3. Ringe

3.1 Ringe und Ideale

3.1.1 Def Eine Menge R mit einer Verknüpfung $+: R \times R \to R$ und $\cdot : R \times R \to R$, $(R, +, \cdot)$, heißt (kommutativer) Ring (mit 1), falls

1) $(R, +)$ eine abelsche Gruppe ist (mit Neutralem 0)
2) $(R, \cdot)$ ein kommutatives Monoid ist (mit Neutralem 1)
3) (Distributivität) $\forall a, b, c \in R$:
$a \cdot (b + c) = a \cdot b + a \cdot c$.

Bsp

1) $\mathbb{Z}$
2) $\mathbb{Z}_n$. Wir haben bisher die abelsche Gruppe $(\mathbb{Z}_n, +)$ betrachtet.
Wir definieren zusätzlich
$\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$: $[a] \cdot [b] = [a \cdot b]$.

Dies ist wohldefiniert:
Sei $[a'] = [a]$, $[b'] = [b]$ $\Rightarrow$
$a - a' = k \cdot n$, $b - b' = l \cdot n$ für $k, l \in \mathbb{Z}$

$\Rightarrow$
$[a' \cdot b'] = [(a-kn)(b-ln)] =$
$[ab + n(-kb - al + kln)] = [ab]$.

Wegen der Eigenschaften der Multiplikation auf $\mathbb{Z}$ ist die Operation assoziativ und kommutativ, und $[1]$ ist Neutrales.

Die Distributivität wird auch von $\mathbb{Z}$ vererbt.

3) Jeder Körper ist ein Ring.
4) Sei K ein Körper, der Polynomring $K[x]$ ist ein Ring.

3.1.2 Lemma (Einfache Rechenregeln)

Sei R ein Ring, $x, y, z \in R$. Dann gilt:

1) $-(-x) = x$
2) $-(x+y) = -x + (-y) = -x - y$
3) $x + y = z \Leftrightarrow x = z - y$

4) $x \cdot 0 = 0 \cdot x = 0$

5) $(-x) \cdot y = x \cdot (-y) = -xy$

6) $(-x) \cdot (-y) = xy$

7) $x(y-z) = xy - xz$

8) $(-1) \cdot x = -x$.

<u>Beweis</u>:

1), 2) haben wir in 2.1.5 3) für beliebige Gruppen gezeigt (hier nur in der Schreibweise +).

3) „$\Rightarrow$" Addiere $-y$ auf beiden Seiten

„$\Leftarrow$" Addiere y "

„Kürzungsregel"

4) $0 \cdot x = (0+0) \cdot x = 0 \cdot x + 0 \cdot x \Rightarrow$

$0 \cdot x = 0$ wegen der Kürzungsregel.

5) $xy + (-x) \cdot y = (x-x) \cdot y = 0 \cdot y = 0$

$\Rightarrow -xy = (-x) \cdot y$

Genauso für $x \cdot (-y)$.

6) $(-x)\cdot(-y) \overset{5)}{=} -(x\cdot(-y)) \overset{5)}{=} -(-xy)$

$\overset{1)}{=} xy$

7) $x(y-z) = x(y+(-z)) = xy + x(-z)$

$= xy + (-xz) = xy - xz$

8) $0 = 0\cdot x = (-1+1)\cdot x = (-1)\cdot x + x$

$\Rightarrow (-1)\cdot x = -x.$ $\square$

<u>3.1.3 Def</u> Sei R ein Ring.

$a \in R$ heißt <u>Einheit</u>, falls $\exists\, b \in R$:

$ab = 1$.

$(R^*, \cdot)$ ist die <u>Einheitengruppe</u>.

a heißt <u>Nullteiler</u>, falls $\exists\, b \neq 0$, $b \in R$: $ab = 0$.

Bsp

1) Sei K ein Körper. $K^* = K \setminus \{0\}$.
K hat keine Nullteiler außer 0.

2) $\mathbb{Z}^* = \{\pm 1\}$. $\mathbb{Z}$ hat keine Nullteiler außer 0.

3) $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$
2 und 3 sind Nullteiler, da $2 \cdot 3 = 6 = 0$
4 ist Nullteiler, da $3 \cdot 4 = 12 = 0$
$\mathbb{Z}_6^* = \{1, 5\}$, denn $1 \cdot 1 = 1$ und $5 \cdot 5 = 25 = 1$.
$\Rightarrow \mathbb{Z}_6 = \{\text{Nullteiler}\} \cup \{\text{Einheiten}\}$

4) In $K[x]$ gibt es keine Nullteiler außer 0.
$(K[x])^* = K^*$

3.1.4 Def Sei $\emptyset \neq U \subset R$, so daß U mit der Einschränkung von $+$ und $\cdot$ wieder ein Ring ist (nicht notwendig mit 1), dann ist U ein Unterring.

Bsp $2\mathbb{Z} \subset \mathbb{Z}$ ist ein Unterring (ohne 1).

