§4 Ringe

4.1 Def Ein Ring $(R,+,\cdot)$ ist eine Menge zusammen mit 2 Verknüpfungen

$$R\times R \to R \quad (a,b)\mapsto (a+b)$$
$$R\times R \to R \quad (a,b)\mapsto (a\cdot b)$$

für die gilt

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

(R2) Die Multiplikation ist assoziativ

(R3) Die Verknüpfungen sind distributiv

$(a+b)\cdot c = a\cdot c + b\cdot c \qquad a(b+c) = a\cdot b + a\cdot c$

Existiert darüber hinaus ein 1-Element

(R4) $\exists\, 1\in R$ mit $a\cdot 1 = 1\cdot a = a \ \forall a\in R$

so spricht man von einem Ring mit 1.

Ist die Multiplikation kommutativ

(R5) $a\cdot b = b\cdot a$ so spricht man von einem kommutativen Ring.

Bem Mit Hilfe des Distributivgesetz sieht man sofort

$a\cdot 0 = 0\cdot a = 0$, sowie $(-a)\cdot b = a\cdot(-b) = -ab$

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

Beispiele 0) Der Nullring $R=\{0\}$. In dem Fall ist 0 auch 1-Element.

1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind kommutative Ringe mit 1

2) K Körper, V ein K-Vektorraum. Dann ist

$End(V) = \{f: V\to V \mid f \text{ k-linear}\}$

ein Ring mit $1 = id_V$. Ist $V\cong K^n$ dann ist $End(V)\cong M(n\times n, K)$ der Ring der $n\times n$-Matrizen. Ist $\dim V\geq 2$ so ist $End(V)$ nicht kommutativ

3) R ein Ring, X eine Menge. $R^X = \{f: X\to R\}$ ein Ring vermöge $(f\pm g)(x) = f(x)\pm g(x)$

4) $\mathcal{C}[0,1]$:= Menge d. stetigen Fkt ist ein Ring und Unterring von $\mathbb{R}^{[0,1]}$

5) $R_1, \dots, R_n$ Ringe. Dann sind durch komponentenweise definierte Verknüpfungen $R_1 \times R_2 \times \dots \times R_n$ zu einem Ring.
Die meisten Ringe, die betrachtet werden sind kommutative Ringe mit 1.

4.2 <u>Def</u> Ein Ringhomomorphismus $\varphi: R \to S$ ist eine Abb zwischen Ringen die $\varphi(a \pm b) = \varphi(a) \pm \varphi(b)$ erfüllt.
Sind R und S Ringe mit 1, so verlangt meist zusätzlich

$\varphi(1_R) = 1_S$ (Wegen $\varphi(1)^2 = \varphi(1)$ ist das keine starke zusätzliche Bedingung)

Man spricht von unitären Ringhomomorphismen

4.3 <u>Def</u> Sei R ein Ring. Eine Teilmenge $(\neq \emptyset)$ $I \subset R$ heißt ein Ideal, wenn $a, b \in I \Rightarrow a+b \in I$

$a \in I, r \in R \Rightarrow ra \in I$ gilt.

<u>Beispiele</u> 1) Die Ideale in $\mathbb{Z}$ sind die Mengen $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ und 0, $n \geq 1$

2) $\varphi: R \to S$ ein Ringhomomorphismus. Dann ist $\ker \varphi = \{a \in R, \varphi(a) = 0\} \subset R$ ein Ideal.

In der Tat $a, b \in \ker \varphi$, $r \in R$

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

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

$\Rightarrow a, b \in \ker \varphi$, $ra \in \ker \varphi$

In nicht kommutativen Ringen unterscheidet man Linksideal, Rechtsideal und beidseitige Ideale.

Jedes (beidseitige) Ideal $I \subset R$ ist Kern eines Ringhomomorphismus.
Wir können der Quotientengruppe $(R/I, +)$ eine Ringstruktur geben, indem wir repräsentantenweise multiplizieren

$(r_1 + I) \cdot (r_2 + I) := r_1 r_2 + I$

Dies ist wohldefiniert, da I ein Ideal ist

$(r_1 + a)(r_2 + b) = r_1 r_2 + \underbrace{a r_2 + r_1 b + ab}_{\in I}$ $a, b \in I$

Also $(r_1+a)(r_2+b)+I = r_1 r_2 + I$

Beispiele 1) $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$

2) Man nennt R/I den Restklassenring von R modulo I und schreibt für Äquivalenzrelation auf R

$a \sim b \Leftrightarrow a-b \in I$ häufig $a \equiv b \mod I$.

