Matematik 211, 1975

Anders Thorup

Algebra

Håndskrevne noter

Algebra, Mat 211, 1978

INDHOLD

Oversigt 10

KONGRUENSRELATIONER s. 1-19 19

0. Relationer
1. Ækvivalensrelationer.
2. Kongruensrelationer.
3. Kongruensrelationer i en gruppe.
4. Kongruensrelationer i en kommutativ gruppe.
5. Kongruensrelationer i en ring.

RINGE s. 1-49 49

1. Ring. Homomorfi. Delring.
2. Eksempler.
3. Foldningsringe.
4. Regulære og invertible elementer.
5. Ideal og kvotientring.
6. Kommutation. Centrum.
7. Associative algebraer over en kommutativ ring.

IDEALER I KOMMUTATIVE RINGE s.1-27 27

1. Ideal og kvotient.
2. Ideal frembragt af delmængde.
3. Noetherske ringe og hovedidealringe.
4. Maksimalideal og primideal.
5. Idealoperationerne. Den kinesiske restklassesætning.

FAKTORIELLE RINGE s.1-29 29

1. Irreducible elementer og primelementer.
2. Faktorielle ringe.
3. Største fælles divisor.
4. Gauß' sætning.

(fortsættes).

Algebra, Mat 211, 1978.

INDHOLD (fortsat).

ALGEBRAISKE ELEMENTER. s. 1-38 — 38

1. Algebraiske elementer.
2. Udvidelser.
3. Indskud om symmetriske polynomier.
4. Algebraens fundamentalsætning.
5. Endelige, reelle divisionsalgebraer.

KATEGORIER s. 1-28 — 28

1. Kategoribegrebet.
2. Funktorer
3. Kategoriske definitioner.

OPGAVER s. 1-8 — 8

Antal sider (excl. indholdsfort.) — 208

OVERSIGT

0. Relationer. Definitioner.

1. Ekvivalensrelationer. 1.1: Kvotient, repræsentant, kanonisk afbildning. 1.2: Homomorfisætning (eller udvidelsessætning) for mængder. 1.3: Isomorfisætning for mængder.

2: Kongruensrelationer. 2.1: Kongruensrelation. Kvotienten $(M,*)/\sim$. 2.2: Homomorfisætning for mængder med komposition. 2.3: Isomorfisætning for mængder med komposition.

3. Kongruensrelationer i en gruppe. 3.1: Normale undergrupper og kongruensrelationer. Kvotientgruppe. 3.2: Homomorfisætning for grupper. 3.3: Isomorfisætning for grupper. 3.4: Bemærkning om venstreækvivalens og højreækvivalens. Indix af undergruppe. Lagranges sætning. 3.5: Noethers isomorfisætning for grupper. 3.6: Noethers isomorfi. 3.7: Specialtilfældet $G/N \rightrightarrows (G/N_0)/(N/N_0)$.

4. Kongruensrelationer i en kommutativ gruppe. Additiv skrivemåde.

5. Kongruensrelationer i en ring. 5.1: Idealer og kongruensrelationer. 5.2: Homomorfisætning for ringe. 5.3: Isomorfisætning for ringe. 5.4: Noethers isomorfisætning for ringe.

OVERSIGT

1. Ring. Homomorfi. Delring.: 1.1: Ring. 1.2: Homomorfi. Kerne. Isomorfi. 1.3: Delring. 1.4: Billedring.

2. Eksempler. 2.1: Nulringen. 2.2: Talringe. 2.3: Eksempel. 2.4 - 2.5: Endomorfiringe. 2.6: Funktionsringe. 2.7 - 2.8: Polynomier. 2.9: Potensrækker. 2.10: Polynomier i flere variable. 2.11: Matricer 2.12: Produkt af ringe. 2.13 - 2.15: Eksempler 2.16: Den kanoniske homomorfi $\mathbb{Z} \to \Lambda$. 2.17: Dirichletrækker. 2.18 - 2.19: Modsat ring og antihomomorfi.

3. Foldningsringe. 3.1: Foldningsringen $\Lambda[S]$. 3.2: Indlejringen $\Lambda \hookrightarrow \Lambda[S]$. 3.3: Indlejringen $S \hookrightarrow \Lambda[S]$. 3.4 - 3.5: Additiv og multiplikativ skrivemåde. 3.6: $\Lambda[X]$. 3.7: $\Lambda[X_1, \dots, X_n]$. 3.8 - 3.11: Rækker.

4. Regulære og invertible elementer. 4.1: Invertibelt element. 4.2: Regulært element. 4.3: Nulreglen. 4.4: Skævlegeme. 4.5: Integritetsområde. 4.6: Eksempler. 4.7: Homomorfi. 4.8 - 4.9: Polynomier. 4.10: Potensrækker. 4.11: Matricer. Determinant. 4.12: Produkt af ringe. 4.13: Dirichletrækker.