3.1.5 Def Seien R, S Ringe.
$\varphi: R \to S$ heißt <u>Ringhomomorphismus</u>
$\Leftrightarrow$ $\varphi(a+b) = \varphi(a) + \varphi(b)$
$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ $\forall a, b \in R$.
Sind R und S Ringe mit 1, so verlangen wir außerdem $\varphi(1_R) = 1_S$.

Bem Bild und Kern von Ringhomomorphismen sind Unterringe (siehe 2.1.14 für Gruppen).

3.1.6 Def Sei R ein kommutativer Ring mit 1. Ein <u>Ideal</u> $I \subset R$ ist eine nicht-leere Teilmenge mit
$a + b \in I$, $r \cdot a \in I$
$\forall a, b \in I$, $r \in R$.

3.1.7 Lemma Ein Ideal ist eine Untergruppe bez $+$.

<u>Beweis:</u>
Da $r \cdot a \in I$ $\forall r \in R$, $a \in I$
folgt $(-1) \cdot a = -a \in I$ $\forall a \in I$.

Damit erfüllt I das Untergruppen-kriterium bez $+$. $\square$

<u>Bemerkung:</u> Wegen Lemma 3.1.6, und da die Addition in R abelsch ist, ist $(R/I, +)$ abelsche Gruppe mit $[0] = 0 + I$ als Neutralem.
Die Def eines Ideals ist so gewählt, daß auch die Mult nach R/I vererbt wird:

<u>3.1.8 Satz</u> (Quotientenring / Faktorring)
Sei R ein Ring, I ein Ideal.
Dann ist R/I mit den repräsentantenweise definierten Operationen ein Ring mit $[1] = 1 + I$ als Neutralem bez. $\cdot$, der <u>Quotientenring/ Faktorring</u>.

<u>Beweis:</u>
Betrachte $[r_1] = [r_1'], \ [r_2] = [r_2']$ in R/I, dann ist $r_1' = r_1 + a$, $r_2' = r_2 + b$ mit $a, b \in I \Longrightarrow$

$$[r_1' \cdot r_2'] = [(r_1 + a)(r_2 + b)] =$$

$$[r_1 r_2 + \underbrace{r_1 b}_{\in I} + \underbrace{r_2 a}_{\in I} + \underbrace{ab}_{\in I}]$$

$$= [r_1 r_2].$$

Damit ist die Multiplikation wohldefiniert. Die weiteren Eigenschaften werden vererbt. $\square$

<u>3.1.9 Lemma</u>: Seien R, S Ringe, $\varphi: R \to S$ ein Ringhomomorphismus. Dann ist $\mathrm{Ker}(\varphi)$ ein Ideal.

<u>Beweis</u>: Seien $a, b \in \mathrm{Ker}(\varphi) \Rightarrow$

$\varphi(a+b) = \varphi(a) + \varphi(b) = 0 + 0 = 0 \Rightarrow$

$a + b \in \mathrm{Ker}(\varphi)$. Sei $r \in R \Rightarrow$

$\varphi(r \cdot a) = \varphi(r) \cdot \varphi(a) = \varphi(r) \cdot 0 = 0$

$\Rightarrow r \cdot a \in \mathrm{Ker}(\varphi)$. $\square$

<u>3.1.10 Satz</u> (Homomorphiesatz)

Seien R, S Ringe, $\varphi: R \to S$ ein Ringhomomorphismus.

Dann ist $R/\mathrm{Ker}\,\varphi \cong \mathrm{Im}\,\varphi$.

<u>Beweis</u>: Aus dem Homomorphiesatz für Gruppen 2.2.6 folgt, daß

es einen Isomorphismus $\tilde{\varphi}: R/_{\mathrm{Ker}(\varphi)} \to \mathrm{Im}\,\varphi$ der additiven Gruppen gibt.

Dieser ist Ringhomomorphismus, denn

$$\tilde{\varphi}([r_1]\cdot[r_2]) = \varphi(r_1\cdot r_2) =$$

$$\varphi(r_1)\cdot\varphi(r_2) = \tilde{\varphi}([r_1])\cdot\tilde{\varphi}([r_2]).$$

$\square$

3.1.11 Def Sei R ein Ring, $A \subset R$.

$$\langle A\rangle := \bigcap_{\substack{A\subset I\subset R\\ I \text{ Ideal}}} I$$

heißt das von A erzeugte Ideal.

3.1.12 Lemma

$$\langle a_1,\dots,a_n\rangle = \left\{\sum_{i=1}^{n} r_i a_i \mid r_i\in R\right\}$$

Beweis Übung.

Bemerkung: Lemma 3.1.12 gilt analog für $\langle A\rangle$, $|A|=\infty$, dann läßt man rechts nur endliche Summen zu.

Bsp $\langle 1\rangle = R$.