4.4 Definition Sei R ein Ring (mit 1) Eine R-Algebra S ist ein Ring ~~mit~~ mit 1 zusammen mit einem injektiven Ringhomomorphismus $i: R \to S$, sodass $i(R) \subseteq \mathcal{Z}(S)$
$= \{a \in R \mid ra = ar \ \forall r \in R\}$

Beispiel 1) S beliebiger Ring mit 1 $\mathbb{Z} \to S$ $n \mapsto n \cdot 1_S$

ist $\ker \varphi = k\mathbb{Z}$ so ist S eine $\mathbb{Z}/k\mathbb{Z}$-Algebra

2) V ein K-Vektorraum. Dann ist $\mathrm{End}(V)$ eine K-Algebra der Form $K \to \mathrm{End}(V)$
$\lambda \mapsto \lambda \cdot id_V$

4.5 Konvention (nicht Standard)

Unter einem Ring (abweichend von der Def von E. Noether) verstehen wir stets einen kommutativen Ring mit 1.

Björn Poonen: Folgende werden Ringe ohne 1 mit Rng bez.

Bsp $2\mathbb{Z}$ ist Rng.

$\mathcal{C}_c(\mathbb{R}) = \{f: \mathbb{R} \to \mathbb{R} \mid$ stetig mit kompakten Träger$\}$ ist nur ein Ring ohne 1.

$\mathcal{C}_c(\mathbb{R}) \subset \mathcal{C}(\mathbb{R})$ ist aber ein Ideal in $\mathcal{C}(\mathbb{R})$

4.6 Der Polynomring

Sei R ein Ring. Dann definieren wir $R[x]$ wie folgt:

Als Menge $R^{(\mathbb{N})} = \{a: \mathbb{N} \to R \mid a_i = a(i) = 0$ für fast alle $i\}$

$= \{(a_0, a_1, \dots, a_n, 0, \dots) \mid a_i \in R\}$

Die Addition ist komponentenweise erklärt.

Die Multiplikation $(a_0, a_1, \dots a_n, 0) \cdot (b_0, b_1, \dots, b_m, 0, \dots) = (c_0, c_1, \dots c_{n+m}, 0)$

wobei $c_k = \sum_{i+j=k} a_i \cdot b_j$

Für $x = (0, 1, 0, \dots)$ gilt dann $x^i = (0, \dots, 0, \underset{\substack{\uparrow \\ i\text{-te Position}}}{1}, 0, \dots 0)$

Wir können daher $(a_0, a_1, \dots, a_n, 0, \dots) = \sum_{i=0}^{n} a_i x^i$ schreiben.

Die Elemente ~~aller~~ nennen wir Polynome und

$R[x] = \{\sum_{i=0}^{n} a_i x^i \mid a_i \in R\}$ den Polynomring.

Die Multiplikationsformel $\sum_{i=0}^{n} a_i x^i \cdot \sum_{j=0}^{m} b_j \cdot x^j$

$= \sum_{k=0}^{n+m} (\sum_{i+j=k} a_i b_j) x^k$

$R \hookrightarrow R[x]$, vermöge $a \mapsto a x^0 = a = (a, 0, \dots 0)$

$R[x]$ ist eine R-Algebra.

4.7 Satz (Universelle Eigenschaft des Polynomrings)

Sei R ein Ring, S eine R-Algebra und $s \in S$.

Dann gibt es genau einen R-Algebrahomomorphismus

$R[x] \to S$ mit $x \mapsto s$

Beweis: Wegen der R-Algebrastruktur von S muss $\sum_{i=0}^{n} a_i x^i$ auf $\sum_{i=0}^{n} a_i s^i$ abgebildet werden und dies definiert einen Homomorphismus $\square$

Man kann also für x bel. $s \in S$ einsetzen.

Man nennt daher $x \in R[x]$ auch eine Unbestimmte.

Den Polynomring mit n Unbestimmten $x_1, \dots, x_n$ definiert man rekursiv $R[x_1, \dots, x_n] = R[x_1, \dots, x_{n-1}][x_n]$.

Man beachte allerdings, dass man in Polynome mit mehreren Unbestimmten nicht beliebige Tupel $s_1, \dots, s_n$ von R-Algebra einsetzen kann.

Wegen $x_i x_j = x_j x_i \in R[x_1, \dots, x_n]$ müssen s_j miteinander komm.