5. Ideal og kvotientring. 5.1: Ideal. 5.2: Trivielt ideal. 5.3: Idealer i $\mathbb{Z}$. 5.4: Kerne. 5.5 - 5.7: Karakteristik. 5.8: Kongruensrelation. 5.9: Udvidelsessætning. 5.10: Isomorfisætning. 5.11: Noethers isomorfisætning. 5.12 - 5.17: Endelige ringe. $\mathbb{Z}/n$. 5.18: Idealer i $\mathrm{Mat}_n(\Lambda)$.

6. Kommutation. Centrum. 6.1 - 6.2: Kommutant. Bikommutant. 6.3: Centrum. Centralt element. 6.4 - 6.9: Eksempler.

(fortsættes)

OVERSIGT (fortsat)

7. Associative algebraer over en kommutativ ring: 7.1-2: Definition af R-algebra. 7.3: $\mathbb{Z}$-algebra, algebra over delring af centret, $Mat_n(R)$, $Afb(T,R)$, $R[X]$, foldningsringen $R[S]$. 7.4-5: Notation. 7.6: Algebra defineret ved bilineært produkt. 7.7: Delalgebra. 7.8: Algebrahomomorfi. 7.9: At indsætte a i polynomiet p. 7.10: Eksempel. Polynomiet X^2+1 over $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{H}, \mathbb{Z}/2, \mathbb{Z}/65$. 7.11: $End_L(V)$. 7.12: Homomorfien $p \mapsto p(a)$. 7.13: Delalgebraen $R[a]$. 7.14: Division med rest. 7.15: Division med normeret polynomium. 7.16: Struktur af $R[X]/(d)$. 7.17. Rødder i R for polynomium $p \in R[X]$. 7.18: Eksempler ① Rødder i $\mathbb{C}$, ② Rødder i $\mathbb{F}_p$. 7.19: Indsættelse i polynomium med ikke kommutative koefficienter. 7.20: Hamilton-Cayley's sætning.

OVERSIGT

1. Ideal og kvotient. 1.1-2: Ideal og kongruensrelation. 1.3: Udvidelsessætning. 1.4: Kerne og billede. Isomorfisætning. 1.5-6: Noethers isomorfisætning.

2. Ideal frembragt af delmængde. 2.1: Ideal frembragt af delmængde. 2.2: Endeligt frembragte idealer. Hovedidealer. Multipla. 2.3: Eksempler. ① Ringen $\mathbb{Z}$. ② Ringen $C^0[0,1]$. ③ Ringen $K[X,Y]$. ④ En delring af $\mathbb{Q}[X]$. 2.4: Eksempel. Kvadratiske talringe. Normen $N: R \to \mathbb{Z}$. 2.5: Eksempel. Idealet $(3, 2+\sqrt{-5})$ i $\mathbb{Z}[\sqrt{-5}]$.

3. Noetherske ringe og hovedidealringe. 3.1: Definition af noethersk ring. 3.2: Eksempler. 3.3: Karakteriseringer af noetherske ringe. 3.4: Kvotient af noethersk ring. 3.5: Hilberts basissætning. 3.6: Eksempler. $\mathbb{Z}[X_1, \cdots, X_n]$ og $L[X_1, \cdots, X_n]$. 3.7: Eksempel. Kvadratisk talring. 3.8: Eksempel. Delring af noethersk ring. 3.9: Definition af hovedidealring. 3.10: Sætning om $L[X]$, hvor L er et legeme. 3.11: Sætning om tilstrækkelig betingelse for at en ring er en hovedidealring. 3.12: Gauß' talring. 3.13: En opstigende kædes egenskab for idealer i en hovedidealring.

4. Maksimalideal og primideal. 4.1: Karakterisering af legemer. 4.2: Definition af maksimalideal. 4.3: Karakterisering af maksimalideal. 4.4: Eksempel. Ringen $\mathbb{Z}$. 4.5: Eksempel. Ringen $C^0[0,1]$. 4.6: Eksempel. Idealet $(3, 2+\sqrt{-5})$ i ringen $\mathbb{Z}[\sqrt{-5}]$. 4.7: Definition af primideal. 4.8: Karakterisering af primideal. 4.9: Maksimalidealer er primidealer. 4.10: Kernen for en homomorfi ind i et integritetsområde. 4.11: Eksempel. Primidealer i $\mathbb{Z}[X]$. 4.12: Eksempel. Primidealer i $\mathbb{Z}$. 4.13: Primidealer i en kva-

(fortsættes)

OVERSIGT (fortsat)

dratisk talring.

