Disposition til

Algebra 2

Malthe Munk Karbo '14

18. juni 2017

INDHOLD

KAPITEL 1

HOMOMORFIER, IDEALER OG KVOTIENTRINGE

Taleplan

1. Ringhomomorfier, idealer og kvotientringe defineres,
2. Første isomorfisætning for ringe,
3. Fjerde isomorfisætning for ringe.

Beviser

Definition 1.1
En ringhomomorfi φ *mellem to ringe* R, S *er en funktion* $\varphi\colon R \to S$ *som opfylder:*

1. φ *er en gruppehomomorfi,*
2. φ *bevarer multiplikation, i.e., for alle* $a, b \in R$ *gælder der* $\varphi(ab) = \varphi(a)\varphi(b)$.

Definition 1.2
En delring $I \subseteq R$ *er et* (venstre- hhv. højre- hhv. tosidet-)ideal *hvis* $aI \subseteq I$ *hhv.* $Ia \subseteq I$ *hhv. begge to for alle* $a \in R$.

Definition 1.3
Lad R *være en ring med ideal* $I \subseteq R$, *da defineres* kvotientringen *til* $R/I := \{a + I | a \in R\}$. *Dette er en ring under naturlige operatoner.*

Proposition 1.4 (proposition 5 DF)
Hvis $\varphi\colon R \to S$ *er en ring homomorfi er* $\varphi(R)$ *en delring af* S *og* $\ker \varphi$ *er et ideal i* R.

Proposition 1.5 (1. isomorfisætning for ringe)
Hvis $\varphi\colon R \to S$ *er en ringhomomorfi mellem ringe* R *og* S *så er* $R/\ker(\varphi) \cong \varphi(R)$ *via* $\overline{r} \mapsto \varphi(r)$, $\overline{r} \in R/\ker(\varphi)$.

Ydermere, givet et ideal $I \subseteq R$, *så er afbildningen* $R \to R/I$, $r \mapsto [r]_I$ *en surjektiv ringhomomorfi med* $\ker = I$. *Altså er alle idealer lig kernen for en ring homomorfi.*

Bevis.
Pr. første isomorfisætning for grupper gælder der at afbildningen $\overline{\varphi}\colon R/\ker(\varphi) \to$

$\mathrm{Im}(\varphi)$, $[r]_{\ker(\varphi)} \mapsto \varphi(r)$ er en veldefineret isomorfi af grupper. Så der mangler kun at vise at den bevarer multiplikation. Lad $[a]_{\ker(\varphi)}, [b]_{\ker(\varphi)} \in R/\ker(\varphi)$, da har vi

$$\overline{\varphi}([ab]_{\ker(\varphi)}) = \varphi(ab) = \varphi(a)\varphi(b) = \overline{\varphi}([b]_{\ker(\varphi)})\overline{\varphi}([b]_{\ker(\varphi)})$$

Givet et ideal $I \subseteq R$, så er afbildningen $\pi\colon r \mapsto [r]_I$ en surjektiv gruppehomomorfi $R \to R/I$ pr. første isomorfisætning for grupper. Og hvis $r, s \in R$ da er

$$\pi(rs) = [rs]_I = [r]_I[s]_I = \pi(r)\pi(s),$$

så π er en surjektiv ringhomomorfi med $\ker(\pi) = I$. □

Proposition 1.6 (4. isomorfisætning for ringe)
For et ideal $I \subseteq R$, da giver tilordningen $A \mapsto A/I$ inklusionsbevarende bijektive korrespondancer:

$$\{\textit{Delringe af } R \textit{ som indeholder } I\} \to \{\textit{Delringe af } R/I\},$$
$$\{\textit{Idealer af } R \textit{ som indeholder } I\} \to \{\textit{Idealer af } R/I\}.$$

Bevis.
Fjerde isomorfisætning for grupper giver, da $(I, +)$ er en normal undergruppe af $(R, +)$, en inklusionsbevarende bijektive korrespondancer mellem additive undergrupper af R som indeholder I og additive undergrupper af R/I, så lad A være en gruppe med $I \subseteq A$.

1. Lad $a, b \in A$. Da er $[a]_I[b]_I = [ab]_I \in A/I \iff ab \in A$, så A er en ring hvis og kun hvis A/I er en ring.
2. Lad $a \in A$ og $r \in R$. Da er $[r]_I[a]_I = [ra]_I \in A/I \iff ra \in A$, så A er et ideal hvis og kun hvis A/I er et ideal.

□

Example 1.7
1. Afbildningen $\varphi\colon \mathbb{Z}[x] \to \mathbb{Z}$, $p(x) \mapsto p(0)$ er en ring-homomorfi med $\ker\varphi = (x)$, og $\mathrm{im}\varphi = \mathbb{Z}$ så sætningen ovenover giver $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$.
2. $n\mathbb{Z}$ er et ideal i $\mathbb{Z}$.
3. $(x) \subseteq \mathbb{Z}[x]$ ideal.

KAPITEL 2

MAKSIMALIDEALER OG PRIMIDEALER

Taleplan

1. Definering af maksimalidealer og primidealer.
2. Ethvert ægte ideal er indeholdt i et maksimalidealer.
3. R kommutativ ring, $M \subseteq R$ maksimalideal hvis og kun hvis R/M legeme.
4. R kommutativ ring, P primideal i R hvis og kun hvis R/P integritetsområde.

Beviser

Definition 2.1
For en ring R defineres $\mathcal{R} := \{I \subseteq R | I \text{ ideal i } R\}$. Dette er en partielt ordnet mængde ved inklusion.

Definition 2.2 (maksimal ideal)
Et ideal M i en ring R siges at være et maksimalideal hvis $M \neq R$ og M er maksimalt element i den partielt ordnede mængde $\mathcal{R}$ (i.e. $M \subset I$ medfører $I = M$ eller $I = R$).

Lemma 2.3 (zorns)
Hvis alle totalt ordnede delmængder i en partielt ordnet mængde $(A, \leq)$ har en øvre grænse, så har A et maksimalt element.

Proposition 2.4
Ethvert ægte ideal I i en ring R med enhed er indeholdt i et maksimalt ideal.

Bevis.
Lad $I \subseteq R$ være et ægte ideal i en ring R med enhed, så $1 \in R \Rightarrow R \neq 0$.

Lad $\mathcal{S} := \{S \in R \mid S \text{ ægte ideal med } I \subseteq S\}$. Da er $\mathcal{S}$ en ikke-tom (da $I \in \mathcal{S}$) partielt ordnet mængde ved inklusion. Lad $\mathcal{T}$ være en totalt ordnet delmængde (kæde) af $\mathcal{S}$, og definer

$$J := \bigcup_{T \in \mathcal{T}} T.$$

Da er J et ideal: $0 \in T$ for alle $T \in \mathcal{T}$ så $J \neq \emptyset$. Hvis $a, b \in J$, er der idealer $A, B \in \mathcal{T}$ med $a \in A$ og $b \in B$. Da $\mathcal{T}$ totalt-ordnet antager vi $A \subseteq B$. Så er $a, b \in B$ og $a+b \in B$ så $a + b \in J$. For $r \in R$ har vi

$$rJ = \bigcup_{T \in \mathcal{T}} \underbrace{rT}_{\subseteq T} \subseteq \bigcup_{T \in \mathcal{T}} T = J,$$

og tilsvarende er $Jr \subseteq J$, så J er et ideal i R.