Mit $R[s]$ bzw. $R[s_1, \dots, s_n] \subset S$ bez. wir das Bild d. Substitutionshomomorphismus

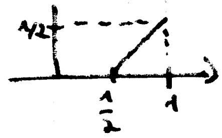
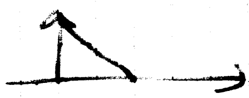
Beispiel: K Körper $A \in M(n \times n, K) = End(K^n)$ dann wir eine Substitutionshomom.

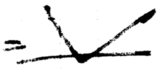
$\varphi: K[x] \to End(K^n)$, $x \mapsto A$

und das Minimalpolynom ist das normierte Polynom kleinsten Grades in $\ker \varphi$.

4.8 Def R Ring. Ein Element $a \in R$ heißt <u>Nullteiler</u>, wenn es ein $b \in R$, $b \neq 0$ mit $ab = 0$ gibt.
R heißt Integritätsring, wenn $0 \in R$ der einzige Nullteiler ist.
Ein Element $a \in R$ heißt eine Einheit, wenn es ein $b \in R$ gibt mit $a \cdot b = 1$.
Mit $R^\times = \{a \in R \mid a \text{ Einheit}\}$ bezeichnet die Menge der Einheiten. Dies ist eine multiplikative Gruppe.
Beispiele 1) Die Nullteiler von $\mathbb{Z}/6\mathbb{Z}$ sind $\{\bar{0}, \bar{2}, \bar{3}, \bar{4}\}$.
In diesem Fall sind die verbleibenden Elemente
$\{\bar{1}, \bar{5}\}$ Einheiten $\bar{5} \cdot \bar{5} = \overline{25} = \bar{1}$

2) $\mathcal{C}[0,1]$ ist ein kein Integritätsring für

f  und g  gilt $f \cdot g = 0$.

Die Einheiten von $\mathcal{C}[0,1]$ sind die Funktionen ohne Nullstellen. Die Funktion $h =$ , ist eine Funktion, die weder ein Nullteiler noch eine Einheit ist.
4.9 <u>Satz</u> Ist R ein Integritätsring, dann ist auch $R[x]$ ein Integritätsring. In diesem Fall sind die Einheiten von $R[x]$ die Einheiten $R^\times \subset R \subset R[x]$.
Notation $f = \sum_{i=0}^{n} a_i x^i$ mit $a_n \neq 0$, dann ~~heißt~~ ist der Grad von f
$\deg f = n$ und a_n heißt Leitkoeffizient.
$\deg 0 = -\infty$
<u>Rechenregeln</u>: $f, g \in R[x]$. Dann gilt
$\deg(f+g) \leq \max\{\deg f, \deg g\}$ und
$\deg(fg) \leq \deg f + \deg g$
Ist R ein ~~[illegible]~~ Integritätsring. Dann gilt für f mit $\deg f = n$
und Leitkoeffizient a_n und g mit $\deg g = m$, LK b_m

dass $\deg(f g) = n+m$, da der Leitkoeffizient des Produkt $a_n \cdot b_m \neq 0$

Also $R[x]$ ist ebenfalls Integritätsring und als Einheiten nenn wir Polynome mit Grad 0 in Betracht

Also $R[x]^\times = R^\times$

<u>Bem</u> In einem Integritätsring R gilt die Kürzungsregel

$$a \cdot b = 0 \implies a = 0 \lor b = 0$$

In beliebigen Ringen ist dies falsch: $\bar{2} \cdot \bar{3} = 0$ ...

4.10 <u>Def</u> Ein Ring K in dem jedes von 0 verschiedene Element eine Einheit ist, nennt man einen Körper.

<u>Beispiel</u>

4.11 <u>Satz</u> jeder endliche Integritätsring ist ein Körper.

<u>Beweis</u> Sei $\mathbb{F}$ ein endlicher ~~...~~ Integritätsring und $b \in \mathbb{F} \setminus \{0\}$. Multiplikation mit b liefert eine inj. Abb ($\mathbb{F}$ Integr. ring)

$$\mathbb{F} \xrightarrow{\cdot b} \mathbb{F}, \; a \mapsto a \cdot b$$

Dann gilt $a_1 b = a_2 b \iff (a_1 - a_2) b = 0$

$\implies a_1 - a_2 = 0 \implies a_1 = a_2$

Da $\mathbb{F}$ endl. ist ist die Abb $\mathbb{F} \xrightarrow{b} \mathbb{F}$ auch surjektiv. Es existiert also ein $a \in \mathbb{F}$ mit $a \cdot b = 1$, d.h. $b \in \mathbb{F}$ ist eine Einheit und $a = b^{-1}$ sein Inverses.