5. Idealoperationerne. Den kinesiske restklassesætning. 5.1-3: Fællesmængde, sum og produkt. 5.4: Eksempel. Idealer i $\mathbb{Z}$. 5.5: Eksempel. 3 = produkt af to maksimalidealer i $\mathbb{Z}[\sqrt{-5}]$. 5.6: Komaksimale idealer. 5.7: Sætning om komaksimale idealer. 5.8: Eksempel. Ringen $\mathbb{Z}$. Primiske tal. 5.9: Den kinesiske restklassesætning. 5.10: Eksempel. Ringen $\mathbb{Z}$. 5.11. Eksempel. Ringen $L[X]$. 5.12: Eksempel. Ringen $\mathbb{Z}[\sqrt{-5}]$.

OVERSIGT

1. Irreducible elementer og primelementer. 1.1: Definition af enhed. Relationen "associeret med". 1.2: Eksempler. Ringene $\mathbb{Z}$ og $L[X]$. 1.3: Definition af divisor. Triviel divisor. 1.4: Definition af irreducible elementer. 1.5: Eksempler. Ringene $\mathbb{Z}$ og $L[X]$, $\mathbb{C}[X]$, $\mathbb{R}[X]$ og $\mathbb{Q}[X]$. 1.6: Eksempel. Kvadratiske talringe. 1.7: Inklusioner mellem hovedidealerne. 1.8: Karakterisering af irreducibelt element ved det frembragte hovedideal. 1.9: Definition af primelement. 1.10: Karakterisering af primelement ved det frembragte hovedideal. 1.11: Primelementer er irreducible. 1.12: Eksempel. Ringen $\mathbb{Z}[\sqrt{-5}]$. 1.13: Primtallene i $\mathbb{Z}$. 1.14: Irreducible elementer i en hovedidealring. 1.15: Eksempler. Ringene $\mathbb{Z}$ og $\mathbb{Z}[i]$.

2. Faktorielle ringe. 2.1: Definition af irreducibel opløsning og primopløsning. 2.2: Entydighed af primopløsning. 2.3: Eksempel. Ringen $\mathbb{Z}[\sqrt{-5}]$. 2.4: Definition af faktoriel ring. 2.5: Irreducible elementer i en faktoriel ring. 2.6: Karakterisering af faktorielle ringe. 2.7: Eksistens af irreducible opløsninger. 2.8: Irreducible opløsninger i $\mathbb{Z}$, $L[X]$ og kvadratisk talring $\mathbb{Z}[\xi]$. 2.9: Irreducible opløsninger i en noetherisk ring. 2.10: Hovedsætning om hovedidealer. 2.11: Eksempler. Ringene $\mathbb{Z}$ og $L[X]$. 2.12-13: Primelementer i Gauß' talring $\mathbb{Z}[i]$ og primtal i $\mathbb{Z}$. Ligningen $x^2+y^2=p$. 2.14-15: Primopløsninger i en faktoriel ring og i dens brøklegeme. 2.16: Løsninger til ligningen $x^2+y^2=n$.

3. Største fælles divisor. 3.1: Største fælles divisor. Primiske elementer. 3.2-3: Største fælles divisor og idealet (a,b). 3.4: Største fælles divisor i en hovedidealring. 3.5: Største fælles divisor i faktoriel ring. 3.6: Anvendelse på hovedidealring.

(fortsættes)

OVERSIGT (fortsat)

4. Gauß' sætning. 4.1: Konstante primelementer i $R[X]$. 4.2: Definition af primitivt polynomium. 4.3: Gauß' lemma. 4.4: Polynomier med koefficienter i brøklegemet. 4.5: Korollar til Gauß' lemma. 4.6: Bemærkning om korollaret. 4.7: Gauß' sætning. 4.8: Polynomiumsringene $\mathbb{Z}[X_1, \ldots, X_n]$ og $L[X_1, \ldots, X_n]$. 4.9: Schönemann-Eisensteins irreducibilitetskriterium. 4.10: Eksempler. $X^n \pm p$, $X^{p-1} + \ldots + X + 1$ i $\mathbb{Z}[X]$, $X^n + Y^n - 1 \in L[X, Y]$.

OVERSIGT

1. Algebraiske elementer. 1.1: Dimension af L-algebra. 1.2: Eksempel. Algebraerne $\mathrm{Mat}_n(L)$, $\mathrm{End}_L(V)$, $L[X]$, $L[X]/(f)$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$. 1.3: Transcendente og algebraiske elementer. Minimalt polynomium. Grad af et algebraisk element. 1.4: Delalgebraen $L[\alpha]$. 1.5: Eksempler. Minimale polynomier for matricer, for $i \in \mathbb{C}$ og for kvaternioner.