Vi mangler blot at vise, at $J \in \mathcal{S}$. Hvis ikke, så er $J = R \iff 1 \in J \iff 1 \in T$ for et $T \in \mathcal{T}$, men det er antaget umuligt. Så J er en øvre grænse for $\mathcal{T}$, så zorns lemma sikrer eksistensen af et maksimalideal $M \in \mathcal{S}$. □

Proposition 2.5
Lad $I \subseteq R$ være et ideal i en ring R med $1 \neq 0$. Da gælder

1. *$I = R$ hvis og kun hvis I indeholder en enhed.*
2. *Hvis R er kommutativ, så er R er legeme hvis og kun hvis $\mathcal{R} = \{0, R\}$.*

Bevis.
(1): $I = R$ medfører $1 \in I$. Antag $u \in I$ er en enhed, så er $1 = u^{-1}u \in I$ så for alle $r \in R$ har vi $r = r \cdot 1 \in I$.

(2): R legeme hvis og kun hvis $R^\times = R \backslash \{0\}$. Lad $(0) \neq I$ være et ideal i R. Da er $I \cap R^\times \neq \emptyset$, så pr. (1) er $I = R$. Antag nu at de eneste idealer i R er 0 og R. Lad u være et vilkårligt element i $R \backslash \{0\}$. Per antagelse er $(u) = R$, så $1 \in (u)$, og derfor er der $u^{-1} \in R$ så $u^{-1}u = 1$. □

Proposition 2.6 (R komm ideal max iff kvotient legeme)
Lad R være en unital kommutativ ring. Da er et ideal M i R maksimalt hvis og kun hvis kvotientringen R/M er et legeme.

Bevis.
Per fjerde isomorfisætning er der en bijektiv korrespondance mellem idealer A i R som indeholder M og idealer A/M i R/M. Så M er maksimal hvis og kun hvis de eneste idealer i R/M lig R/M og (0) og per ovenstående sker dette hvis og kun hvis R/M et legeme. □

Definition 2.7
Et primideal P i en kommutativ ring R er et ægte ideal sådan at hvis $ab \in P$ så er $a \in P$ eller $b \in P$ for alle $a, b \in R$.

Proposition 2.8
Et ideal P i en kommutativ ring R er et primideal hvis og kun hvis R/P er et integritetsområde

Bevis.
For $a, b \in R$:

$$ab \in P \iff \overline{ab} = \overline{a}\overline{b} = 0$$

ses let nu. □

Proposition 2.9
For R kommutativ gælder: $M \subseteq R$ maksimal ideal medfører M primideal

Bevis.
M maksimalt $\iff$ R/M legeme $\implies$ at R/M integritetsområde $\iff$ M prim. □

Modsatte gælder ikke: $(x) \in \mathbb{Z}[x]$ prim men ikke maks ($\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ ikke legeme eller $(x) \subseteq (2, x) \subseteq \mathbb{Z}[x]$).

Example 2.10
1. $2\mathbb{Z}$ er maksimalt i $\mathbb{Z}$ men $4\mathbb{Z} \subseteq 2\mathbb{Z}$ er ikke.
2. $(2, x) \subseteq \mathbb{Z}[x]$ er maksimalt ($\mathbb{Z}[x]/(2, x) \cong \mathbb{Z}/2\mathbb{Z}$ som er et legeme)

KAPITEL 3

BRØKRINGE

Taleplan

1. Definering af en relation på $R \times D$ for kommutativ ring R og multiplikativt lukket mængde $D \subseteq R$.
2. Definition af brøkringen $D^{-1}R$.
3. Naturlig ring homomorfi $R \mapsto D^{-1}R$.
4. Brøkringens universalegenskab.

Beviser

Definition 3.1
En delmængde D af en kommutativ unital ring R siges at være multiplikativt lukket hvis $1 \in D$ og for all $d, d' \in D : dd' \in D$.

I det følgende er R en unital kommutativ ring, og $D \subseteq R$ er en multiplikativt lukket delmængde. (eks $R \backslash \mathfrak{P}$ hvor $\mathfrak{P}$ er et primideal, $R^{\times}$ mængden af enheder og lign.)

Definition 3.2
For multiplikativt lukket delmængde, $D \subseteq R$, defineres en relation $\sim$ på $R \times D$ til

$$(r, d) \sim (r', d') \iff \exists u \in D : rd'u = r'du$$

Dette er en ækvivalensrelation (kan vises), og vi annoterer $[(r, d)]_{\sim} := \frac{r}{d}$

Definition 3.3 (Brøkringen)
For multiplikativt lukket delmængde, $D \subseteq R$, defineres delmængden af ækvivalensklasser R mht. D til

$$D^{-1}R := \left\{ \frac{r}{d} \mid r \in R,\ d \in D \Big(\right\}$$

Dette kan vises at være en kommutativ unital ring med $0 := \frac{0}{1}$ og $1 := \frac{1}{1}$ og $(+, \cdot)$ defineret ved

$$\frac{r}{d} + \frac{s}{t} := \frac{rt + sd}{dt} \text{ og } \frac{r}{d}\frac{s}{t} := \frac{rs}{dt}.$$

(disse kan vises at være veldefinerede, i.e., uafhængige af valg af repræsentanter). I denne ring gælder de 'almindelige' regneregler for brøker fx forlængelse af brøker med elementer fra D.

Bemærk: hvis D ikke indeholder 0 eller nogen nuldivisorer, så er $\frac{r}{d} = 0 \iff r = 0$, og hvis $0 \in D$ så er $D^{-1}R = 0$-ringen.

Definition 3.4
Afbildningen $\rho\colon R \to D^{-1}R$, $r \mapsto \frac{r}{1}$ er 'den kanoniske ringhomomorfi til brøkringen'. Det er let at vise at det er en ringhomomorfi med $\rho(1) = 1$.

Pr bemærkningen: hvis D ikke indeholder 0 eller nogen nuldivisorer, da er ρ injektiv (kernen er nul).

Theorem 3.5 (brøkringens universalegenskab)
Den kanoniske ringhomomorfi $\rho\colon R \to D^{-1}R$ har følgende universalegenskab: For alle kommutative unitale ringe S og alle ringhomomorfier $\varphi\colon R \to S$ så $\varphi(D) \subseteq S^{\times}$ eksisterer $\tilde{\varphi}\colon D^{-1}R \to S$ så følgende diagram kommuterer:

$$\begin{tikzcd}
R \arrow[rr, "\varphi"] \arrow[dr, "\rho"'] & & S \\
& D \arrow[ur, "\tilde{\varphi}"'] &
\end{tikzcd}$$

Og den er givet ved $\tilde{\varphi}(\frac{r}{d}) = \varphi(r)\varphi(d)^{-1}$ for $\frac{r}{d} \in D^{-1}R$, og φ injektiv medfører $\tilde{\varphi}$ injektiv.

Bevis.
Først vises **entydighed**: Hertil bemærkes at $\frac{r}{d} = \frac{r}{1}(\frac{d}{1})^{-1} = \rho(r)\rho(d)^{-1}$. Så hvis $\tilde{\varphi}\colon D^{-1}R \to S$ er en unital ringhomomorfi så diagrammet kommuterer, da gælder $\tilde{\varphi}(\frac{r}{d}) = \tilde{\varphi}(\rho(r)\rho(d)^{-1}) = \varphi(r)\varphi(d)^{-1}$, så denne afbildning må være på den form.

Eksistensen: Vi skal blot vise denne afbildning er veldefineret. Lad $\frac{r}{d} = \frac{r'}{d'}$, sådan at $rd'u = r'du$ for et $u \in D$. Da $\varphi(D) \subseteq S^{\times}$, findes $\varphi(u)^{-1} \in S$, og har

$$\varphi(rd'u) = \varphi(r'du) \iff \varphi(r)\varphi(d)^{-1} = \varphi(r')\varphi(d')^{-1} \iff \tilde{\varphi}(\frac{r}{d}) = \tilde{\varphi}(\frac{r'}{d'}).$$

Det vises let at denne bevarer produkter og addition samt er unital.