3.2 Der Polynomring

3.2.1 Def Sei R ein Ring. Der Polynomring $R[x]$ ist definiert als

$$R[x] = \{ a_0 + a_1 x + \dots + a_n x^n, \ a_i \in R, \ n \in \mathbb{N} \}$$

Wir definieren für

$$f = \sum_{k=0}^{n} a_k x^k \quad \text{und} \quad g = \sum_{k=0}^{m} b_k x^k \in R[x]$$

die Summe

$$f + g = \sum_{k=0}^{m+n} (a_k + b_k) \, x^k ,$$

wobei wir die Konvention verwenden, daß $a_k = 0$ für $k > n$ und $b_k = 0$ für $k > m$,

und das Produkt

$$f \cdot g = \sum_{k=0}^{m+n} \left(\sum_{i=0}^{k} a_i \, b_{k-i} \right) x^k$$

(das ist $(a_n x^n + \dots + a_0) \cdot (b_m x^m + \dots + b_0)$ ausmultipliziert).

Insbesondere ist für

$$f = x^i = 1 \cdot x^i + 0 \cdot x^{i-1} + \dots + 0$$

$$g = x^j = 1 \cdot x^j + 0 \cdot x^{j-1} + \dots + 0$$

$$f \cdot g = x^i \cdot x^j = \sum_{k=0}^{i+j} \underbrace{\left(\sum_{l=0}^{k} a_l b_{k-l} \right)}_{\substack{\text{falls } k < i+j, \text{ ist} \\ \text{immer einer der beiden} \\ \text{Koeffizienten } = 0.}} x^k = x^{i+j}$$

Wie man leicht nachrechnet, ist $R[x]$ ein kommutativer Ring mit 1.

Ist $f = \sum_{k=0}^{n} a_k x^k$ und $a_n \neq 0$, so heißt $n =: \deg(f)$ der <u>Grad</u> von f. Wir setzen $\deg(0) = -\infty$.

Der <u>Leitkoeffizient</u> von $f \neq 0$, $LC(f)$, ist a_n, wobei $n = \text{grad}(f)$.

Es gilt

$\deg(f+g) \leq \max\{\deg f, \deg g\}$ und

$\deg(f+g) = \max\{\deg f, \deg g\} \Longleftrightarrow$

$\deg f \neq \deg g$ oder $\deg f = \deg g$ und $LC(f) \neq -LC(g)$

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

$\deg(f\cdot g) = \deg f + \deg(g) \iff$

$LC(f) \cdot LC(g) \neq 0$

<u>Bsp</u>: In $\mathbb{Z}_6[x]$ ist

$(2x+1)\cdot(3x^2+2x+1) =$

$6x^3 + (2\cdot 2+3\cdot 1)x^2 + (2\cdot 1+1\cdot 2)x$

$+ 1\cdot 1 = 0x^3 + 1\cdot x^2 + 4\cdot x + 1$

$= x^2 + 4x + 1$.

<u>Bem</u> Wir erhalten Polynomringe in mehreren Veränderlichen rekursiv durch

$R[x_1,\dots,x_n] := R[x_1,\dots,x_{n-1}][x_n]$

3.2.2 Def (K-Algebra)

Ein K-Vektorraum, auf dem zusätzlich eine Multiplikation $\circ : A \times A \to A$ definiert ist, so daß $(A, +, \circ)$ ein Ring mit 1 ist, heißt <u>K-Algebra</u>, falls die Skalarmultiplikation $\cdot$ mit der Ringmultiplikation $\circ$ verträglich ist:

$\forall \lambda \in K,\ x, y \in A$:

$$\lambda \cdot (x \circ y) = (\lambda \cdot x) \circ y = x \circ (\lambda \cdot y)$$

Ist $K = R$ ein Ring und A ein R-Modul mit verträglicher zusätzlicher Multiplikation, so nennen wir A R-Algebra.

<u>Bsp</u>

1) Sei K ein Körper. $\mathrm{Mat}(n \times n, K)$ ist K-Algebra.

2) Sei K ein Körper, V ein K-Vektorraum. $\mathrm{End}_K(V)$ ist K-Algebra.

3) Sei R ein Ring, $\emptyset \neq X$ eine Menge.

$\mathrm{Abb}(X, R) = \{ f : X \to R \}$

ist mit der punktweisen Addition

$$f+g\,(x) = f(x) + g(x)$$ und Mult

$$f\cdot g\,(x) = f(x)\cdot g(x) \quad \forall\, x \in X$$

ein Ring.

Wir definieren zusätzlich die Skalarmultiplikation

$$(\lambda \cdot f)(x) = \lambda \cdot f(x) \quad \forall\, x \in X,\ \lambda \in R$$

und erhalten so eine R-Algebra.

<u>Bemerkung</u>: Wir können eine R-Algebra auch auffassen als einen (kommutativen) Ring $(A, +, \cdot)$ und einen Ringhomomorphismus $\varphi: R \longrightarrow A$, der die Skalarmultiplikation darstellt $(\lambda \longmapsto \lambda \cdot 1_A)$.