2. Udvidelser. 2.1: Udvidelse af legemer. 2.2-3: Endelige og algebraiske udvidelser. 2.4: Eksempel. Udvidelserne $\mathbb{C}/\mathbb{R}$, $\mathbb{C}/\mathbb{Q}$ og $\mathbb{R}/\mathbb{Q}$. 2.5: Udvidelse frembragt af en delmængde. Adjunktion af elementer fra en udvidelse. 2.6: Algebraiske og transcendente elementer i en udvidelse. 2.7: Division i $L[\alpha] = L(\alpha)$. 2.8: Eksempel. Udvidelsen $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. 2.9: Dimension af vektorrum over en udvidelse. 2.10: Dimension af gentagen udvidelse. 2.11: Adjunktion af endelig mange algebraiske elementer i en udvidelse. 2.12-13: Algebraisk hylster i en udvidelse. 2.14 – 15: Gentagen algebraisk udvidelse. 2.16: Algebraisk afsluttede legemer. 2.17: Legemet af tal algebraiske over $\mathbb{Q}$. Transcendente tal. 2.18: Eksempel på transcendente tal. Liouville's sætning. 2.19: Entydighed af udvidelse $L \hookrightarrow L(\alpha)$. 2.20: Eksempel. Komplex konjugering: $\mathbb{C} \to \mathbb{C}$. 2.21-22. Adjunktion af rod i et irreducibelt polynomium. Definition af $\mathbb{C}$. 2.23: Adjunktion af rødder i et polynomium.

3. Indskud om symmetriske polynomier. 3.1-2: Polynomier i flere variable. Indsættelse i et polynomium. 3.3: Grad af monomium og polynomium. 3.4-6: Ordning af multiindices. Signatur. 3.7: Eksempel på ordning efter signatur. 3.8: Elementarsymmetriske polynomier. 3.9: Polynomiet Δ. 3.10: Definition af symmetrisk polynomium. 3.11: Eksempler. De elementarsymmetriske polynomier. Diskriminanten $D = \Delta^2$. 3.12-13: Hovedsætning om symmetriske polynomier. 3.14: Eksem-

(fortsættes)

OVERSIGT (fortsat)

pler. $X_1^2+X_2^2$, $X_1^3+X_2^3$, $D=(X_1-X_2)^2$ (for $n=2$), D (for $n=3$). 3.15: Anvendelse af hovedsætningen. 3.16: Eksempel. Polynomiet $X^3+2X+5 \in \mathbb{Z}[X]$.

4. Algebraens fundamentalsætning. 4.1: Algebraens fundamentalsætning. 4.2: De irreducible polynomier i $\mathbb{C}[X]$ og $\mathbb{R}[X]$.

5. Endelige, reelle divisionsalgebraer. 5.1: Definition af divisionsalgebra og integritetsalgebra. 5.2: Endelige integritetsalgebraer. 5.3: Delalgebraer af endelige divisionsalgebraer. 5.4: Eksempler. Endelige udvidelser. $\mathbb{R}, \mathbb{C}, \mathbb{H}$. 5.5: Endelige divisionsalgebraer over et algebraisk afsluttet legeme. 5.6: Frobenius' sætning.

OVERSIGT

1. Kategoribegrebet. 1.1: Beskrivelse. 1.2: Isomorfi. 1.3: Endomorfi og automorfi. 1.4: (Sets). 1.5: (Gr). 1.6: (AG), (L-vect), (Rings), (R-alg). 1.7: (Top), (Met, cont), (Met, $dist_{\leq}$). 1.8: (Trip). 1.9: (Top_0), (Met_0, cont). 1.10: Cat(M), hvor M er et monoid. 1.11: Cat(T), hvor T er mængde med refleksiv, transitiv relation. 1.12: Kategorien $\mathcal{C}^{\bullet\to\bullet}$ af morfier i $\mathcal{C}$. Kategorien $\mathcal{M}_{H,S}$. 1.13: Den modsatte kategori $\mathcal{C}^{op}$. 1.14: Diagrammer. Kommutative diagrammer.

2. Funktorer. 2.1: Beskrivelse. 2.2: Funktor anvendt på isomorfi og på kommutativt diagram. 2.3: Definition af kontravariant funktor. 2.4: Funktorers rolle. 2.5: $(\,)^*$:(L-vect) $\to$ (L-vect). 2.6: Funktorerne T: ($Diff_0$) $\to$ ($\mathbb{R}$-vect). 2.7 ① $H \mapsto \tilde{H}$. ② $R \mapsto \tilde{R}$. ③ $G \mapsto \hat{G}$. ④ $\Lambda \mapsto \Lambda[X]$. ⑤ $\Lambda \mapsto \Lambda^*$ ⑥ $M \mapsto \mathbb{Z}^{(M)}$. ⑦ $(M,\sim) \longmapsto M/\sim$. 2.8: Funktorer fra Cat(M). 2.9: Funktorer fra Cat(T). 2.10: Kategorien Open(X) og præknipper. 2.11: Funktoren $Hom_{\mathcal{C}}(-,-)$. 2.12: Homotopifunktoren. Brouwers fixpunktssætning. 2.13: Solitairespillet. 2.14: Glemsommefunktoren. 2.15: Delkategori. 2.16: $\mathcal{K} \supseteq$ (Semigr) $\supseteq$ (Monoids) $\supseteq$ (Gr) $\supseteq$ (AG).

