2.4.5 Def Ein euklidischer Ring ist ein paar (R,δ) mit R Integritätsring, $\delta: R\setminus\{0\}\to\mathbb{N}_0$: $\forall f\in R, g\in R\setminus\{0\}$ $\exists q\in R$ $f=qg+r$, $\delta(r)<\delta(g)$ oder $r=0$.

2.4.6 Bsp (i) $R=\mathbb{Z}$, $\delta(m)=|m|$ (ii) $R=K[X]$, K Körper mit $\delta(f)=\operatorname{grad} f$ (iii) $\mathbb{Z}[i]=\{x+iy : x,y\in\mathbb{Z}\}$ ("ganze Gauß'sche Zahlen") mit $\delta(x+iy)=|x+iy|^2=x^2+y^2$

Seien $f, g\neq 0$ gegeben. Sei $q\in\mathbb{Z}[i]$ mit minim. Abstand in $\mathbb{C}$ zu f/g. Kreise mit Zentren in $\mathbb{Z}[i]$ und Radius $\frac{1}{\sqrt{2}}$ überdecken $\mathbb{C}$ $\rightsquigarrow$ $B_{1/\sqrt{2}}(f/g)\cap\mathbb{Z}[i]\neq\phi \Rightarrow |q-\frac{f}{g}|\leq\frac{1}{\sqrt{2}}$

$r:=f-qg \Rightarrow |r|=|f-qg|=|\frac{f}{g}-q||g|\leq\frac{1}{\sqrt{2}}|g|<|g|$. ▣

2.4.7 Satz R euklidisch $\Rightarrow$ R Hauptidealring.
Insbesondere: K Körper $\Rightarrow$ $K[X]$ Hauptidealring.

Beweis. Sei $\mathfrak{a}\subset R$ Ideal. z.z. $\exists a\in R: \mathfrak{a}=(a)$.
OBdA $\mathfrak{a}\neq\{0\}$. Wähle $a\in\mathfrak{a}\setminus\{0\}$ mit $\delta(a)=\min\{\delta(b): b\in\mathfrak{a}\setminus\{0\}\}$.
Behauptung: $\mathfrak{a}=(a)$. In der Tat, sei $f\in\mathfrak{a}$. Division mit Rest $\rightsquigarrow$ $\exists q,r\in R$, $f=qa+r$, $\delta(r)<\delta(a)$ oder $r=0$. Nun $a\in\mathfrak{a}\Rightarrow qa\in\mathfrak{a}\Rightarrow r=f-qa\in\mathfrak{a}$. Wahl von a $\rightsquigarrow$ $r=0$.
Also $f=qa\in(a)$. ▣

2.4.8 Def. Ein Ring R heißt *noetersch*, falls jede aufsteigende Kette von Idealen $\mathfrak{a}_1\subset\mathfrak{a}_2\subset\dots$ in R wird stationär, d.h. $\exists n\in\mathbb{N}$ mit $\mathfrak{a}_i=\mathfrak{a}_n$ für alle $i\geq n$. (Emmy Noether, 1882-1935)

Bemerkung (i) R noetersch $\Leftrightarrow$ jedes Ideal $\subset R$ endlich erzeugt
(ii) Hilbertscher Basissatz: R noethersch $\Rightarrow$ $R[X]$ noethersch
(iii) Sei $T\subset\mathbb{C}[X_1,\dots,X_n]$ (allgemeiner $K[X_1,\dots,X_n]$, K alg. abgeschl.)
Sei $Z(T)=\{z\in\mathbb{C}^n: \forall P\in M; P(z)=0\}$; $Y\subset\mathbb{C}^n$ heißt affin-algebraisch, falls $\exists T\subset\mathbb{C}[X_1,\dots,X_n]$ mit $Y=Z(T)$.