Så vises **injektivitet**: Antag φ injektiv og at $\tilde{\varphi}(\frac{r}{d}) = 0 \iff \varphi(r)\varphi(d)^{-1} = 0$, så må $r = 0$ så $\frac{r}{d} = 0$, så $\ker(\tilde{\varphi}) = 0$. □

Example 3.6
1. Hvis $D = R\backslash\{0\}$ kaldes brøkringen $D^{-1}R$ for brøklegemet over R. For $\mathbb{Z}$ får vi $\mathbb{Q}$.
2. samme som ovenover: For $R = Z[x]$ får vi $Q[x]$, for $Q[x]$ får vi $Q[x]$ igen.

KAPITEL 4

DEN KINESISKE RESTKLASSESÆTNING

Taleplan

1. Produktring og komaksimalitet
2. Den kinesiske restklassesætning ($n = 2$)
3. Den kinesiske restklassesætning $n \geq 2$
4. En anvendelse.

her

Beviser

For en familie af ringe $(R_\alpha)_{\alpha \in A}$ kan man danne produktringen $\prod_{\alpha \in A} R_\alpha$ hvor addition og multiplikation sker indgangsvist. Fra nu af er R en kommutativ unital ring.

Definition 4.1
To idealer $I, J \subseteq R$ siges at være komaksimale hvis $I + J = R$, i.e., hvis der findes $x \in I$ og $y \in J$ så $x + y = 1$.

Eksempel: For $n, m \in \mathbb{Z}$ indbyrdesk primiske er $n\mathbb{Z} + m\mathbb{Z} = \mathbb{Z}$.

Proposition 4.2 (DKR n=2)
Givet idealer $I_1, I_2 \subseteq R$, da er afbildningen $\varphi\colon R \to R/I_1 \times R/I_2$ givet ved

$$r \mapsto ([r]_{I_1}, [r]_{I_2}), \quad r \in R$$

en ringhomomorfi med $\ker \varphi = I_1 \cap I_2$. *Hvis I_1 og I_2 er komaksimale er φ surjektiv og $I_1 \cap I_2 = I_1 I_2$ og*

$$R/(I_1 I_2) \cong R/I_1 \times R/I_2.$$

Bevis.
Det er oplagt en ringhomomorfi. Hvis $\varphi(r) = (0, 0)$ så er $r \in I_1$ og $r \in I_2$, så $\ker \varphi = I_1 \cap I_2$. Antag nu at I_1 og I_2 er komaksimale, og vælg $x \in I_1$ og $y \in I_2$ så $1 = x + y$. Da er $x = 1 - y$ og $y = 1 - x$ så $\varphi(x) = (0, 1)$ og $\varphi(y) = (1, 0)$. Så for $([r_1]_{I_1}, [r_2]_{I_2}) \in R/I_1 \times R/I_2$ har vi

$$\varphi(r_1 y + r_2 x) = \varphi(r_1)(1, 0) + \varphi(r_2)(0, 1) = ([r_1]_{I_1}, 0) + (0, [r_2]_{I_2}) = [r_1]_{I_1}, [r_2]_{I_2}).$$

Og der gælder generelt at $I_1 I_2 \subseteq I_1 \cap I_2$. Den modsatte inklusion vises ved: lad $c \in I_1 \cap I_2$, og lad $x \in I_1$ og $y \in I_2$ så $x + y = 1$. Så er

$$c = c \cdot 1 = c(x+y) = \underbrace{cx}_{\in I_1 I_2} + \underbrace{cy}_{\in I_1 I_2} \in I_1 I_2.$$

Ved første isomorfisætning har vi

$$R/I_1 \times R/I_2 \cong R/(I_1 \cap I_2) = R/(I_1 I_2).$$

□

I tilfældet med $I_1, I_2, \ldots, I_n$ idealer fås en generalisering

Proposition 4.3
Lad $I_1, I_2, \ldots, I_n \subseteq R$ være idealer. Da er afbildningen $\varphi\colon R \to R/I_1 \times \cdots \times R/I_n$ givet ved

$$r \mapsto ([r]_{I_j})_{1 \le j \le n}$$

en ringhomomorfi med $\ker \varphi = I_1 \cap I_2 \cap \cdots \cap I_n$. *Ydermere, hvis $I_1, I_2, \ldots, I_n$ er indbyrdes komaksimale er afbildningen surjektiv og $I_1 \cap I_2 \cap \cdots \cap I_n = I_1 I_2 \ldots I_n$ og der er en isomorfi*

$$R/(I_1 I_2 \ldots I_n) \cong R/I_1 \times R/I_2 \times \cdots \times R/I_n.$$

Bevis.
φ er klart en veldefineret homomorfi og

$$r \in \ker \varphi \iff [r]_{I_j} = 0 \ \forall 1 \le j \le n \iff r \in I_1 \cap \cdots \cap I_n.$$

Resten af beviset følger direkte hvis vi kan vise at I_1 og $I_2 I_3 \ldots I_n$ er komaksimale. Dette gøres ved induktion: gælder for $n = 2$ pr. ovenstående. Antag det gælder for $n > 2$ og lad $I_1, I_2, \ldots, I_{n+1}$ være indbyrdes komaksimale. For $2 \ge i \ge n+1$ vælges $x_j \in I_1$ og $y_j \in I_j$ så $x_j + y_j = 1$. Definer $J := I_2 I_3 \cdots I_{n+1}$ Så er

$$1 = \prod_{2 \le j \le n+1} (x_j + y_j) \in I_1 + y_2 y_3 \cdots y_{n+1} \subseteq I_1 + J.$$

Så I_1 og $J = I_2 I_3 \cdots I_{n+1}$ er komaksimale, så tilfældet $n = 2$ giver $I_1 I_2 \cdots I_{n+1} = I_1 \cap I_2 \cap \cdots \cap I_{n+1}$.

Vi mangler at vise at afbildningen $R \to R/I_1 \times R/I_2 \times \ldots R/I_{n+1}$ er surjektiv. lad $[b_i]_{I_i} \in R/I_i$ for $i = 1, 2, \ldots, n+1$. Pr. induktionsantagelsen findes $b \in R$ så $[b]_{I_i} = [b_i]_{I_i}$ for $i = 2, 3, \ldots, n+1$. Pr. n=2 findes også $a \in R$ så $[a]_{I_1} = [b_1]_{I_1}$ og $[a]_J = [b]_J$. Da har vi $a - b_j = \underbrace{(a-b)}_{\in J} + (b - b_j) \in J + I_j \subseteq I_j$ for $j = 2, 3, \ldots, n+1$. Så $[a - b_j]_{I_j} = [0]_{I_j} \iff [a]_{I_j} = [b_j]_{I_j}$ for $j = 2, 3, \ldots, n+1$. Så

$$a \mapsto ([a]_{I_1}, [a]_{I_2}, \ldots, [a]_{I_{n+1}}) = ([b_1]_{I_1}, [b_2]_{I_2}, \ldots, [b_{n+1}]_{I_{n+1}}).$$

□

Example 4.4
For $\mathbb{Z}$: Hvis $n_1, \ldots, n_k \in \mathbb{Z}$ er parvist primiske og $a_1, \ldots, a_k \in \mathbb{Z}$, da findes $x \in \mathbb{Z}$ så $x \equiv a_i \bmod n_i$ for $1 \leq i \leq k$. Eksempel: $n_1 = 3$ og $n_2 = 10$, da får vi $\mathbb{Z}/30\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$, via $[n]_30 \mapsto ([n]_3, [n]_10$ med invers $([a]_3, [b]_{10}) \mapsto [10a - 9b]_{30}$. Så hvis vi vil løse

$$x \cong 2\ |3$$
$$x \cong 6\ |10$$

har vi $x = 10 \cdot 2 - 9 \cdot 6 = -34$, så alle løsningerne er lig -34 mod 30, altså $x = \ldots, -94, -64, -34, -4, 26, 56, \ldots$.