3. Kategoriske definitioner. 3.1: Kategorisk definition. Universel egenskab. 3.2-3: Initial- og finalobjekt. 3.4: Eksempler. (Sets), (Trip), (Gr), (AG), (L-vect), (Rings), (R-alg), (Top), (Met, cont), (Met, $dist_{\leq}$), ($Sets_0$), (Gr_0), (AG_0), (L-$vect_0$), ($Rings_0$), (R-alg_0), (Top_0), (Met_0, cont), (Met_0, $dist_{\leq}$), ($Arch_0$), Cat(T), $\mathcal{M}_{H,S}$, $\mathcal{R}_{R,S}$, $\mathcal{K}_G$. 3.5-7: Produkt i en kategori. 3.8: Eksemplerne. 3.9: Dual definition. Sum i en kategori. 3.10: Eksemplerne. 3.11: Funktorer og produkter (og summer). 3.12: Eksempler.

KONGRUENSRELATIONER.

0. Relationer

0.1. En relation R i en mængde M er som bekendt en delmængde $R \subseteq M \times M$. At $(x,y) \in R$ [resp. $(x,y) \notin R$] skrives ofte xRy [resp. $x \not R y$].

0.2 DEFINITIONER. En relation R i M kaldes
refleksiv, hvis der for alle $x \in M$ gælder xRx,
irrefleksiv, hvis der for intet $x \in M$ gælder xRx,
symmetrisk, hvis der for alle $x, y \in M$ gælder
$$xRy \Rightarrow yRx,$$
asymmetrisk, hvis der for alle $x, y \in M$ gælder
$$xRy \wedge yRx \Rightarrow y = x,$$
transitiv, hvis der for alle $x, y, z \in M$ gælder
$$xRy \wedge yRz \Rightarrow xRz,$$
og *total*, hvis der for alle $x, y \in M$ gælder
$$x = y \vee xRy \vee yRx.$$

0.3. DEFINITION. En transitiv relation R i M kaldes også en *præ-ordning*. Hvis R desuden er asymmetrisk, kaldes R en (partiel) *ordning*, og (M,R) kaldes en (partielt) *ordnet mængde*. Bemærk, at en relation, der er transitiv og irrefleksiv, er asymmetrisk og dermed en ordning. Som betegnelse for ordninger bruges ofte et af tegnene $<$, $\leqslant$, $\prec$, $\subset$ (eller $>$, $\geqslant$, $\succ$, $\supset$). Hvis $(M, \prec)$ og $(N, \prec)$ er ordnede mængder, siges en afbildning $f: M \to N$ at være *ordenstro*, eller at være en *homomorfi* : $(M, \prec) \longrightarrow (N, \prec)$, hvis

hvis der for alle $x, y \in M$ gælder

$$x \prec y \Rightarrow f(x) \prec f(y).$$

0.4. DEFINITION. Lad $(M, \prec)$ være en ordnet mængde. Et element $a \in M$ kaldes maximalt (resp minimalt), hvis der for alle $x \in M$ gælder

$$a \prec x \Rightarrow a = x.$$

(resp. $x \prec a \Rightarrow x = a$)

Det kaldes sidste (resp første) element i M, hvis der for alle $x \in M$ gælder $x \preceq a$ (resp. $a \preceq x$). Et sidste element er naturligvis maksimalt. Det omvendte gælder i almindelighed kun når ordningen er total.

0.5. DEFINITION. Lad $(M, \prec)$ være en ordnet mængde. En delmængde $S \subseteq M$ siges at være opad begrænset (resp. nedad begrænset), hvis der findes et element $a \in M$, så at der for alle $x \in S$ gælder

$$x \preceq a \quad [\text{kort: } S \preceq a]$$

(resp $a \preceq x$ [kort: $a \preceq S$]).

Et sådant element $a \in M$ kaldes da en majorant (resp minorant) for S. Hvis der findes en første majorant (resp. en sidste minorant) a for S, siges S at have et supremum (resp. infimum) og vi skriver

$$a = \sup S \quad (\text{resp. } a = \inf S).$$

0.6. DEFINITION. En relation R i M kaldes en ækvivalensrelation, hvis den er refleksiv, symmetrisk og transitiv. Delmængden af M af formen $\{x \in M \mid xRa\}$, med $a \in M$ kaldes da ækvivalensklasser.

1. Ækvivalensrelationer.

1.1. Lad M være en mængde. Hvis $\sim$ er en ækvivalensrelation i M, kan vi opfatte ækvivalensklasserne ved $\sim$ som elementer i en ny mængde, mængden af ækvivalensklasser. Mængden af ækvivalensklasser m.h.t. $\sim$ kaldes kvotienten (eller kvotientmængden) af M m.h.t. $\sim$ og betegnes $M/\sim$.