Siehe 2.4.20

2.4.20

Z.B. $\{(z,w)\in\mathbb{C}^2 : w=z^2\}$, $\{(z,w)\in\mathbb{C}^2 : zw=0\}$

Für $Y\subset\mathbb{C}^n$ definiere $I(Y)=\{f\in K[X_1,\dots,X_n] : \forall z\in Y, f(z)=0\}$. das Ideal von Y. Es gibt eine bemerkenswerte Korrespondenz zwischen geom. Eig. von affin-alg. Teilmengen $Y\subset\mathbb{C}^n$ und algebraische Eig. deren Ideale $I(Y)$ (z.B. Y irred. $\Leftrightarrow$ $I(Y)$ prim)

(iv) Hilbertscher Nullstellensatz: Sei $\mathfrak{a}\subset\mathbb{C}[X_1,\dots,X_n]$, sei $P\in\mathbb{C}[X_1,\dots,X_n]$ mit $P|_{Z(\mathfrak{a})}=0$ i.e. $P\in I(Z(\mathfrak{a}))$
Dann $\exists r\in\mathbb{N}$ mit $P^r\in\mathfrak{a}$.

2.4.9 Lemma R Hauptidealring $\Rightarrow$ R noethersch

Beweis Seien $\mathfrak{a}_1\subset\mathfrak{a}_2\subset\dots$. Setze $\mathfrak{a}=\bigcup_{i\in\mathbb{N}}\mathfrak{a}_i$ $\rightsquigarrow$ $\mathfrak{a}$ Ideal
$\rightsquigarrow \exists a\in R: \mathfrak{a}=(a)$. $\rightsquigarrow \exists i: a\in\mathfrak{a}_i \Rightarrow \mathfrak{a}=(a)\subset\mathfrak{a}_i\subset\mathfrak{a}$
$\Rightarrow \mathfrak{a}=\mathfrak{a}_i$ ▤

2.4.10 Satz Sei R noethersch. Dann besitzt jedes $a\neq 0$, $a\notin R^*$ eine endliche Produktdarstellung von irred. Elem. Ist R Hauptidealring, so kann man irred durch prim ersetzen.

Beweis R noethersch $\Rightarrow$ jede nicht-leere Menge S von Idealen in R hat ein maximales Elem, d.h. $\exists\mathfrak{a}\in S$ mit $\mathfrak{a}\subset\mathfrak{b}\in S\Rightarrow\mathfrak{a}=\mathfrak{b}$. (Anderenfalls, wähle $\mathfrak{a}_1\in S$ bel., dann wähle $\mathfrak{a}_1\subsetneq\mathfrak{a}_2\in S$ usw. $\rightsquigarrow$ nicht stationäre Kette $\mathfrak{a}_1\subsetneq\mathfrak{a}_2\subsetneq\dots$ ↯)
Angenommen ist die Beh. 2.4.10 falsch. Sei
$S=\{(a) : a\in R\setminus\{0\}, a\notin R^*, a \text{ kein Prod. von irred. Elem}\}$
Sei $\mathfrak{a}=(a)$ ein maximales Elem; a ist nicht irred. $\rightsquigarrow$

$\rightsquigarrow$ $\exists b, c \notin R^*$: $a = bc \rightsquigarrow (a) \subsetneq (b), (c)$

(Wäre $(a) = (b)$, so $\exists u \in R^*$ $a = bu \rightsquigarrow bu = bc \overset{R \text{ Int.ring}}{\rightsquigarrow} u = c$ ↯)

(a) maximal $\Rightarrow$ (b), (c) $\notin S$ also sind b, c Prod. von irred. Elem

$\Rightarrow$ a ebenfalls ↯. ▤

2.4.11 Def Ein Ring R heißt faktoriell, wenn jedes $a \in R \setminus \{0\}$, $a \notin R^*$ Produkt von Primelem. ist.

Bsp. R Hauptidealring $\Rightarrow$ R faktoriell.

2.4.12 Lemma Sei R faktoriell. Dann gilt

(i) $p \in R$ irred $\Leftrightarrow$ $p \in R$ prim

(ii) Die Zerlegung ist eindeutig bis auf Reihenfolge und Assoziiertheit (:= Gleichheit mod R^*) von Faktoren

d.h. $a = p_1 \cdots p_r = q_1 \cdots q_s$ mit p_i, q_j prim $\Rightarrow r = s$ und nach evtl. Umordnung gilt $q_i = \varepsilon_i p_i$, $\varepsilon_i \in R^*$.

