$ und $\bar{f}$ primitiv. (und daher in $R[X]$): dann setze $a = \prod_{p \in P} p^{\nu_p(f)}$

und betrachte $\bar{f} = a^{-1} \cdot f$

Konkret multipliziert man Nenner der Koeff. so aus, dass sich ~~eine Konstante~~ ergibt. der ggT der Koeff. 1 wird.

Bsp: • $f = \frac{1}{2}X^2 + \frac{1}{4}X + 4 \in Q[X] \rightsquigarrow f = \frac{1}{4} \cdot (2X^2 + X + 16)$, $(2X^2 + X + 16) \in \mathbb{Z}[X]$ + primitiv

• $f = \frac{1}{2}X + \frac{1}{3} \in Q[X] \rightsquigarrow f = \frac{1}{6}(3X + 2)$

Lemma 2.32 (Lemma von Gauß) R faktoriell und $p \in R$ prim.
Dann gilt für $f, g \in Q(R)[X]$, dass $v_p(fg) = v_p(f) + v_p(g)$

Beweis: für $f=0$ oder $g=0$ ist die Beh. klar $(\infty - \infty)$.
seien also $fg \neq 0$. schreibe $f = a \cdot \bar{f}$, $g = b \cdot \bar{g}$, $a,b \in Q(R)^\times$, $\bar{f}, \bar{g} \in R[X]$ primitiv. Dann gilt

$$v_p(f \cdot g) = v_p((ab) \cdot (\bar{f}\bar{g})) = v_p(ab) + v_p(\bar{f}\bar{g})$$

(direkt rechnen)

$$= v_p(a) + v_p(b) + v_p(\bar{f}\bar{g}).$$

es genügt also zz. dass $v_p(f \cdot g) = v_p(f) + v_p(g)$ für $f, g \in R[X]$ primitiv.
Da $v_p(\bar{f}) = 0 = v_p(g)$ müssen wir zeigen, dass $v_p(f \cdot g) = 0$, mit anderen Worten, dass es einen Koeffizienten von $f \cdot g$ gibt, welcher nicht von p geteilt wird.
Betrachte den Ringhom. $R[X] \xrightarrow{\pi} R/(p)[X]$ dessen Kern genau die Polynome $h \in R[X]$ sind, sodass $p \nmid h_i$.
wir wollen also zeigen, dass $\pi(fg) \neq 0$.
es gilt $\pi(fg) = \pi(f) \cdot \pi(g)$. Da $v_p(f) = 0 = v_p(g)$ folgt, dass $\pi(f) \neq 0 \neq \pi(g)$. Da p prim $\Rightarrow R/(p)$ Integritätsbereich und damit, dass $\pi(fg) \neq 0$. ∎

Bemerkung: ist R faktoriell, $f, g \in Q(R)[X]$ normiert und $fg \in R[X]$ so
folgt $f, g \in R[X] \Rightarrow 0 = v_p(fg) = v_p(f) + v_p(g)$ ~~⇒~~ da $v_p(f), v_p(g) \geq 0$ da normiert
folgt $v_p(f) = 0 = v_p(g)$

Beispiel: $f \in \mathbb{Z}[X]$ normiert, $\alpha \in \mathbb{Q}$ eine Nullstelle. Dann gilt
$f = (X - \alpha) \cdot g$ und $g \in \mathbb{Q}[X]$ normiert. Nach der Bemerkung folgt dass $(X-\alpha)$ und $g \in \mathbb{Z}[X]$. (und damit $\alpha \in \mathbb{Z}$).
es folgt dass viele Polynome keine rationalen Nullstellen haben
zB $X^3 - X^2 + 5$ (ist α NS so gilt $\alpha \mid 5 \Rightarrow \alpha \in \{\pm 1, \pm 5\}$).

Satz 2.33 (Gauß) Sei R faktoriell. Dann ist $R[X]$ faktoriell.
Des weiteren ist $q \in R[X]$ prim genau dann, wenn

a) q ist Primelement von R, oder

b) q ist primitiv in $R[X]$ und prim in $Q(R)[X]$.

Insbesondere ist ein primitives Polynom $q \in R[X]$ irreduzibel $\Leftrightarrow$ $q \in Q(R)[X]$ irreduzibel ist.

Beweis: Zuerst zeigen wir, dass die Elemente wie in a) und b) prim sind. Sei also $q \in R$ prim und teile q das Produkt fg:
wir erinnern, dass $q \mid h \Leftrightarrow [h] = 0$ in $R/(q)[X] \leftarrow R[X]$
wir haben also $0 = \bar{\pi}(f \cdot g) = \bar{\pi}(f) \cdot \bar{\pi}(g)$. Da q prim ist $R/(q)$ Integritätsbereich und somit auch $R/(q)[X]$ - es folgt, dass $\bar{\pi}(f) = 0$ oder $\bar{\pi}(g) = 0$, also ist q prim in $R[X]$.
Sei nun q primitiv in $R[X]$ und prim in $Q(R)[X]$. und gelte $q \mid fg$ in $R[X]$. es folgt, dass (OBdA) $q \mid f$ in $Q(R)[X]$, dh.
$f = q \cdot h$ für ein $h \in Q(R)[X]$. zeigen wir, dass $h \in R[X]$ so sind wir fertig. Nach dem Gauß Lemma gilt $\forall p \in R$ prim

$$0 \leq v_p(f) = v_p(q) + v_p(h) = v_p(h) \quad (\text{da } v_p(q) = 0 \text{ da } q \text{ primitiv})$$