KAPITEL 5

EUKLIDISKE RINGE

Taleplan

1. Definition af euklidiske ringe (og få eksempler)
2. Euklidisk $\implies$ PID
3. Euklids algoritme samt GCD
4. GCD =rest fra euklids algoritme

Beviser

I det følgende antages R at være et integritetsområde (kommutativ uden nuldivisorere)

Definition 5.1
En funktion $N\colon R \to \mathbb{N}_0$ *med* $N(0) = 0$ *kaldes en* norm *på integritetsområdet* R. *Hvis* $N(a) > 0$ *for* $a \neq 0$ *kaldes* N *en positiv norm.*

Definition 5.2
Et integritetsområde R *siges at være* Euklidisk *hvis der er en norm* N *på* R *så for alle* $a, b \in R$ *hvor* $b \neq 0$ *findes elementer* $q, r \in R$ *så*

$$a = qb + r \qquad \text{hvor } r = 0 \text{ eller } N(r) < N(b).$$

Example 5.3
Følgende er eksempler på euklidiske ringe:

1. Ethvert legeme: $N = 0$, har $a = ab^{-1}b$ for $b \neq 0$.
2. De hele tal $\mathbb{Z}$: $N = \|\cdot\|$: For $b \neq 0$, antag $b > 0$. Da $\mathbb{Z} = \cup_{n\in\mathbb{Z}}[nb, (n+1)b[$ findes der givet $a \in \mathbb{Z}$ et $k \in \mathbb{Z}$ så $a \in [kb, (k+1)b[$. Sættes $r := a - kb \in [0, b[$ har vi $a = kb + r = kb + a - kb$ og $|r| < |b|$. For $b < 0$ er $-b > 0$.
3. De Gaussiske heltal $\mathbb{Z}[i]$ med $N = \|\cdot\|^2$ (skitse).

Definition 5.4 (Hovedidealområde (PID))
Et hovedidealområde (PID) er et integritetsområde R *hvori de eneste ægte idealer er idealerne frembragt af enkelte elementer, i.e.* $I \subseteq R$ *ideal og* $(0) \neq I \neq R \implies I = (a)$ *for et* $a \in R\backslash\{0\}$.

Proposition 5.5 (euklid => PID)
Hvis R er en euklidisk ring så er R et integritetsområde.

Bevis.
Lad I være et ideal i R. Hvis $I = (0)$ er vi færdige. Antag $I \neq (0)$. Lad $0 \neq d \in I$ sådan at $N(d) \leq N(a)$ for alle $0 \neq a \in I$. Da er $(d) \subseteq I$. Lad $a \in I$. Da er $a = qd + r$ med $N(r) < N(d)$. Da $N(d) \leq N(a)$ for $a \neq 0$ må $r = 0$ så $a = qd$ derfor er $a \in (d)$. □

Theorem 5.6 (Euklids algoritme)
I en euklidiske ring R med norm N, så givet $a \in R$, $0 \neq b \in R$, da findes $q_0, \ldots, q_n, q_{n+1} \in R$ og $r_0, \ldots, r_n \in R$ så

$$
\begin{aligned}
a &= q_0 b + r_0, r_0 \neq \quad 0 \text{ og } N(r_0) < N(b) && (0)\\
b &= q_1 r_0 + r_1, r_1 \neq \quad 0 \text{ og } N(r_1) < N(r_0) && (1)\\
r_0 &= q_2 r_1 + r_2, \quad r_2 \neq 0 \text{ og } N(r_2) < N(r_1) && (2)\\
&\vdots\\
r_{n-2} &= q_n r_{n-1} + r_n, \quad r_n \neq 0 \text{ og } N(r_n) < N(r_{n-1}) && (\text{n})\\
r_{n-1} &= q_{n+1} r_n && (\text{n+1})
\end{aligned}
$$

Bevis.
For $(a, b) \in R \times R \backslash \{0\}$ findes $q, r \in R$ så

$$a = qt + r \text{ hvor } r = 0 \text{ eller } N(r) < N(b).$$

successivt opnås følger $q_0, q_1, \ldots$ og $r_0, r_1, \ldots$ som opfylder (0),(1),..., og sådan at følgen $N(r_i)$ aftager i $\mathbb{N}_0$, derfor er følgen 0 fra et vist $n + 1 \in \mathbb{N}$. □

Example 5.7
Lad $R = \mathbb{Z}$ og $a = 100, b = 6$. Da har vi

$$
\begin{aligned}
a = 100 &= 16 \cdot 6 + 4\\
4 &= 4 \cdot 1 + 0,
\end{aligned}
$$

så $r_0 = 4$, $q_0 = 16$ og $q_1 = 1$ og $r_1 = 0$.

Definition 5.8
For $a, b \in R$, hvor R er et integritetsområde siger vi at b går op i a ($b \mid a$) hvis der findes $x \in R$ så $a = bx$, eller ækvivalent, hvis $(a) \subseteq (b)$.

Definition 5.9 (GCD)
For $a, b \in R$, så siges et element $d \in R$ at være største fælles divisor for a og b hvis:

1. *$d \mid a$ og $d \mid b$, eller ækvivalent, $(a) \subseteq (d)$ og $(b) \subseteq (d)$.*

2. *$d' \mid a$ og $d' \mid b$ medfører $d' \mid d$ eller ækvivalent $(a) \subseteq (d)$ og $(b) \subseteq (d)$ medfører $(d) \subseteq (d')$.*

I dette tilfælde sættes $d := gcd(a, b)$.

Proposition 5.10
For $a, b \in R$ vil $(a, b) = (d)$ medføre, at $d = gcd(a, b)$ og der findes $x, y \in R$ så $d = ax + by$.

Bevis.
da $d \in (a, b)$ findes der (pr. definition) $x, y \in R$ så $d = ax + by$. Vi har også $(a), (b) \subseteq (a, b) = (d)$ så pr. definition vil $d \mid a$ og $d \mid b$. Hvis der findes d' så $(a) \subseteq (d')$ og $(b) \subseteq (d')$ da vil $(d) = (a, b) \subseteq (d')$ så $d' \mid d$. □

Nemt korollar

Corollary 5.11
R PID medfører at $gcd(a, b)$ findes for alle $a, b \in R$.

Theorem 5.12
For en euklidisk ring R, med $a \in R$ og $b \in R \backslash \{0\}$, da vil slut elementet r_n af euklids algoritme

$$a = q_0 b + r_0, r_0 \neq \quad 0 \text{ og } N(r_0) < N(b) \tag{0}$$
$$b = q_1 r_0 + r_1, r_1 \neq \quad 0 \text{ og } N(r_1) < N(r_0) \tag{1}$$
$$r_0 = q_2 r_1 + r_2, \quad r_2 \neq 0 \text{ og } N(r_2) < N(r_1) \tag{2}$$
$$\vdots$$
$$r_{n-2} = q_n r_{n-1} + r_n, \quad r_n \neq 0 \text{ og } N(r_n) < N(r_{n-1}) \tag{n}$$
$$r_{n-1} = q_{n+1} r_n \tag{n+1}$$

være $gcd(a, b)$, altså $(a, b) = (r_n)$.

Bevis.
Sæt $r_{-2} := a$, $r_{-1} := b$ og $r_{n+1} := 0$. Da er

$$r_{i-2} = q_i r_{i-1} + r_i, \quad \text{for alle } i = 0, \dots, n+1$$

sådan at $(r_{i-2}, r_{i-1}) = (r_{i-1}, r_i)$ for alle $i = 0, \dots, n+1$, sådan at

$$(a, b) = (r_{-2}, r_{-1}) = (r_{-1}, r_0) = \cdots = (r_{n-1}, r_n) = (r_n, r_{n+1}) = (r_n)$$

da $r_{n+1} = 0$. □

KAPITEL 6

HOVEDIDEALOMRÅDER (PID)

Taleplan

1. Definition af hovedidealområder (PID'er) samt nogle eksempler
2. I hovedidealområde findes $gcd(a, b)$ for alle a, b og $gcd(a, b) = ax + by$
3. Ikke-nul primidealer i hovedidealområder er maksimalidealer
4. integritetsområde + D-H norm => hovedidealområde.