<u>3.2.3 Bsp</u> Sei R ein Ring mit 1, dann ist die <u>charakteristische Abb.</u>

$$\chi: \mathbb{Z} \longrightarrow R: n \mapsto n \cdot 1_R = \underbrace{1_R + \dots + 1_R}_{n\text{-Mal}}$$

ein Ringhomomorphismus.

Durch χ wird R zu einer $\mathbb{Z}$-Algebra.

$\forall\, n \in \mathbb{Z},\ r \in R$: $\chi(n)\cdot r = (1_R + \dots + 1_R)\cdot r$
$= r + \dots + r = r\cdot(1_R + \dots + 1_R) = r\cdot\chi(n)$.

3.2.4 Def Seien A_1, A_2 R-Algebren, mit $i_1: R \to A_1$, $i_2: R \to A_2$.
Ein Ringhomomorphismus $\varphi: A_1 \to A_2$ heißt R-Algebren-Homomorphismus, falls $\varphi \circ i_1 = i_2$:

$$\begin{tikzcd} A_1 \arrow[r, "\varphi"] & A_2 \\ R \arrow[u, "i_1"] \arrow[ur, "i_2"'] & \end{tikzcd}$$

Anders gesagt:
φ ist mit allen 3 Operationen verträglich:

$$\varphi(a+b) = \varphi(a) + \varphi(b)$$
$$\varphi(a\cdot b) = \varphi(a)\cdot\varphi(b)$$
$$\varphi(\lambda\cdot a) = \varphi(i_1(\lambda)\cdot a) = \varphi(i_1(\lambda))\cdot\varphi(a) = i_2(\lambda)\cdot\varphi(a) = \lambda\cdot\varphi(a)$$

$\forall\, a, b \in A_1$, $\lambda \in R$.

3.2.5 Satz (Universelle Eigenschaft des Polynomrings)

Sei R ein kommutativer Ring mit 1, A eine R-Algebra, $a \in A$.
Dann $\exists!$ R-Algebrenhomomorphismus
$\varphi: R[X] \longrightarrow A$ mit $X \longmapsto a$,
den Einsetzehomomorphismus.
Das Bild von φ heißt die von a erzeugte Unteralgebra $\langle a \rangle \subset A$.
Analog bei mehreren Veränderlichen.

Beweis: Durch $\varphi(a_0 + a_1 X + \dots + a_n X^n) = a_0 + a_1 \cdot a + \dots + a_n \cdot a^n$ ist der eindeutige Homomorphismus gegeben. $\square$

Bsp

1) Sei V ein K-Vektorraum. $\mathrm{End}_K(V)$ ist K-Algebra, und wir kennen den Homomorphismus
$\varphi_f: K[X] \longrightarrow \mathrm{End}_K(V): X \mapsto f$
bzw
$\varphi_A: K[X] \longrightarrow \mathrm{Mat}(n, K): X \mapsto A$

Das charakteristische Polynom und das Minimalpolynom eines Endomorphismus/ einer Matrix sind im Kern.

2) Sei $d \in \mathbb{Z}$, $\sqrt{d} \in \mathbb{C}$, betrachte

$$\varphi : \mathbb{Z}[x] \longrightarrow \mathbb{C}$$
$$x \longmapsto \sqrt{d}$$

Dann ist

$$\operatorname{Im}(\varphi) =: \mathbb{Z}[\sqrt{d}]$$
$$= \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\},$$ denn $d^2 \in \mathbb{Z}$.

Der Begriff des Ideals ist auch durch Nullstellenmengen von Polynomen motiviert:

<u>3.2.6 Def</u> Seien $f_1, \dots, f_r \in K[x_1, \dots, x_n]$

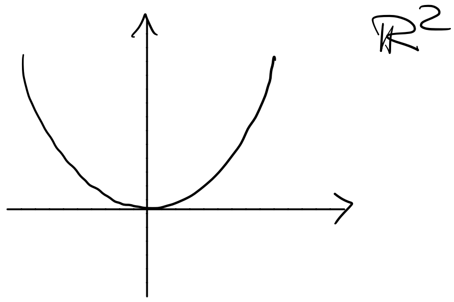
Setze $V(f_1, \dots, f_r) = \{p \in K^n \mid f_i(p) = 0 \ \forall i\}$ die <u>affine Varietät</u> der f_i (die gemeinsame Nullstellenmenge).

<u>Bsp</u>

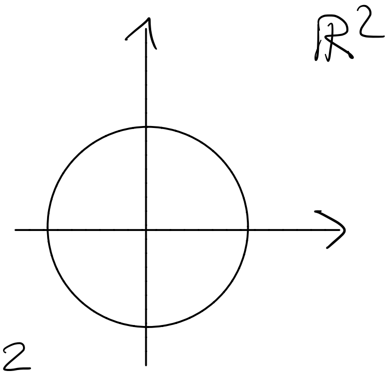
1) $V(1) = \emptyset$, $\quad V(0) = K^n$

2) Seien $f_i = \sum a_{ij} x_j - b_i$ lineare Polynome, $A = (a_{ij})$, $b = (b_i)$, dann ist $V(f_1, \dots, f_r) = \text{Lös}(A, b)$ ein affiner Unterraum des K^n.