<u>Beispiele</u>

1) $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ ist ein Körper genau dann, wenn p prim ist.

2) Ist $\mathbb{F}_q$ ein Körper mit q-Elementen, dann ist der Kern des Ringhomom. $\mathbb{Z} \to \mathbb{F}_q$, $n \to n \cdot 1_{\mathbb{F}_q}$ genau $p \cdot \mathbb{Z}$.

Da $\mathbb{F}_q$ ein Integritätsring ist, ist auch $\mathbb{Z}/\ker\varphi$ ein

Integritätsring, also $\ker \varphi = p\mathbb{Z}$ für eine Primzahl p.
Man hat also eine Injektion $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathbb{F}_q$
Dies macht $\mathbb{F}_q$ zu einer $\mathbb{F}_p$-Algebra. Da $\mathbb{F}_p$ ein Körper ist, ist $\mathbb{F}_q$ also ein $\mathbb{F}_p$-Vektorraum mit $\dim < \infty$
$\dim_{\mathbb{F}_p} \mathbb{F}_q = n$. Es gilt also $q = p^n$.

4.11 Konstruktion des Quotientenkörpers

Sei R ein Integritätsring, dann lässt sich analog zur Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$ ein Quotientenkörper $Q(R)$ definieren: Auf $R \times R\setminus\{0\}$ führen wir die folgende Äquivalenzrelation ein: $(a,b) \sim (c,d) :\Leftrightarrow a\cdot d = b\cdot c$
Für die Transitivität brauchen wir, dass R ein Integritätsring ist.

$(a,b) \sim (c,d) \sim (e,f)$
$\Rightarrow ad = bc \quad , \quad cf = de$
$\Rightarrow adf = bcf \quad , \quad bcf = bde$
$\Rightarrow (af - eb)\cdot d = 0 \quad , \quad d \neq 0 \Rightarrow af = eb$
$\Rightarrow (a,b) \sim (e,f)$

Wir definieren den Quotientenkörper $Q(R) = \dfrac{R\times R\setminus\{0\}}{\sim}$
und bezeichnen mit $\frac{a}{b}$ die Äquivalenzklasse von $(a,b) \in R \times R\setminus\{0\}$.

Addition und Multiplikation werden wie üblich Repräsentantenweise definiert:

$$\frac{a}{b} + \frac{c}{d} := \frac{ad + cb}{bd} \qquad \frac{a}{b}\cdot\frac{c}{d} := \frac{ac}{bd}$$

Man überlegt sich leicht, dass diese Verknüpfungen wohldefiniert sind.

Vermöge die Inklusion $R \hookrightarrow Q(R)$ $a \mapsto \frac{a}{1}$ wird R zu einem Unterring von $Q(R)$.
$Q(R)$ ist ein Körper: zu $\frac{a}{b} \neq 0 = \frac{0}{1}$ also $a \neq 0$

ist $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$ das Inverse Element:

$$\left(\left(\frac{a}{b} \cdot \frac{b}{a}\right) = \frac{1}{1} = 1\right)$$

Satz 4.12 (Universelle Eigenschaft d. Quotientenkörpers)
Sei R ein Integritätsring und sei $\varphi: R \to K$ ein injektiver Ringhomomorphismus in einem Körper K. Dann ex. eine eindeutig bestimmte Fortsetzung von φ zu einem Ringhomom. Φ auf den Quotientenkörper

$$\begin{tikzcd} R \arrow[r, hook, "\varphi"] \arrow[d, hook] & K \\ Q(R) \arrow[ur, "\exists!\Phi"'] & \end{tikzcd}$$

<u>Beweis</u>: Da φ inj. ist gilt $\varphi(b) \neq 0 \; \forall b \in R \setminus \{0\}$
Es muss $\Phi\left(\frac{a}{b}\right) = \varphi(a) \cdot (\varphi(b))^{-1} \in K$ gelten,
da $1 = \Phi(1) = \Phi\left(b \cdot \frac{1}{b}\right) = \varphi(b) \cdot \Phi\left(\frac{1}{b}\right)$
und daher $\Phi\left(\frac{a}{b}\right) = \Phi\left(\frac{a}{1}\right) \cdot \Phi\left(\frac{1}{b}\right) = \varphi(a) \cdot (\varphi(b))^{-1}$
Die so repräsentantenweise definierte Abb Φ ist wohldef. □