Beviser

R integritetsområde.

Definition 6.1 (Hovedidealområde (PID))
Et hovedidealområde (PID) er et integritetsområde R hvori de eneste ægte idealer er idealerne frembragt af enkelte elementer (hovedidealer), i.e. $I \subseteq R$ ideal og $(0) \neq I \neq R \implies I = (a)$ for et $a \in R \backslash \{0\}$.

Definition 6.2 (GCD)
For $a, b \in R$, så siges et element $d \in R$ at være største fælles divisor for a og b hvis:

1. *$d \mid a$ og $d \mid b$, eller ækvivalent, $(a) \subseteq (d)$ og $(b) \subseteq (d)$.*
2. *$d' \mid a$ og $d' \mid b$ medfører $d' \mid d$ eller ækvivalent $(a) \subseteq (d)$ og $(b) \subseteq (d)$ medfører $(d) \subseteq (d')$.*

I dette tilfælde sættes $d := gcd(a, b)$.

Proposition 6.3
For $a, b \in R$ vil $(a, b) = (d)$ medføre, at $d = gcd(a, b)$ og der findes $x, y \in R$ så $d = ax + by$.

Bevis.
da $d \in (a, b)$ findes der (pr. definition) $x, y \in R$ så $d = ax + by$. Vi har også $(a), (b) \subseteq (a, b) = (d)$ så pr. definition vil $d \mid a$ o.g $d \mid b$. Hvis der findes d' så $(a) \subseteq (d')$ og $(b) \subseteq (d')$ da vil $(d) = (a, b) \subseteq (d')$ så $d' \mid d$. $\square$

Corollary 6.4
R PID medfører at $\gcd(a, b)$ findes for alle $a, b \in R$.

Proposition 6.5 (prim ideal er maksimalt i hovedidealområde)
Lad (p) være et ikke-nul primideal i et hovedidealområde R. Da er (p) maksimalt.

Bevis.
Antag (m) er et ideal som indeholder (p) med $(m) \neq R$. Da er $p \in (m)$, så der er $sr \in R$ så $p = rm$, så $rm = p \in (p)$. Da (p) er et primideal er $r \in (p)$ eller $m \in (p)$. Hvis $m \in (p)$ er $(m) = (p)$ så antag at det er $r \in (p)$. Da er $r = ps$ for et $s \in R$, og vi har

$$p = rm = psm \implies sm = 1,$$

så m er en enhed så $(m) = R$ □

Og den modsatte gælder altid: R kommutativ og M maksimaltideal i R medfører M primideal (R/M legeme => integritet iff prim).

Definition 6.6
En norm N er en Dedekind-Hasse norm hvis N er positiv og for alle ikke-nul $a, b \in R$ holder det at enten er $a \in (b)$ eller der er et ikke-nul element i $r \in (a, b)$ med $N(r) < N(b)$ (altså enten $b \mid a$ eller $\exists s, t \in R$ så $0 < N(sa - tb) < N(b)$).

Proposition 6.7
Et integritetsområde R med en D-H norm N er et hovedidealområde.

Bevis.
Antag I er et ikke-nul ideal i R og $0 \neq b \in I$ med $N(b)$ minimalt ($N(a) \geq N(b)$ for alle $0 \neq a \in I$). Lad $0 \neq a \in I$, da er $(a, b) \subseteq I$. Da vil $(a) \in (b)$, for ellers ville der være $sa - tb \in (a, b) \subseteq I$ så $N(as - tb) < N(b)$, men $N(b)$ er antaget mindst muligt, heraf får vi $I \subseteq (b)$, så $I = (b)$. □

KAPITEL 7

FAKTORIELLE RINGE (UFD)

Taleplan

1. Definition af faktorielle ringe (UFD)
2. Eksempler
3. PID => faktoriel ring

Beviser

Lad R være et integritetsområde (kommutativt med enhed uden nul-divisorere).

Definition 7.1
R integritetsområde:

1. *Lad $r \in R$ være en ikke-enhed og et ikke-nul element. Så er r* irreducibel *i R hvis $r = ab$, $a, b \in R$ medfører a eller b er enhed.*
2. *Et ikke nul-element $p \in R$ er et* primelement *hvis (p) er et prim ideal. (tænk $p \mid ab$ medfører $p \mid a$ eller $p \mid b$).*
3. *$a, b \in R$* associerer *hvis $a = bu$ for en enhed $u \in R$, skriver $a \overset{asc}{\sim} b$.*
4. *$p \in R$ prim $\implies$ p irreducibel*

I PID ring R: $r \in R \implies r$ primelement.

Definition 7.2 (faktorielle ringe (UFD))
Et faktoriel ring (UFD) et et integritetsområde R sådan at alle ikke-enheder $0 \neq r \in R \backslash R^{\times}$ opfylder følgende:

1. *r kan skrives som et endeligt produkt af irreducerbare elementer $p_i \in R$, i.e., $r = p_1 p_2 \cdots p_n$.*
2. *Ovenstående dekomposition er entydig op til associerede: $r = q_1 q_2 \cdots q_m$ medfører $n = m$ og man kan få $p_i \overset{asc}{\sim} q_i$ ved om-nummerering.*

Example 7.3
Eksempler omfatter bl.a. $\mathbb{Z}$ eller alle legemer F samt $F[x]$ (dette følger af nedestående samt UFD iff polynomie ring UFD)

Proposition 7.4 (PID => faktoriel ring (UFD))
Alle hovedidealområder (PID) er faktorielle ringe (UFD).

Bevis.
Lad R være et hovedidealområde og $r \in R$ være ikke-nul og ikke-enhed. Hvis r er irreducibel er vi færdige. Antag for modstrid, at r er reducerbar, men r ikke er et produkt af endeligt mange irreducerbare. Da har vi for $k \geq 2$ at vi kan skrive $r = \prod_{i \geq 1}^{k} r_i^k$ med i hvert fald r_k^k en reducerbar ikke-enhed for $2 \leq k$, måske flere. Dette giver en følge hvis $r_1^1 := r$.

Antag for simpeltheds skyld at for $k > 2 \in \mathbb{N}$ er $r_i^k = r_i^{k-1}$ for $1 \leq i < k-1$, så bogens eksempel genskabes, i.e.,

$$\begin{aligned} r = r_1^2 r_2^2 &= r_1 r_2 \\ r_1^3 r_2^3 r_3^3 &= r_1 r_{21} r_{22} \\ r_1^4 r_2^4 r_3^4 r_4^4 &= r_1 r_{21} r_{221} r_{222} \\ r_1^5 r_2^5 r_3^5 r_4^5 r_5 &= r_1 r_{21} r_{221} r_{2221} r_{2222} \end{aligned}$$

For hvert $k \geq 2$ vælg da $r_k := r_k^k \in (r_i^k)_{i=1}^k$ sådan at vi får en strengt-voksende følge af idealer i R, altså:

$$(r) \subset (r_2) \subset (r_3) \subset \cdots \subset R$$

Dette kan ikke ske! Givet en voksende kæde af idealer i R, $I_1, I_2, \ldots$ vil der være $n \in \mathbb{N}$ så $I_k = I_n$ for $k \geq n$: Lad $I_1 \subset I_2 \subset \cdots \subset R$ være en voksende kæde af ægte idealer, og definer idealet $I := \cup_{i \geq 1} I_i$. Da R er PID er $I = (a)$ for et $a \in I_n$ for et n. Men da har vi $I_n \subset I = (a) \subset I_n$. Så $I = I_n$, så $I_k = I_n$ for $k \geq n$. Derfor må processen ovenover terminerer, sådan at vi får en endelig dekomposition af r ved irreducible.