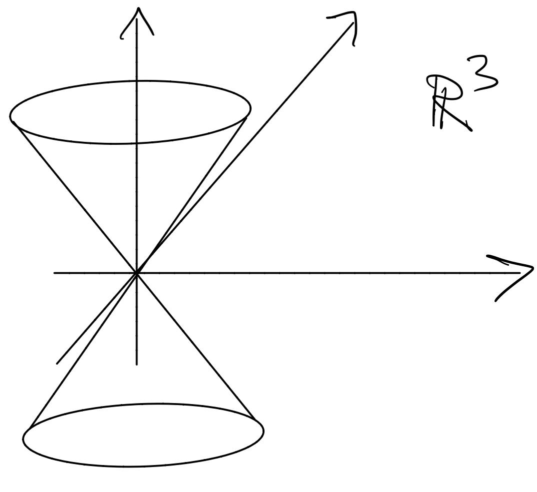
3) $f = x^2 - y \in \mathbb{R}[x,y]$

$V(f) =$ 

4) $f = x^2 + y^2 - 1$

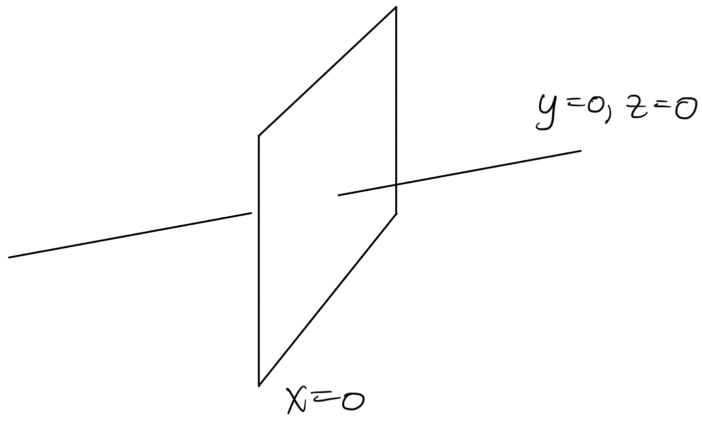
$V(f) =$ 

5) $f = x^2 + y^2 - z^2$



6) $f_1 = xy, \ f_2 = xz,$

$V(f_1, f_2) =$



<u>Bemerkung:</u>

$V(f_1, \dots, f_r)$ hängt nur von dem von den f_i erzeugten Ideal $I = \langle f_1, \dots, f_r \rangle$ ab, denn wenn $f_1(p) = \dots = f_r(p) = 0$, dann auch $\sum r_i f_i(p) = 0$ für $r_i \in K[X_1, \dots, X_n]$.

<u>3.2.7 Def</u> Sei $I \subset K[X_1, \dots, X_n]$ ein Ideal, dann ist

$V(I) = \{ p \in K^n \mid f(p) = 0 \ \forall f \in I \}$

die Verschwindungsmenge von I.

Wir werden sehen (noethersche Ringe), daß $V(I)$ eine affine Varietät ist, da jedes $I \subset K[X_1, \dots, X_n]$ endlich erzeugt ist.

Ist $V \subset K^n$, so ist

$I(V) := \{ f \in K[x_1, \dots, x_n] \mid f(p) = 0 \ \forall p \in V \}$
das <u>Verschwindungsideal</u> von V

3.2.8 Lemma $I(V)$ ist ein Ideal.

Beweis: Seien $f, g \in I(V) \Rightarrow$
$f(p) = 0 = g(p) \ \forall p \in V \Rightarrow f+g\,(p) = 0$
$\forall p \in V \Rightarrow f+g \in I(V)$. Sei
$r \in K[x] \Rightarrow (r \cdot f)(p) = 0 \ \forall p \in V$
$\Rightarrow r \cdot f \in I(V)$. $\square$

Ideale kommen bei der Betrachtung geometrischer Objekte, die durch polynomiale Gleichungen gegeben sind, in natürlicher Weise vor.

3.3 Noethersche Ringe

3.3.1 Satz Sei R ein kommutativer Ring mit 1.
Dann sind äquivalent:

1) Jedes Ideal $I \subset R$ ist endlich erzeugt.

2) Jede aufsteigende Kette
$I_1 \subset I_2 \subset I_3 \subset \cdots$ von Idealen
wird stationär, i.e. $\exists$ m mit
$I_m = I_{m+1} = I_{m+2} = \cdots$

3) Jede nicht-leere Menge von Idealen besitzt bezüglich der Inklusion ein maximales Element.

Erfüllt R diese Eigenschaften, so heißt R <u>noethersch</u>.