Wir zeigen nun: Jedes element $0 \neq f \in R[X] \setminus R[X]^\times$ ist Produkt von elementen wie in a) oder b). es folgt (IA) dass R faktoriell ist. und dann, dass jedes primelement eine in a) oder b) ist.
(Primelemente sind irreduzibel, da $R[X]$ integritätsbereich).

Sei also $0 \neq f \in R[X] \setminus R[X]^\times$. Sei $a = ggT(\{f(i)\}_{i \geq 0})$
dann gilt $f = a \cdot \tilde{f}$ und $\tilde{f}$ ist primitiv
Da $a = q_1 \cdot \ldots \cdot q_r$ mit $q_i \in R$ prim (und daher auch in $R[X]$ prim) genügt es anzunehmen, dass f primitiv ist.
sei also $f = c \cdot f_1 \cdot \ldots \cdot f_n$ mit $c \in Q(R)^\times$, $f_1, \ldots, f_n \in Q(R)[X]$ prim
(dies existiert da $Q(R)[X]$ faktoriell, sogar Hauptidealring, ist).

Schreibe $f_i = a_i \bar{f}_i$ mit $a_i \in Q(R)^\times$, $\bar{f}_i$ primitiv (und immernoch prim in $Q(R)[X]$)

$\Rightarrow f = c' \cdot \bar{f}_1 \cdot \ldots \cdot \bar{f}_n$ mit $c' = c \cdot a_1 \cdot \ldots \cdot a_n \in Q(R)^\times$

Wir zeigen nun $c' \bar{f}_1 \in R[X]$ und primitiv. (und immernoch prim in $Q(R)[X]$)

dann ist $f = (c'\bar{f}_1) \cdot \bar{f}_2 \cdot \ldots \cdot \bar{f}_n$ die gewünschte Darstellung.

sei also $p \in R$ prim. Es gilt

$$v_p(f) = v_p(c') + v_p(\bar{f}_1) + \ldots + v_p(\bar{f}_n) \qquad v_p(\bar{f}_i) = 0 \text{ da } \bar{f}_i \text{ primitiv}$$

$$\Rightarrow \quad 0 = v_p(c') \qquad v_p(f) = 0$$

also gilt $c' \in R \subseteq Q(R)$. außerdem gilt

$v_p(c'\bar{f}_1) = v_p(c') + v_p(\bar{f}_1) = 0$ und somit $c'\bar{f}_1$ primitiv ∎

Irreduzibilitätskriterien

Sei K ein Körper und $f \in K[X]$, $K[X]^\times$ so wollen wir untersuchen, wann f reduzibel ist, also wann aus $f = gh$ folgt, dass $g \in K^\times$ oder $h \in K^\times$.

- ist $\operatorname{grad}(f) = 1$, so folgte $\operatorname{grad}(g) = 0$ oder $\operatorname{grad}(h) = 0$ und somit ist f irreduzibel.
- ist $\operatorname{grad}(f) \geq 2$ und α eine Nullstelle von f so gilt $f = (X - \alpha) \cdot g$ und $\operatorname{grad}(g) \geq 1 \Rightarrow f$ ist reduzibel.

Ü.A.: es gibt reduzible Polynome in $\mathbb{R}[X]$ ohne Nullstellen (in $\mathbb{R}$).

Ist R faktoriell $K = Q(R)$ und $0 \neq f \in K[X]$ so gibt es $c \in K^\times$, $\bar{f} \in R[X]$ mit $\bar{f}$ primitiv (Bem. 5.28) und f ist irreduzibel $\Leftrightarrow \bar{f}$ ist irreduzibel und $\bar{f}$ reduzibel in $K[X] \overset{\text{Satz von Gauß}}{\Leftrightarrow} \bar{f}$ reduzibel in $R[X]$. also:

$f \in K[X]$ irreduzibel $\Leftrightarrow \bar{f} \in K[X]$ irreduzibel $(=) \bar{f} \in R[X]$ irreduzibel.

Satz 2.34 (Eisenstein) Sei R faktoriell, $f = \sum_{i=0}^{n} a_i X^i \in R[X]$ primitiv von grad $n > 0$ und $p \in R$ prim sodass $p \mid a_i$ für $i < n$ und $p \nmid a_n$. Dann gilt

$p^2 \nmid a_0 \Rightarrow f$ ist irreduzibel in $R[X]$ (und daher auch in $Q(R)[X]$).