Nu vises entydighed af dekompositionen op til association: Lad n være antallet af irreducible faktorer i dekompositionen for r. Hvis $n = 0$ er r enhed. Antag $n \geq 1$ og at det er sandt for $n - 1$. Lad

$$r = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m \quad m \geq n,$$

hvor q_i og p_j er irreducible. Her tillades $q_i = p_j$. Da p_1 er irreducible og R er PID er p_1 et primelement så $p_1 \mid q_1 q_2 \cdots q_m$, så $p_1 \mid q_1$ (ved omrokering af q_i'erne). Så er $q_1 = p_1 u$ for en enhed u, da q_1 er irreducibel. Så har vi ved at fjerne p_1 fra begge sider

$$p_2 p_3 \cdots p_n = u q_2 q_3 \cdots q_m.$$

Pr. induktionsantagelsen er $p_i \overset{asc}{\sim} q_i$ for $2 \leq i \leq n$ ved passende omrokering. Hvis $m > n$, da findes en enhed u så, ved at fjerne venstre siden ovenover:

$$1 = u q_{n+1} q_{n+2} \cdots q_m$$

Altså er $q_{n+1} q_{n+2} \cdots q_m = u^{-1}$ hvorfor $m = n$. $\square$

KAPITEL 8

FAKTORISERING I DE GAUSSISKE HELTAL.

Taleplan

1. Definition af Gaussiske Heltal og Field-norm.
2. Kriterie for irreducibel i $\mathbb{Z}[i]$
3. Et lemma om primtalsform
4. Sætning om primtal=sum af to kvadrater
5. De irreducible elementer i $\mathbb{Z}[i]$

Beviser

Definition 8.1
*De **Gaussiske heltal** $\mathbb{Z}[i]$ er mængden $\{a + ib \mid a, b, \in \mathbb{Z}\} \subseteq \mathbb{C}$. De er udstyret med en **Field-norm**: $N: \mathbb{Z}[i] \to \mathbb{N}_0$, $a + ib \mapsto a^2 + b^2 = (a + ib)(a - ib)$. Enhederne er $\{\pm 1, \pm i\}$ (et element x er enhed hvis og kun hvis $N(x) = \pm 1$). Den er **Euklidisk** og derfor **PID** og derfor **UFD**.*

Hvis $\alpha \in \mathbb{Z}[i]$ opfylder $N(\alpha) = \pm p$ hvor p er et primtal, da er α irreducibel: Lad $\alpha = by$ for $b, y \in \mathbb{Z}[i]$. Da field-normen N er multipliktiv får vi

$$\pm p = N(\alpha) = N(by) = N(b)N(y)$$

Hvorfor vi får

$$N(b) = \pm p \text{ og } N(y) = \pm 1 \text{ eller } N(y) = \pm p \text{ og } N(b) = \pm 1$$

Så enten b eller y er enhed, så α er reducibel.

Det følgende lemma kan bevises:

Lemma 8.2
Et primtal $p \in \mathbb{Z}$ deler et heltal $n^2 + 1$ hvis og kun hvis $p = 2$ eller $p \equiv 1 \bmod 4$.

En kort bemærkning: Alle tal $n \in \mathbb{Z}$ opfylder $n^2 \equiv 0, 1 \bmod 4$. Thi hvis n er lige er $n = 2m$ for et $m \in \mathbb{Z}$ og så har vi $n^2 = 4m^2 \equiv 0 \bmod 4$. Hvis n ulige er $n = 2m + 1$ for $m \in Z$ og så er $n^2 = (2m + 1)^2 = 4(m^2 + m) + 1 \equiv 1 \bmod 4$.

Theorem 8.3 (Fermats sum of square theorem)
Et primtal p er summen af to kvadrater, $p = a^2 + b^2$ for $a, b \in \mathbb{Z}$ hvis og kun hvis $p = 2$ eller $p \equiv 1 \mod 4$. Og a, b er entydige op til fortegn og at bytte plads.

Bevis.
Hvis $a^2 + b^2 = p = c^2 + d^2$ i $\mathbb{Z}$ er $N(a + ib) = p = N(c + id)$ i $\mathbb{Z}[i]$. Da er $N(a + ib)$ et primtal, så $a + ib$ er irreducibel, samme gælder for $a - ib$ og $c + id$ og $c - id$. Ergo er

$$\begin{aligned}
a + ib &= \pm 1(c + id) = \pm c + (\pm d)i \text{ eller} \\
a + ib &= \pm i(c + id) = \mp d + (\pm c)i \text{ eller} \\
a + ib &= \pm 1(c - id) = \dots
\end{aligned}$$

Så entydigheden holder. Hvis $p = 2$ er $p = 1^2 + 1^2$ og vi er færdige.

$\Longrightarrow$: Antag $p > 2$ og $p = a^2 + b^2$ for $a, b \in \mathbb{Z}$. Da er $p \equiv 0, 1, 2 \mod 4$ pr. bemærkningen ovenover ($b^2, a^2 \equiv 0$ eller $1 \mod 4$). Da p er ulige må $p \equiv 1 \mod 4$.

$\Longleftarrow$: Antag $p > 2$ og $p \equiv 1 \mod 4$. Da har vi pr. lemma'et tidligere at $p \mid n^2 + 1$ i $\mathbb{Z}$ for et $n \in \mathbb{Z}$. Så har vi

$$p \mid n^2 + 1 = (n + i)(n - i) \in \mathbb{Z}[i].$$

Hvis p er irreducibel (og derfor primelement) i $\mathbb{Z}[i]$, da vil $p \mid n + i$ eller $p \mid n - i$ i $\mathbb{Z}[i]$, hvilket det ikke kan. Derfor er p reducibel, så $p = (a + ib)(c + id)$. Da $N(p) = p^2$ må $N(c + id) = N(a + ib) = p$, men så har vi $N(a + ib) = a^2 + b^2 = p$. □

Theorem 8.4
Op til association er de irreducible elementer i $\mathbb{Z}[i]$:

1. $1 + i$
2. *primtal p, $p \equiv 3 \mod 4$*
3. *elementerne af formen $a \pm ib$ med $a^2 + b^2 = p$, p primtal med $p \equiv 1 \mod 4$.*

Bevis.
Først $\Longrightarrow$:

(1): Vi har $N(1 + i) = 2$ så pr. tidligere argument er det irreducibelt.

(2): Kontraposition: Lad p være et reducibelt primtal. Da har vi $p = \alpha\beta$, hvor $\alpha = \alpha_1 + i\alpha_2$ og $\beta = \beta_1 + i\beta_2$ og $N(p) = p^2$ medfører $N(\alpha) = p = N(\beta)$, så $p = \alpha_1^2 + \alpha_2^2$, men, igen pr. tidligere argument, er $p = \alpha_1^2 + \alpha_2^2 \not\equiv 3 \mod 4$.

(3): Hvis $a + ib$ opfylder $a^2 + b^2 = p$, hvor p er et primtal med $p \equiv 1 \mod 4$ har vi pr. tidligere argument at $a + ib$ er irreducibelt i $\mathbb{Z}[i]$.

Så $\Longleftarrow$: Lad $\pi \in \mathbb{Z}[i]$ være et irreducibelt (og derfor primelement). Da er $P := Z \cap (\pi)$ prim ideal i $\mathbb{Z}$, som er et hovedidealområde, så $P = (p)$ for et primelement i $\mathbb{Z}$. Da har vi $p \in (p) \subseteq (\pi)$ i $\mathbb{Z}[i]$ så $p = k\pi$ for $k \in \mathbb{Z}[i]$. Vi har nu tre tilfælde for p:

1. Hvis $p = 2$ er $p = (1+i)(1-i) = (-i)(1+i)^2$, som er irreducibelt, altså er $\pi \overset{asc}{\sim} (1+i)^2$.
2. Hvis $p \equiv 3 \bmod 4$ er p irreducibelt i $\mathbb{Z}[i]$ pr ovenstående. Så $\pi \overset{asc}{\sim} p$.
3. Hvis $p \equiv 1 \bmod 4$ er, pr. fermats sum of square theorem, $p = (a+ib)(a-ib)$, hvor både $(a-ib), (a+ib)$ er irreducible, så $\pi \overset{asc}{\sim} a+ib$ eller $a-ib$.