<u>Beweis:</u>

„1) ⇒ 2)": Sei $I_1 \subset I_2 \subset \cdots$ eine Kette von Idealen. Dann ist
$I = \bigcup_{i=1}^{\infty} I_i$ ein Ideal:

sei $a, b \in I$
$\Rightarrow \exists\, j_1, j_2 \in \mathbb{N} : a \in I_{j_1},\ b \in I_{j_2}$,
OE $j_1 < j_2$, dann ist $a \in I_{j_1} \subset I_{j_2}$,
also $a, b \in I_{j_2} \Rightarrow a+b \in I_{j_2}$
$\Rightarrow a+b \in I$

Sei $a \in I$, $r \in R$
$\Rightarrow \exists\, j : a \in I_j \Rightarrow r \cdot a \in I_j$

$\Rightarrow ra \in I$

$\overset{1)}{\Rightarrow}$ $I = \langle a_1, \dots, a_r \rangle$ ist endlich erzeugt.

Für jedes a_i $\exists$ j_i mit $a_i \in I_{j_i}$.

Sei $k = \max\{j_i \mid i = 1, \dots, r\}$, dann ist $a_1, \dots, a_r \in I_k \Rightarrow$

$\langle a_1, \dots, a_r \rangle \subset I_k \Rightarrow I \subset I_k$

$\Rightarrow$ ab k ist die Kette stationär.

$\square$

„2) $\Rightarrow$ 3)": Angenommen, (3) gilt nicht. Dann gibt es eine Menge M von Idealen, so daß $\forall I \in M$ $\exists$ $I' \in M$: $I \subsetneq I'$

Rekursiv können wir eine Kette erzeugen, die nicht stationär wird.

„3) $\Rightarrow$ 1)": Sei I ein Ideal. Betrachte

$M = \{ J \subset I \mid J$ ist endlich erzeugtes Ideal $\}$

$M \neq \emptyset$, denn $\langle 0 \rangle \in M$.

Sei J ein maximales Element von

M. $\exists\, a_1, \dots, a_r$: $J = \langle a_1, \dots, a_r \rangle$.

Angenommen, $J \subsetneq I$, dann $\exists\, a \in I \setminus J$, $J \subsetneq \langle a_1, \dots, a_r, a \rangle \subset I$

$\Rightarrow \langle a_1, \dots, a_r, a \rangle \in M$ $\lightning$ zur Maximalität von J $\Rightarrow J = I$ ist endlich erzeugt. $\square$

Bsp: $\mathbb{Z}$ ist noethersch. Jede Untergruppe bez. $+$ ist von der Form $n\mathbb{Z} = \langle n \rangle$, also von einem Element erzeugt.

3.3.2 Lemma

R hat nur zwei Ideale $\Leftrightarrow$ R ist Körper

Beweis:

„$\Rightarrow$" $\{0\}$, R sind Ideale. Sie sind die einzigen. Für $a \neq 0$, $a \in R$ folgt damit $\langle a \rangle = R$ $\Rightarrow$ $\exists\, r \in R$: $r \cdot a = 1$ $\Rightarrow$ a ist invertierbar und R ist ein Körper.

„$\Leftarrow$" $\{0\}$, R sind Ideale. Sei $I \subset R$ ein Ideal mit $0 \neq a \in I$ $\Rightarrow$ $a^{-1} \cdot a = 1 \in I$ $\Rightarrow$ $r \cdot 1 = r \in I$ $\forall r \in R$ $\Rightarrow$ $I = R$ $\Rightarrow$ es gibt keine weiteren Ideale.

3.3.3 Korollar Ein Körper K ist noethersch.

Beweis: K hat nur zwei Ideale, $K = \langle 1 \rangle$, $\{0\} = \langle 0 \rangle$, beide sind endlich erzeugt. $\square$

3.3.4 Satz (Hilberts Basissatz)

R noethersch $\Rightarrow$ $R[X]$ noethersch

3.3.5 Korollar

R noethersch $\Rightarrow$ $R[X_1, \ldots, X_n]$ noethersch.

Beweis: Hilberts Basissatz 3.3.4 und Induktion. $\square$

3.3.6 Korollar

Sei K ein Körper, $K[X_1, \ldots, X_n]$ ist noethersch.

<u>Beweis</u>: Hilberts Basissatz 3.3.4 und Induktion mit Induktionsanfang 3.3.3. $\square$

3.3.7 Korollar

Die Verschwindungsmenge $V(I)$ eines Ideals $I \subset K[x_1, \dots, x_n]$ (Def. 3.2.7) ist eine affine Varietät (Def. 3.2.6).

<u>Beweis</u>: Da $I = \langle f_1, \dots, f_r \rangle$ endlich erzeugt, ist $V(I) = V(f_1, \dots, f_r)$. $\square$

3.3.8 Def.

Sei $f = a_k x^k + \dots + a_0 \in R[x]$ ein Polynom. $a_i x^i$ heißt <u>Term</u> von f, x^i <u>Monom</u>, a_i <u>Koeffizient</u>, $a_k x^k$ der <u>Leitterm</u> $LT(f)$, x^k <u>Leitmonom</u> $LM(f)$. Falls $LC(f) = 1$, heißt f <u>normiert</u>.