En ækvivalensklasse X kan altså opfattes dels som en delmængde af af M ($X \subseteq M$), dels som et element i kvotienten $M/\sim$ ($X \in M/\sim$). Hvis $x \in X$, siger vi, at x er en repræsentant for X.

Idet vi for hvert element $x \in M$ med $\textcircled{x}$ betegner den ækvivalensklasse, som indeholder x, altså

$$\textcircled{x} = \{ x' \in M \mid x' \sim x \},$$

defineres ved $x \mapsto \textcircled{x}$ en surjektiv afbildning

$$0 : M \to M/\sim,$$

kaldet den kanoniske afbildning. At x er repræsentant for ækvivalensklassen X, betyder, at $\textcircled{x} = X$.

1.2. DEFINITION. Lad $\sim$ være en ækvivalensrelation i M. En afbildning $f : M \to P$ siges at respektere ækvivalensrelationen $\sim$, hvis

$$\forall x, x' \in M : \; x \sim x' \Rightarrow f(x) = f(x').$$

(ELLER UDVIDELSESSÆTNING)

"HOMOMORFI"SÆTNING FOR MÆNGDER. Lad $\sim$ være en ækvivalensrelation i M, og lad $0 : M \to M/\sim$ være den kanoniske afbildning ind i kvotienten.

Til hver afbildning $f: M \to P$, som respekterer $\sim$, findes netop én afbildning $\tilde{f}: M/\sim \to P$, således at $\tilde{f} \circ O = f$.

$$\begin{array}{ccc} M & \xrightarrow{O} & M/\sim \\ {\scriptstyle f}\downarrow & \swarrow_{\tilde{f}} & \\ P & & \end{array}$$

Bevis. Trivielt. ▨

En afbildning $g: M/\sim \to P$, som opfylder $g \circ O = f$, kaldes en udvidelse af f til $M/\sim$ (idet afbildningen O er understået). Sætningen udsiger altså, at en afbildning $f: M \to P$, som respekterer $\sim$, entydigt kan udvides til en afbildning fra kvotienten $M/\sim$. Udvidelsen $\tilde{f}$ siges at være inducert af f.

1.3. Lad nu M være en vilkårlig mængde, og betragt en afbildning $f: M \to P$. Ved

$$x \underset{f}{\sim} x' \Leftrightarrow f(x) = f(x')$$

defineres da en relation $\underset{f}{\sim}$ i M, som let ses at være en ækvivalensrelation. Den hertil hørende kvotient $M/\underset{f}{\sim}$ betegnes også M/f. Det er en umiddelbar følge af definitionen, at f respekterer $\underset{f}{\sim}$. Afbildningen f inducerer altså en afbildning $\tilde{f}: M/f \to P$.

"ISOMORFI"SÆTNING FOR MÆNGDER. Lad $f: M \to P$ være en afbildning. Den inducerede afbildning $\tilde{f}: M/f \to P$ giver da en bijektiv afbildning af kvotienten M/f på billedet $f(M) \subseteq P$.

$$\begin{array}{ccc} M & \xrightarrow{O} & M/f \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle \tilde{f}} \\ P & \hookleftarrow & f(M) \end{array}$$

Bevis. Trivielt. ▨

2. Kongruensrelationer

2.1. Lad $(M,*)$ være en mængde M med en komposition $*$. En ækvivalensrelation $\sim$ i M siges at <u>harmonere</u> med kompositionen $*$, eller at være en <u>kongruensrelation</u> m.h.t. $*$, eller at være en <u>kongruensrelation i $(M,*)$</u>, hvis der for alle $x, x', y, y' \in M$ gælder

$$x \sim x' \Rightarrow x*y \sim x'*y \quad \wedge \quad y*x \sim y*x'.$$

Af transitiviteten følger så, at $x \sim x' \wedge y \sim y' \Rightarrow x*y \sim x'*y'$.

Hvis $\sim$ er en kongruensrelation i $(M,*)$, kan vi i kvotienten $M/\sim$ definere en komposition $\tilde{*}$, således at der for alle $x, y \in M$ gælder

$$\textcircled{x} \,\tilde{*}\, \textcircled{y} = \textcircled{x*y}.$$

Kompositionen $\tilde{*}$ defineres således: Er X, Y elementer i $M/\sim$, altså ækvivalensklasser, kan vi vælge repræsentanter $x, y \in M$ – altså $X = \textcircled{x}$, $Y = \textcircled{y}$ – og betragte ækvivalensklassen $\textcircled{x*y}$, der indeholder $x*y$. Denne ækvivalensklasse er uafhængig af det foretagne valg, thi er x', y' andre repræsentanter for X, Y, finder vi $x \sim x'$, $y \sim y'$ og dermed $x*y \sim x'*y'$. Følgelig kan denne ækvivalensklasse betegnes $X \tilde{*} Y$.