$\square$

KAPITEL 9

FAKTORIELLE POLYNOMIUMSRINGE

Taleplan

1. Kort genopfriskning af polynomiumsringen $R[x]$
2. R integritetsområde $\implies$ $R[x]$ integritetsområde og $R^\times = R[x]^\times$
3. Definition af primitiv
4. Lemmaer: 1.1 og Gauss om primelementer og primitive elemente i $R[x]$.
5. Theorem: R UFD $\implies$ $R[x]$ UFD.

Beviser

I det følgende er R et integritetsområde. Da har vi

1. $R[x]$ er et integritetsområde
2. Polynomiumsringen $R[x]$ har de samme enheder som R, altså $R[x]^\times = R^\times$
3. $\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$ for $f, g \neq 0$.
4. For et ideal $I \subseteq R$ har vi, hvis $I[x]$ er idealet frembragt af I i $R[x]$, at $R[x]/I[x] \cong (R/I)[x]$.
5. Hvis $p \in R$ er primelement da er $p \in R[x]$ også et primelement, i.e. $(p) \subseteq R$ primideal $\implies$ $(p)[x] \subseteq R[x]$ primideal.

Note: For R UFD (faktoriel) så eksisterer GCD altid.

Definition 9.1 (primitive polynomier)
For R UFD ring, da siges et polynomium $f(x) = \sum_{i\geq 0} a_i x^i$ siges at være primitivt *hvis $gcd(f(x)) := gcd(a_i) \in R^\times$, altså største fælles divisor for koefficienterne i $f(x)$ er en enhed.*

Note: For R UFD: $f(x) \in R[x]$ er ikke-primitivt hvis og kun hvis der er irreducibelt (eller prim) element $p \in R$ så $p \mid f(x)$ i $R[x]$.

Følgende lemmaer gælder for R UFD:

Lemma 9.2 (Gauss)
For R UFD og $f(x), g(x) \in R[x]$ gælder:

$$f(x)g(x) \text{ primitivt} \iff f(x) \text{ og } g(x) \text{ primitive.}$$

Bevis.
skitse: For $\implies$: Antag $f(x) \in R[x]$ ikke primitivt, da findes irreducibel $p \in R$ så $p \mid f(x)$ så $p \mid f(x)g(x)$

For $\impliedby$: Antag $f(x)g(x)$ ikke primitivt. Da findes irreducibel (primelement) $p \in R$ så $p \mid f(x)g(x)$ i $R[x]$. Da p også primelement i $R[x]$ må $p \mid f(x)$ eller $p \mid g(x)$, altså er en af dem er ikke-primitiv. □

Der gælder også følgende lemma:

Proposition 9.3
Hvis R UFD med brøklegeme F, og $c \in F$. Lad $f(x) \in R[x]$. Hvis $cf(x) \in R[x]$ og er primitivt, da er $c = \frac{1}{u}$ for $u \neq 0$ i R. Hvis $f(x)$ selv er primitivt, da er u enhed og vi har $c = u^{-1} \in R$.

Bevis.
Skriv $c = \frac{r}{s}$ sådan at $gcd(r, s) = 1$ og $s \neq 0$. Lad $f(x) = a_0 + a_1x + \dots$. Da er $cf(x) = \frac{ra_0}{s} + \frac{ra_1}{s}x + \dots$, altså koefficienterne er $c_i := \frac{a_i r}{s}$. Så $s \mid ra_i$, og $gcd(r, s) = 1$ medfører $s \mid a_i$. Da $c_i = r\frac{a_i}{s}$ må $r \mid c_i$ i R. Antagelsen $cf(x)$ er primitivt, så r må være en enhed, så $c = \frac{r}{s} = \frac{1}{sr^{-1}}$ hvor $sr^{-1} \in R$.

Da $cf(x) = \frac{1}{u}f(x) \in R[x]$ må $u \mid a_i$. Så hvis $gcd(a_1, a_2, \dots) = 1$ må u være en enhed, altså hvis $f(x)$ primitivt er u enhed. □

Vi har også sætning:

Theorem 9.4
For R UFD med brøklegeme F med $f(x) \in R[x]$ gælder:

1. *For $\deg(f(x)) = 0$: $f(x)$ irreducibel i $R[x] \iff f(x)$ irreducibel i R.*
2. *For $\deg(f(x)) > 0$: $f(x)$ irreducibel i $R[x] \iff f(x)$ primitiv i $R[x]$ og irreducibel i $F[x]$.*

Vi har lemma:

Lemma 9.5
For R UFD: ethvert ikke-nul og ikke-enhed primitivt polynomium $f(x) \in R[x]$ med $\deg f(x) > 0$ har en irreducibel opløsning i $R[x]$.

Bevis.
Vi gør det ved induktion over $n = \deg f(x)$:

For $n = 1$: Da $\deg f(x) = 1$ er $f(x)$ irreducibel i $F[x]$ (for $f(x) = g(x)h(x)$ medfører $1 = \deg(f(x)) = \deg(g(x)) + \deg(h(x))$ så enten $g(x)$ eller $h(x)$ er konstante i $F[x]$, og i legemet F er konstante polynomier enheder), og da $f(x)$ ogs er antaget primitiv i er det derfor irreducibel i $R[x]$ (ovenstående sætning (2)).

For $n > 1$: Hvis $f(x)$ er irreducibelt i $R[x]$ er vi færdige. Antag ikke og lad $f(x) = g(x)h(x)$ være en faktorisering af irreducible $g(x), h(x) \in R[x]$. Da $f(x)$ er primitiv har vi pr. gauss at $g(x)$ og $h(x)$ er primitive i $R[x]$, og da de ikke er enheder må $\deg(h(x)), \deg(g(x)) > 0$. Da har vi

$$n = \deg(f(x)) = \deg(h(x)) + \deg(g(x)) \implies \deg(h(x)), \deg(g(x)) < n$$

Så pr. induktionsantagelsen har de begge en irreducibel opløsning i $R[x]$, hvorfor deres produkt må være en irreducibel opløsning for $f(x)$ i $R[x]$. □

Lemma 9.6
For integritetsområde R er primopløsninger entydige op til associering.

Proposition 9.7
R UFD medfører $R[x]$ UFD

Bevis.
To dele: **Eksistens og entydighed op til asociation**.

Eksistens: Lad $f(x) \in R[x]$ være $\neq 0$ og ikke-enhed. Lad $d = gcd(f(x))$ så $f(x) = df_1(x)$ hvor $f_1(x)$ er et primitivt polynomium i $R[x]$. Hvis $d \in R$ er enhed, da er $f(x)$ primitivt. Hvis d ikke er en enhed, så har d en faktorisering $d_1 d_2 \cdots d_n$ af irreducible elementer i R, som også er irreducible i $R[x]$. Og da $f_1(x)$ er primitivt så har $f_1(x)$ pr. lemmaet ovenover en opløsning til irreducible. Så $f(x)$ har kan faktoriseres til et produkt af irreducible i $R[x]$.

Entydighed: Lad $f(x) = p \in R[x]$ være et konstant irreducibelt polynomium, da er p irreducibel i R og derfor også primelement (R UFD) og derfor også primelement i $R[x]$ pr. tidligere lemma.