<u>Beweis von Hilberts Basissatz 3.3.4:</u>

Angenommen, $R[x]$ wäre nicht noethersch $\Rightarrow \exists\, I$ nicht endlich erzeugt. Sei $0 \neq f_1 \in I$ mit

$\deg(f_1)$ minimal, $0 \neq f_2 \in I \setminus \langle f_1 \rangle$ mit $\deg(f_2)$ minimal, usw.

$\Rightarrow \deg(f_1) \leq \deg(f_2) \leq \dots$

Wir erhalten eine aufsteigende Kette von Idealen in R:

$\langle LC(f_1) \rangle \subset \langle LC(f_1), LC(f_2) \rangle \subset \dots$

Da R noethersch ist, wird sie stationär, i.e. $\exists\, k$:

$\langle LC(f_1), \dots, LC(f_k) \rangle = \langle LC(f_1), \dots, LC(f_k), LC(f_{k+1}) \rangle$

$\Rightarrow \exists\, b_j \in R$:

$$LC(f_{k+1}) = \sum_{j=1}^{k} b_j \, LC(f_j)$$

Setze $g := \sum_{j=1}^{k} b_j \, X^{\deg(f_{k+1}) - \deg(f_j)} \cdot f_j$.

Dann ist $g \in I$ und

$$LC(g) = \sum_{j=1}^{k} b_j \, LC(f_j) = LC(f_{k+1})$$

$\Rightarrow \deg(g - f_{k+1}) < \deg(f_{k+1})$.

Aber $g - f_{k+1} \in I \setminus \langle f_1, \dots, f_k \rangle$, denn $g - f_{k+1} \in I$ und wäre $g - f_{k+1} \in \langle f_1, \dots, f_k \rangle$, dann wäre, da $g \in \langle f_1, \dots, f_k \rangle$ auch $f_{k+1} \in \langle f_1, \dots, f_k \rangle$ ↯.

Also ist $R[X]$ noethersch. $\square$

3.4 Nullteilerfreie Ringe

3.4.1 Def Ein kommutativer Ring mit 1 ohne nicht-triviale Nullteiler (3.1.3) heißt nullteilerfrei oder Integritätsbereich oder Integritätsring.

Bsp: $\mathbb{Z}$, $K[X]$, K sind nullteilerfrei.

3.4.2 Def Sei R nullteilerfrei.

Wir definieren auf $R \times R \setminus \{0\}$ eine Äquivalenzrelation $(a,b) \sim (c,d) :\Leftrightarrow ad = cb$. Wir schreiben $\frac{a}{b}$ für die Äquivalenzklasse $[(a,b)]$.

Auf der Menge der Äquivalenzklassen

definieren wir durch $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ und $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ eine Addition und Multiplikation. Damit erhalten wir den <u>Quotientenkörper</u> $\mathrm{Quot}(R)$. Er ist der kleinste Körper, in den R eingebettet werden kann: $R \to \mathrm{Quot}(R)$: $a \mapsto \frac{a}{1}$.

<u>Bsp:</u> $\mathbb{Z} \subset \mathbb{Q}$.

<u>3.4.3 Def</u> Sei K ein Körper, $\chi: \mathbb{Z} \to K : n \mapsto n \cdot 1_K$ die charakteristische Abb. aus Def. 3.2.3. Dann ist $\ker(\chi) \subset \mathbb{Z}$ ein Ideal, also $\ker(\chi) = p\mathbb{Z}$ für ein $p \in \mathbb{N}$.

1. Fall: $p = 0 \iff \chi$ injektiv
   Dann läßt sich χ zu einem Monomorphismus $\chi: \mathbb{Q} \hookrightarrow K$ fortsetzen.

2. Fall: $p > 0$. Dann ist

$\mathbb{Z}_p \hookrightarrow K$ wegen des Homomorphie-satzes 3.1.10 ein Unterring von K.
Da K nullteilerfrei ist, muß auch $\mathbb{Z}_p$ nullteilerfrei sein.
Wäre $p = a \cdot b$ zerlegbar, so wären $0 \neq a, b \in \mathbb{Z}_p$ Nullteiler, denn $ab = p = 0$ ↯. Damit ist p prim.

In beiden Fällen nennen wir $p = \mathrm{char}(K)$ die <u>Charakteristik</u> des Körpers K.

<u>Bsp</u>: $\mathrm{char}(\mathbb{Q}) = 0$, $\mathrm{char}(\mathbb{Z}_p) = p$.
($\mathbb{Z}_p$ ist ein Körper, siehe Übung).

<u>3.4.4 Def</u> Sei R ein kommutativer Ring mit 1. Ein Ideal $P \subsetneq R$ heißt <u>Primideal</u>, wenn $\forall a, b \in R$ gilt:
$$a \cdot b \in P \Rightarrow a \in P \text{ oder } b \in P$$

Ein Ideal $m \subsetneq R$ heißt <u>maximales Ideal</u>, wenn für Ideale I mit

$\mathfrak{m} \subsetneq I \subset R$ gilt $I = R$.