Kvotienten $M/\sim$ er altså med denne komposition igen en mængde med en komposition $(M/\sim, \tilde{*})$. Den kaldes kvotienten af $(M,*)$ m.h.t. $\sim$, og betegnes også $(M,*)/\sim$, altså

$$(M,*)/\sim \;=\; (M/\sim, \tilde{*}).$$

Den kanoniske afbildning $0 : M \to M/\sim$ er en surjektiv homomorfi

$$0 : (M,*) \to (M,*)/\sim.$$

Dette udsiger blot, at der for alle $x, y \in M$ gælder

$$\textcircled{x*y} = \textcircled{x} \,\tilde{*}\, \textcircled{y},$$

og det har vi jo opnået ved definitionen af $\tilde{*}$.

Af surjektiviteten alene følger, at en lang række egenskaber nedarves fra $(M,*)$ til $(M/\sim,\tilde{*})$. Som eksempler på sådanne egenskaber nævnes kommutativitet, associativitet, eksistens af neutralt element, eksistens af invers.

Kompositionen i kvotienten $(M,*)/\sim$ betegnes ofte med samme tegn som kompositionen i M. (altså $*$ i stedet for $\tilde{*}$). Som betegnelse for en kongruensrelation vælges ofte tegnet $\equiv$.

(ELLER UDVIDELSESSÆTNING)

2.2. HOMOMORFISÆTNING FOR MÆNGDER MED KOMPOSITION.

Lad $\sim$ være en kongruensrelation i $(M,*)$, og lad $0:(M,*)\to(M/\sim,*)$ være den kanoniske homomorfi ind i kvotienten. Til hver homomorfi $f:(M,*)\to(P,*)$, som respekterer $\sim$, findes netop en homomorfi $\tilde{f}:(M/\sim,*)\to(P,*)$, således at $\tilde{f}\circ 0 = f$.

$$\begin{array}{ccc}(M,*) & \xrightarrow{0} & (M/\sim,*)\\ f\downarrow & \swarrow_{\tilde{f}} & \\ (P,*) & & \end{array}$$

Bevis. Vi ved, at afbildningen $f:M\to P$ entydigt kan udvides til en afbildning $\tilde{f}:M/\sim\to P$, og skal altså blot vise, at $\tilde{f}$ er en homomorfi: $(M/\sim,*)\to(P,*)$. Dette følger trivielt af definitionerne. ▨

2.3. Lad $(M,*)$ være en mængde med en komposition, og betragt en homomorfi $f:(M,*)\to(P,*)$. Det ses let, at billedmængden $f(M)\subseteq P$ er en stabil delmængde af $(P,*)$. Billedet kan derfor betragtes som en mængde med komposition $(f(M),*)$. Det ses ligeledes let, at den til f hørende ækvivalensrelation i M, defineret ved

$$x \underset{f}{\sim} x' \Leftrightarrow f(x) = f(x'),$$

er en kongruensrelation i $(M,*)$. Kvotienten M/f er derfor ligeledes en mængde med en komposition $(M/f,*)$. Af definitionen følger, at homomorfien $f:(M,*)\to(P,*)$ respekterer kongruensrelationen $\tilde{f}$. Homomorfien f inducerer altså en homomorfi $\tilde{f}:(M/f,*)\to(P,*)$.

ISOMORFISÆTNING FOR MÆNGDER MED KOMPOSITION. Lad $f:(M,*)\to(P,*)$ være en homomorfi. Den inducerede afbildning giver da en isomorfi af kvotienten $(M/f,*)$ på billedet $(f(M),*)$.

$$\begin{array}{ccc} (M,*) & \xrightarrow{\circ} & (M/f,*) \\ f\downarrow & & \downarrow\wr\ \tilde{f} \\ (P,*) & \longleftarrow & (f(M),*) \end{array}$$

Bevis. Trivielt. ▨

i $(G,\cdot)$ og de normale undergruppe i $(G,\cdot)$. Kongruensrelationen $\underset{N}{\equiv}$, der hører til den normale undergruppe N i G, kaldes <u>kongruens modulo N</u>, og vi skriver ofte $x' \equiv x \pmod N$ eller $x' \equiv x \,(N)$ i stedet for $x' \underset{N}{\equiv} x$. Kvotienten $(G,\cdot)/\underset{N}{\equiv}$, der er en gruppe, kaldes <u>kvotientgruppen</u> af $(G,\cdot)$ m.h.t. N og betegnes $(G,\cdot)/N$ eller $(G/N,\cdot)$ eller blot G/N.