Antag nu $0 < \deg(f(x))$ for irreducibelt polynomium $f(x) \in R[x]$. Da er $f(x)$ primitiv og irreducibel i $F[x]$. Da $F[x]$ er UFD, er $f(x)$ et primelement i $F[x]$. Antag $f(x) \mid g(x)h(x)$ i $R[x]$, så $f(x) \mid h(x)g(x)$ i $F[x]$, og derfor har vi enten $f(x) \mid h(x)$ eller $f(x) \mid g(x)$ i $F[x]$. Antag $f(x) \mid g(x)$, altså $g(x) = p(x)f(x) \in F[x]$ for et $p(x) \in F[x]$. Vælg $c \in F$ så $cp(x) \in R[x]$ og er primitivt (sæt koefficienter på fælles brøkstreg og gang med nævner og derefter med gcd for resten). Da har vi

$$g(x) = cp(x) \cdot f(x) \in R[x]$$

Og pr. Gauss sætning, da $cp(x)$ og $f(x)$ er primitive er $cg(x)$ også primitivt. Derfor får vi pr. lemma (1.4) at $c = \frac{1}{u}$ for et $0 \neq u \in R$ så $uc = 1$. Da er $p(x) = ucp(x)$, hvorfor $p(x)$ må tilhøre $R[x]$, og derfor har vi $g(x) = p(x)f(x) \in R[x]$, så $f(x) \mid g(x)$ i $R[x]$, så $f(x)$ er et primelement.

Da primopløsninger er entydige (op til association), er vi færdige. $\square$

KAPITEL 10

IRREDUCIBILITETSKRITERIER I POLYNOMIUMSRINGE

Taleplan

1. For legeme F er $F[x]$ euklidisk m.m.
2. Sætning: om rødder i $F[x]$ og faktorisering
3. Sætning: 2. eller 3. grad: $p(x) \in F[x]$ reducibel iff $p(x)$ har rod i F.
4. Lemmaer: 1.1 og Gauss om primelementer og primitive elemente i $R[x]$.
5. Theorem: R UFD $\implies$ $R[x]$ UFD.

Beviser

For et legeme F har $F[x]$ normen deg, som gør $F[x]$ euklidisk. Da kan man udføre divison med rest. Specielt er F integritetsområde og $F^\times = F\backslash\{0\}$, derfor er $F[x]^\times = F\backslash\{0\}$.

Proposition 10.1
For $a \in F$, hvor F er et legeme. Hvis $p(x) \in F[x]$, da gælder

$$p(a) = 0 \iff (x - a) \mid p(x) \in F[x].$$

Bevis.
$\implies$: Hvis $p(a) = 0$, da giver division med rest $r(x), q(x) \in F[x]$ så $p(x) = q(x)(x - a) + r(x)$, og enten er $r(x) = 0$ eller $\deg r(x) < \deg(x - a) = 1$. Da $0 = p(a) = r(a)$ er $r(x) = 0$ så $p(x) = q(x)(x - a) \iff (x - a) \mid p(x) \in F[x]$.

$\impliedby$: Hvis $(x - a) \mid p(x) \in F[x]$ findes $q(x) \in F[x]$ så $p(x) = q(x)(x - a)$, men da er $p(a) = 0$. □

Proposition 10.2
Lad F være et legeme. Hvis $p(x) \in F[x]$ med $\deg p(x) = 2$ eller 3, da gælder

$$p(x) \text{ reducibel i } F[x] \iff p(x) \text{ har en rod i } F.$$

Bevis.
$\implies$: Lad $p(x) = f(x)g(x)$ være en opløsning med $f(x)$ og $g(x)$ ikke enheder i $F[x]$, så $\deg f(x), \deg g(x) > 0$. Hvis $\deg f(x) = n$ og $\deg g(x) = m$ har vi $n + m = 2$ eller

3, så enten n eller m er lig 1. Antag n, så $f(x) = a_0 + a_1 x$. Da er $-a_0 a_1^{-1}$ en rod, for $f(-a_0 a_1^{-1}) = a_0 - a_0 = 0$. derfor er $p(-a_0 a_1^{-1}) = 0$.

$\Longleftarrow$: Hvis $a \in F$ er en rod for $p(x)$ da er $p(x) = q(x)(x-a)$, og da $\deg p(x) = 2$ eller 3 må $\deg q(x) = 1$ eller 2, så både $q(x)$ og $(x-a)$ er ikke-enheder, ergo er $p(x)$ reducibel i $F[x]$. $\square$

Proposition 10.3
For R UFD med brøklegeme F gælder der: hvis $f(x) \in R[x]$ med $\deg f(x) = n > 0$, så $f(x) = a_0 + a_1 x^1 + \dots a_n x^n$ har en rod $\frac{r}{s} \in F$ med $\gcd(r, s) = 1$, da gælder, at $r \mid a_0$ og $s \mid a_n$.

Bevis.
Pr. antagelse har vi

$$\begin{aligned} p\left(\frac{r}{s}\right) = 0 &= a_0 + a_1 \frac{r}{s} + a_2 \left(\frac{r}{s}\right)^2 + \dots + a_n \left(\frac{r}{s}\right)^n \\ \iff 0 &= a_0 s^n + a_1 r s^{n-1} + \dots + a_n r^n \end{aligned}$$

Ved isolering får vi

$a_n r^n = s(-a_{n-1} r^{n-1} - \dots - a_0 s^{n-1})$ og $a_0 s^n = r(-a_1 s^{n-1} - a_2 s^{n-2} r - \dots - a_n r^{n-1})$

Så $r \mid a_0 s^n$ og $s \mid a_n r^n$, men $gcd(r, s) = 1$ så $r \mid a_0$ og $s \mid a_n$. $\square$

Theorem 10.4 (Eisensteins' kriterium)
Lad $P \subseteq R$ være et primideal i integritetsområdet R, og lad $f(x) = a_0 + a_1 x + \dots a_{n-1} x^{n-1} + x^n$ være et monisk polynomium med $\deg f(x) = n > 0$. Hvis $a_i \in P$, for $0 \leq i \leq n-1$ og $a_0 \notin P^2$ da er $f(x)$ irreducibel i $R[x]$.

Bevis.
Antag for modstrid, at $f(x) \in R[x]$ er monisk og opfylder men er reducibel i $R[x]$. Da er $f(x) = p(x)q(x)$ for ikke-enheder

$$p(x) = \sum_{0 \leq i \leq k} p_i x^i \text{ og } q(x) = \sum_{0 \leq j \leq m} q_j x^j$$

Og da $n = k + m$ er $p_k, q_m \neq 0$. Da $f(x)$ monisk er $p_k q_m = a_n = 1 \in R$, så p_k, q_m enheder i R. Da både $p(x)$ og $q(x)$ er ikke-enheder også, må $\deg p(x), \deg q(x) > 0$.

Da får vi, i $(R/P)[x]$, da $a_i \in P$ for $0 \leq i \leq n-1$ at $\overline{a_i} = 0$

$$\overline{p(x)q(x)} = \overline{f(x)} = \overline{a_0} + \overline{a_1} x + \overline{a_2} x^2 + \dots + x^n = x^n,$$

Ergo får vi $\overline{p(x)} = \overline{p_k} x^k$ og $\overline{q(x)} = \overline{q_m} x^m$, hvorfor $\overline{q_0} = 0 = \overline{p_0}$, så $q_0, p_0 \in P$ og derfor har vi $a_0 = p_0 q_0 \in P^2$, modstrid. $\square$

Example 10.5
Hvis $p \in \mathbb{Z}$ er et primtal, og $f(x) = a_0 + a_1 x + \dots a_{k-1} x^{k-1} + x^k$ opfylder $a_i p\mathbb{Z}$ for alle $1 \leq i \leq k-1$, men $a_0 \notin p^2\mathbb{Z}$, da er $f(x)$ irreducibel i $\mathbb{Z}[x]$ og $\mathbb{Q}[x]$.