<u>Def 4.13</u> (Die Charakteristik eines Körpers)
Sei K ein Körper und $\varphi: \mathbb{Z} \to K \quad n \mapsto n \cdot 1_K$
der kanonische Ringhomomorphismus.
Zwei Fälle sind denkbar:
1) φ ist injektiv. In diesem Fall lässt sich $\mathbb{Q} \hookrightarrow K$ als Unterkörper einbetten.
2) $\ker \varphi = p \cdot \mathbb{Z}$, p Primzahl.
In diesem Fall ist $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \hookrightarrow K$ ein Unterkörper.
Man nennt

$$\operatorname{char}(K) = \begin{cases} 0, & \text{falls } \mathbb{Z} \to K \text{ inj.} \\ p, & \text{falls } \ker(\mathbb{Z} \to K) = p\mathbb{Z} \end{cases}$$

die Charakteristik von K und man nennt $\mathbb{Q}$ bzw. $\mathbb{F}_p$ Primkörper.

Def 4.14

Sei R ein Ring. Ein Ideal $P \subset R$ heißt Primideal, wenn $a \cdot b \in P \Rightarrow a \in P$ oder $b \in P$

Ein Ideal $\mathfrak{M} \in R$ heißt <u>maximales Ideal</u>, wenn für Ideale $I \subset R$ mit $\mathfrak{M} \subset I \subsetneq R$ schon gilt $I = \mathfrak{M}$

$\mathfrak{M} \subset R$ ist also maximal in der Menge der echten Ideale von R.

<u>Satz 4.15</u> Sei R ein Ring und $I \subset R$ ein Ideal.

A) Äquivalent sind

(1) I ist ein Primideal

(2) R/I ist ein Integritätsring

B) Äquivalent sind

(1)' I ist ein maximales Ideal

(2)' R/I ist ein Körper

<u>Beweis</u>

A) Seien $a, b \in R$.

$$\begin{array}{ccc} a \cdot b \in I & \Longleftrightarrow & (a+I)(b+I) = 0 \in R/I \\ \Downarrow I \text{ prim} & & \Downarrow R/I \text{ Integritätsring} \\ a \in I \text{ oder } b \in I & \Longleftrightarrow & (a+I) = I \text{ oder } (b+I) = I \end{array}$$

B) Sei $g : R \to R/I$ die Restklassenabb.

Es gibt eine Bijektion $\{\bar{J} \subset R/I \text{ Ideale}\} \rightleftarrows \{J \subset R \text{ Ideale} \mid I \subseteq J \subset R\}$

$$\bar{J} \longmapsto g^{-1}(\bar{J})$$

$$J/I \longleftarrow J$$

Also I maximales Ideal

$\Leftrightarrow$ Die einzigen Ideale in R/I sind 0 oder R/I

$\Leftrightarrow$ Jedes von 0 verschiedene Element $\bar{a}$ in R/I erzeugt das Einheitenideal, d.h. $(\bar{a}) := \{\bar{r} \cdot \bar{a} \mid \bar{r} \in R/I\} = R/I$

Insbes. ex. also ein $\bar{r} \in R/I$ mit $\bar{r} \cdot \bar{a} = 1 \in R/I$

R/I ist ein Körper.

$\square$

Def 4.16 Sei R ein Ring und $a_1, \dots, a_n \in R$
Dann heißt $(a_1, \dots, a_r) := \{r_1 a_1 + \dots + r_n a_n \mid r_i \in R\}$
das von $a_1, \dots, a_n$ erzeugte ideal.
Es ist das kleinste Ideal von R, das $a_1, \dots, a_n$ enthält.
Speziell im Fall $n=1$ spricht man von einem Hauptideal $(a) = \{ra \mid r \in R\}$.
Ein ideal der Form $(a_1, \dots, a_n)$ heißt ein endlich erzeugtes ideal

Satz + Def 4.17 (Emmy Noether)
Sei R ein Ring. Die folgenden Aussagen sind äquivalent
(1) Jedes ideal $I \subset R$ ist endlich erzeugt.
(2) Jede aufsteigende Kette von Idealen

$$I_1 \subset I_2 \subset \dots I_k \subset \dots$$

wird ausschließlich stationär, d.h. $\exists n$ s.d.

$$I_n = I_{n+1} = \dots$$

(3) Jede nichtleere ~~Tei~~ Menge von idealen M hat ein bezüglich inklusion maximales Element
Man nennt einen Ring mit den obigen Eigenschaften einen Noetherschen Ring.