3.4.5 Lemma Sei $p \in \mathbb{Z}$, $p > 0$.
$p\mathbb{Z}$ ist Primideal $\iff$ p prim.

Beweis: „$\Leftarrow$" Sei $ab \in p\mathbb{Z} \Rightarrow p \mid ab \overset{1.12}{\Rightarrow}$ $p \mid a$ oder $p \mid b \Rightarrow a \in p\mathbb{Z}$ oder $b \in p\mathbb{Z} \Rightarrow p\mathbb{Z}$ ist Primideal

„$\Rightarrow$" Sei $p = ab \Rightarrow ab \in p\mathbb{Z} \Rightarrow$ OE $a \in p\mathbb{Z} \Rightarrow p \mid a \Rightarrow$ $\exists\, k: p \cdot k = a \Rightarrow p = p \cdot k \cdot b$ $\Rightarrow k \cdot b = 1 \Rightarrow b = \pm 1 \Rightarrow$ p ist nicht zerlegbar $\Rightarrow p$ ist prim. $\square$

3.4.6 Lemma $p\mathbb{Z} \subset \mathbb{Z}$ ist maximal für p prim.

Beweis: Sei $\langle p \rangle \subsetneq I \Rightarrow \exists\, q \in I$, $q \notin \langle p \rangle \Rightarrow p \nmid q \Rightarrow \mathrm{ggT}(p,q) = 1$ $\Rightarrow \exists\, k, l: kp + lq = 1 \in I \Rightarrow$ $I = \mathbb{Z} \Rightarrow \langle p \rangle$ ist maximal. $\square$

<u>Bsp</u> $\langle 0 \rangle \subset \mathbb{Z}$ ist Primideal, aber nicht maximal.

$6\mathbb{Z} \subset \mathbb{Z}$ ist kein Primideal, denn $2 \cdot 3 = 6 \in 6\mathbb{Z}$ aber $2 \notin 6\mathbb{Z}$, $3 \notin 6\mathbb{Z}$.

$6\mathbb{Z} \subset \mathbb{Z}$ ist auch nicht maximal, denn $6\mathbb{Z} \subsetneq 3\mathbb{Z} \subsetneq \mathbb{Z}$.

<u>3.4.7 Satz</u> Sei $I \subsetneq R$ ein Ideal.

1) I Primideal $\Leftrightarrow$ R/I nullteilerfrei

2) I maximal $\Leftrightarrow$ R/I Körper

<u>Beweis:</u>

1) „$\Rightarrow$" Seien $[a], [b] \in R/I$ mit $[a] \cdot [b] = [0] \Rightarrow ab \in I \Rightarrow$ $a \in I$ oder $b \in I$ $\Rightarrow$ $[a] = [0]$ oder $[b] = [0]$ $\Rightarrow$ es gibt keine Nullteiler.

„$\Leftarrow$" Sei $ab \in I$ aber $a \notin I$, $b \notin I$, dann ist $[a] \neq [0]$, $[b] \neq [0]$ und $[a][b] = [ab] = [0]$ $\Rightarrow [a], [b]$ sind Nullteiler.

2) „$\Rightarrow$" Sei $\mathfrak{m}$ maximal, $[a] \neq [0]$ in $R/\mathfrak{m}$ $\Rightarrow$ $a \notin \mathfrak{m}$ $\Rightarrow$ $\mathfrak{m} \subsetneqq \langle \mathfrak{m}, a \rangle = R$ $\Rightarrow$ $\exists$ $m \in \mathfrak{m}$, $r \in R$: $m + ra = 1$ $\Rightarrow$ $[ra] = [1] \in R/\mathfrak{m}$ $\Rightarrow$ $[a]$ ist invertierbar mit $[a]^{-1} = [r]$.

„$\Leftarrow$" Sei $R/\mathfrak{m}$ Körper und $\mathfrak{m} \subsetneqq I$ ein Ideal. Sei $a \in I \setminus \mathfrak{m}$. Dann ist $[a] \neq [0]$ in $R/\mathfrak{m}$ $\Rightarrow$ $\exists$ $b \in R$: $[a][b] = [1]$ $\Rightarrow$ $1 - ab \in \mathfrak{m}$

$$\Rightarrow \underbrace{1-ab}_{\in \mathfrak{m} \subset I} + \underbrace{ab}_{\in I} = 1 \in I$$

$\Rightarrow$ $I = R$.

$\Rightarrow$ $\mathfrak{m}$ ist maximal. $\square$

3.4.8 Korollar I maximal $\Rightarrow$ I prim

Beweis: I maximal $\Rightarrow$ R/I Körper $\Rightarrow$ R/I nullteilerfrei $\Rightarrow$ I prim. $\square$

3.4.9 Korollar

$\langle 0 \rangle \subset R$ ist Primideal $\Leftrightarrow$ R nullteilerfrei.