Beweis: Wir zeigen die Kontraposition. Sei also $f = g \cdot h$ mit $g, h \in R[X] \setminus R[X]^\times$. Zunächst sehen wir, dass $\operatorname{grad}(g) > 0$: Sonst existiert $q \in R$ prim sodass $q \mid f$, es folgt dass f nicht primitiv ist. analog gilt $\operatorname{grad}(h) > 0$.

Betrachte nun die Abbildung $\pi: R[X] \longrightarrow Q(R/(p))[X]$ induziert von den kan. Abbildungen $R \twoheadrightarrow R/(p) \hookrightarrow Q(R/(p))$.

Wir bekommen $\pi(f) = \pi(g) \cdot \pi(h)$.

und $\pi(f) = a_n \cdot X^n$. aus der Eindeutigkeit der Primzerlegung in $Q(R/(p))[X]$ folgt, dass $\pi(g) = \varepsilon_g \cdot X^k$ und $\pi(h) = \varepsilon_h \cdot X^\ell$, $\varepsilon_g, \varepsilon_h \in Q(R/(p))$ und $k + \ell = n$. es folgt, dass $k = \operatorname{grad}(g)$ und $\ell = \operatorname{grad}(h)$, dann

$n = \operatorname{grad}(g) + \operatorname{grad}(h) \geq k + \ell = n$.

man hat also, dass $g(0) \in \ker(R \twoheadrightarrow R/(p) \hookrightarrow Q(R/(p))) = (p)$

und analog, dass $h(0) \in (p) \Rightarrow p \mid g(0)$ und $p \mid h(0)$

$\Rightarrow p^2 \mid g(0) \cdot h(0) = f(0) = a_0$ ∎

Satz 2.35 (Reduktion mod p) Sei R faktoriell, $f = \sum_{i=0}^{n} a_i X^i \in R[X]$ ($\operatorname{grad}(f) = n$), $p \neq R$ prim und $p \nmid a_n$. Sei $\pi: R[X] \to R/(p)[X]$ die Projektion. Dann gilt:

Ist $\pi(f) \in R/(p)[X]$ irreduzibel, so ist $f \in Q(R)[X]$ irreduzibel.

Ist f zusätzlich primitiv, so ist $f \in R[X]$ irreduzibel.

Beweis: $f \in Q(R)[X]$ irreduzibel $\Leftrightarrow \overline{f} \in Q(R)[X]$ irreduzibel (R. 4.3) wobei $\overline{f} = a \cdot f$ mit $a \in R$, $\overline{f} \in R[X]$ primitiv und $p \nmid \frac{a_n}{a}$ (Leitkoeff. von $\overline{f}$) ($\frac{a_n}{a} \mid a_n$)

es genügt also denn Fall zu betrachten, wo f primitiv ist. Wir zeigen wieder die Kontraposition, nehmen also an, dass f in $R[X]$ reduzibel ist.

Schreibe $f = g \cdot h$, da f primitiv folgt $\operatorname{grad}(g), \operatorname{grad}(h) > 0$.

Dann gilt $\pi(f) = \pi(g) \cdot \pi(h)$ und wie in letztem Beweis gilt

$\operatorname{grad}(\pi(g)) = \operatorname{grad}(g)$ und $\operatorname{grad}(\pi(h)) = \operatorname{grad}(h)$ (da $\operatorname{grad}(\pi(-)) \geq \operatorname{grad}(-)$ und $\operatorname{grad}(\pi f) = \operatorname{grad}(f)$)

$\Rightarrow \pi(f)$ ist reduzibel in $R/(p)[X]$.

Beispiele 2.36 a) $X^n - p \in \mathbb{Z}[X]$, p prim, $n \geq 2$:

Eisenstein $\Rightarrow$ $X^n - p$ irred. in $\mathbb{Q}[X]$ und $\mathbb{Z}[X]$

hat daher keine Nullstellen $\Rightarrow \sqrt[n]{p} \notin \mathbb{Q}$.

b) $P = X^n + Y^n - 1 \in \mathbb{Z}[X,Y] = \mathbb{Z}[X][Y]$:

$P = Y^n + (X-1)(X^{n-1} + \dots + X + 1)$ normiert, $(X-1) \in \mathbb{Z}[X]$ prim

$(X-1) \nmid X^n + \dots + X + 1$ $\left(\mathbb{Z} \cong \mathbb{Z}[X]/(X-1) \leftarrow \mathbb{Z}[X] \right.$

$1 \longleftrightarrow X$

$0 \neq n \longleftrightarrow X^{n-1} + \dots + X + 1$ $\left. \right)$

Eisenstein $\Rightarrow$ P irreduzibel

c) $P = 3X^2 + 5X + 9 \in \mathbb{Z}[X]$ primitiv, Bild in $\mathbb{F}_2[X]$ ist $X^2 + X + 1$ was irreduzibel ist (von Hand überprüfen)

2.35 $\Rightarrow$ P irreduz. in $\mathbb{Z}[X]$ und $\mathbb{Q}[X]$. ∎