(1)$\Rightarrow$(2): Sei $I_1 \subset I_2 \subset \dots$ eine aufsteigende Kette von Idealen. Dann ist $I = \bigcup I_n \subset R$ ein ideal ex
$a, b \in I$ $\exists n_1, n_2$ mit $a \in I_{n_1}$, $b \in I_{n_2}$
Sei $m = \max(n_1, n_2)$, dann sind $a, b \in I_m \subset I$
Nach (1) ist I endl. erzeugt, etwa $I = (a_1, \dots, a_n)$
Sei $a_i \in I_{n_i}$ und $m = \max_{i=1,\dots,n} \{n_i\}$

Dann ist $I = (a_1, \dots, a_n) \subset I_m \subset I_{m+1} \subset \dots \subset I$
also $I = I_m = I_{m+1} = \dots$

(2)⇒(3): Angenommen $M \subset 2^R$ = Potenzmenge ist eine Menge von Idealen, die bzgl. Inklusion kein maximales Element enthält.

Dann gibt es $\forall\ I \in M$ ein $I' \in M$ mit $I \subsetneq I'$

Angefangen mit einem bel. Element $I \in M$ können wir also induktiv eine aufsteigende Kette von Idealen konstruieren. $I_1 \subsetneq I_2 \subsetneq \dots$ die nicht stationär wird ↯

(3)⇒(1): Sei $I \subset R$ ein Ideal. Wir betr.

$$M = \{ J \subset I \mid J \text{ endlich erzeugt} \} \neq \emptyset$$

Nach (3) existiert ein bzgl. Inklusion maximales Element.

$J^* \in M$, etwa $J^* = (a_1, \dots, a_n)$

Wäre $J^* \neq I$ dann ex. ein $a \in I \setminus J^*$ und $(a_1, \dots, a_n, a) \in M$ wäre ein größeres Ideal in $M \Rightarrow J^* = I$ und I ist damit endlich erzeugt.

Satz 4.18 (Hilbertsche Basissatz)

R noethersch $\Rightarrow R[x]$ noethersch.

<u>Kor. 4.19</u> $\mathbb{Z}[x]$, $K[x]$, $\mathbb{Z}[x_1, \dots, x_n]$, $K[x_1, \dots, x_n]$ (mit K Körper) sind noethersch.

<u>Bew:</u> · $\mathbb{Z}$ ist noethersch, da jedes Ideal von der Gestalt $n \cdot \mathbb{Z} = (n) = \{ k \cdot n \mid k \in \mathbb{Z} \}$ also sogar ein Hauptideal ist. In K gibt es nur die Ideale (0) und $(1) = K$.

Wegen $\underset{K}{\mathbb{Z}}[x_1, \dots, x_n] \cong \underset{K}{\mathbb{Z}}[x_1, \dots, x_{n-1}][x_n]$ folgt das Kor.

<u>Beweis von 4.18</u> Sei $I \subset R[x]$ ein Ideal

A: I nicht endl. erzeugt, also insbes. $I \neq 0$

Sei $f_1 \in I$ ein Element vom kleinsten Grad n_1 und sei a_1 der Leitkoeffizient von f_1.

$(f_1 = a_1 x^{n_1} + \text{Terme der Ordnung} < n_1)$

Wir wählen induktiv $f_k \in I \setminus (f_1, \dots, f_{k-1})$ vom kleinsten Grad n_k mit Leitkoeffizient a_k

Nach Konstruktion ist

$$(a_1) \subset (a_1, a_2) \subset \dots \subset (a_1, \dots, a_k) \subset \dots$$

eine aufsteigende Kette von Idealen in R und $n_1 \leq n_2 \leq \dots$

Da R noethersch ex. ein k mit

$$(a_1, \dots, a_k) = (a_1, \dots, a_k, a_{k+1}) = \dots$$

D.h. $a_{k+1} = \sum_{i=1}^{k} r_i a_i$ mit $r_i \in R$

Dann kürzt sich in $g := f_{k+1} - \sum_{i=1}^{k} r_i \cdot x^{n_{k+1} - n_i} \cdot f_i$ der Leitterm weg.

$g \in I \setminus (f_1, \dots, f_n)$ ist also ein Element vom kleineren Grad als f_{k+1}. Dies steht im Widerspruch zur Wahl von f_{k+1}

Man kann also kein Element f_{k+1} vom kleinsten Grad in $I \setminus (f_1, \dots, f_k)$ finden.

$\Rightarrow I = (f_1, \dots, f_k)$ $\square$