Beweis (i) „$\Rightarrow$" Zerl. in Primfaktoren hat nur ein Elem

„$\Leftarrow$" 2.4.2

(ii) $p_1 \cdots p_r = q_1 \cdots q_s \underset{p_1 \text{ prim}}{\Longrightarrow} \exists j : p_1 \mid q_j$. OBdA $j = 1$. Also

$\exists \varepsilon \in R$ mit $q_1 = \varepsilon p_1 \underset{q_1 \text{ irred}}{\Longrightarrow} \varepsilon \in R^*$. Aus $p_1 \cdots p_r = \varepsilon p_1 q_2 \cdots q_s$

$\overset{R \text{ Intring}}{\rightsquigarrow}$ $p_2 \cdots p_r = \underbrace{\varepsilon q_2}_{q_2' \text{ prim}} q_3 \cdots q_s$ Wir setzen das Verfahren fort

$\rightsquigarrow$ Behauptung ▤

2.4.13 Zusammenfassung

$\{K[X], K \text{ Körper}\} \subset \{\text{Euklidische Ringe}\} \subset \{\text{Hauptidealringe}\}$

$\{\text{noethersche Ringe}\}$ $\{\text{faktorielle Ringe}\}$

2.4.14 Bsp. (i) $\mathbb{Z}$ ist faktoriell; {Primelem} = {±Primzahlen}
$n \in \mathbb{Z}\setminus\{0,\pm1\} \rightsquigarrow n$ besitzt eine Zerlegung in Primzahlen eindeutig bis auf Reihenfolge und Vorzeichen.

(ii) $\mathbb{Z}[X]$ ist kein Hauptidealring (ist aber faktoriell nach dem Satz von Gauß 2.5.1). Betrachte das Ideal $(X,2) = \{a_0 + a_1 X + \dots + a_n X^n : n \in \mathbb{N}_0, a_i \in \mathbb{Z}, a_0 \text{ gerade}\}$; es wird nicht von einem Element erzeugt, da die einzigen gemeinsamen Teiler von X und 2 sind ± 1 und $(-1) = (1) = \mathbb{Z}[X]$.

2.4.15 Korollar Sei R faktoriell. Wähle ein Vertretersystem für die Primelementen, der aus jeder Klasse von assoziierten Primelem. genau eins enthält. Dann hat jedes $a \in R\setminus\{0\}$ eine eindeutige Zerlegung

$$a = \varepsilon \prod_{p \in P} p^{\nu_p(a)} \quad \text{mit } \varepsilon \in R^*,\ \nu_p(a) \in \mathbb{N}_0,\ \nu_p(a) = 0 \text{ für fast alle } p$$

$\nu_p(a)$ heißt die Vielfachheit von p in a.

(Z.B. in $\mathbb{Z}$, die Klassen sind $\{p,-p\}$, p prim und wir wählen $P := \{\text{positive Primelem}\} = \{\text{Primzahlen}\}$)

2.4.16 Def. Sei R Integritätsring, $x_1,\dots,x_n \in R$. Ein Elem $d \in R$ heißt ggT von $x_1,\dots,x_n$ falls: (i) $\forall i\ d \mid x_i$ (ii) $\forall d'\left(\forall i\ d' \mid x_i \Rightarrow d' \mid d\right)$
Ein Elem. $v \in R$ heißt kgV von $x_1,\dots,x_n$ falls:
(i) $\forall i\ x_i \mid v$ (ii) $\forall v'\left(\forall i\ x_i \mid v' \Rightarrow v \mid v'\right)$.

2.4.17 Bem. (1) Falls ggT oder kgV existieren, so sind sie eindeutig bis auf Assoziiertheit ($d = ad'$, $d' = bd \Rightarrow d = abd \Rightarrow ab = 1 \Rightarrow a,b \in R^*$)

(2) Ist R faktoriell, $x_i = \varepsilon_i \prod_{p \in P} p^{\nu_p(x_i)}$ $i = 1,\dots,n$, so

$$\mathrm{ggT}(x_1,\dots,x_n) = \prod_{p \in P} p^{\min\{\nu_p(x_1),\dots,\nu_p(x_n)\}},\quad \mathrm{kgV}(x_1,\dots,x_n) = \prod_{p \in P} p^{\max\{\nu_p(x_1),\dots,\nu_p(x_n)\}}$$