Vi har

$$x' \underset{N}{\equiv} x \Leftrightarrow x^{-1}x' \in N \Leftrightarrow x' \in xN.$$

Ækvivalensklasserne hørende til $\underset{N}{\equiv}$ er altså delmængderne af G af formen xN, $x \in G$. Disse ækvivalensklasser kaldes også <u>sideklasser</u> modulo N

3.2. Lad N være en normal undergruppe i $(G,\cdot)$. Det ses let, at en gruppehomomorfi $f:(G,\cdot)\to(H,\cdot)$ (d.v.s. en homomorfi mellem grupper $(G,\cdot)$ og $(H,\cdot)$) respekterer $\underset{N}{\equiv}$, hvis og kun hvis den for hvert element $n \in N$ gælder, at $f(n)$ er det neutrale element i H. Vi siger da, at f <u>forsvinder på N</u>.

Med de nye betegnelser får vi – idet vi undlader at skrive tegnene for kompositionerne – :

(ELLER UDVIDELSESSÆTNING)

HOMOMORFISÆTNING FOR GRUPPER. <u>Lad N være en normal undergruppe i gruppen G, og lad $O:G\to G/N$ være den kanoniske homomorfi ind i kvotientgruppen. Til hver gruppehomomorfi $f:G\to H$, som forsvinder på N, findes netop én homomorfi $\tilde{f}:G/N\to H$, således at $\tilde{f}\circ O = f$.</u>

$$\begin{array}{ccc} G & \xrightarrow{O} & G/N \\ {\scriptstyle f}\downarrow & \swarrow_{\tilde{f}} & \\ H & & \end{array}$$

Bevis. Blot en oversættelse af sætning 2.2. ▨

3. Kongruensrelationer i en gruppe.

3.1. Hvis $\equiv$ er en kongruensrelation i en gruppe $(G,\cdot)$, så er kvotienten $(G,\cdot)/\equiv$ igen en gruppe. Det følger let af at den kanoniske homomorfi $C: (G,\cdot) \to (G/\equiv, \cdot)$ er surjektiv. Vi vil beskrive samtlige kongruensrelationer i gruppen $(G,\cdot)$.

DEFINITION. En undergruppe N i $(G,\cdot)$ kaldes <u>normal</u>, hvis der for alle $x \in G$ gælder

$$xNx^{-1} = N$$

[For en delmængde $N \subseteq G$ betegner vi med xN delmængden $xN = \{xn \mid n \in N\}$. Analogt defineres Nx og xNx^{-1}]

En normal undergruppe i $(G,\cdot)$ kaldes også en <u>normaldeler</u> i $(G,\cdot)$

SÆTNING. <u>Lad $\equiv$ være en kongruensrelation i gruppen $(G,\cdot)$, og lad G_0 betegne den ækvivalensklasse, der indeholder det neutrale element e, altså</u>

$$G_0 = \textcircled{e} = \{x \in G \mid x \equiv e\}.$$

<u>Da er G_0 en normal undergruppe i G, og kongruensrelationen er helt bestemt ved G_0, idet</u>

$$x' \equiv x \iff x^{-1}x' \in G_0.$$

<u>Omvendt, er der i $(G,\cdot)$ givet en normal undergruppe N, så defineres ved</u>

$$x' \underset{N}{\equiv} x \iff x^{-1}x' \in N$$

<u>en kongruensrelation $\underset{N}{\equiv}$ i $(G,\cdot)$, m.h.t. hvilken ækvivalensklassen, der indeholder det neutrale element, er N.</u>

Bevis. □

Af denne sætning følger, at der er en entydig forbindelse mellem kongruensrelationerne

3.3. Lad $f: (G,\cdot) \to (H,\cdot)$ være en gruppehomomorfi. Det er let at se, at billedmængden $f(G)$ er en undergruppe i $(H,\cdot)$. Specielt er billedmængden selv en gruppe. Som tidligere nævnt er den til f hørende ækvivalensrelation $\tilde{f}$ en kongruensrelation. Den til $\tilde{f}$ hørende normale undergruppe i G er

$$N_f = \{x \in G \mid f(x) = f(e)\} = f^{-1}(e')$$

hvor e' er det neutrale element i gruppen H. Denne normale undergruppe kaldes homomorfiens kerne. Denne kerne bestemmer kongruensrelationen $\tilde{f}$, og vi har $(G,\cdot)/\tilde{f} = (G,\cdot)/N_f$. Homomorfien f forsvinder på sin kerne, og inducerer derfor en homomorfi $\tilde{f}: (G,\cdot)/N_f \to (H,\cdot)$, og vi får

ISOMORFISÆTNING FOR GRUPPER. Lad $f: G \to H$ være en gruppehomomorfi med kernen N_f. Den inducerede homomorfi $\tilde{f}: G/N_f \to H$ giver da en isomorfi af kvotientgruppen G/N_f på billedgruppen $f(G)$

$$\begin{array}{ccc} G & \xrightarrow{0} & G/N_f \\ f\downarrow & & \downarrow\!\!\int \tilde{f} \\ H & \hookleftarrow & f(G) \end{array}$$

Bevis. Oversættelse af sætning 2.3. ▨

3.4 BEMÆRKNING. Lad H være en vilkårlig (ikke nødvendigvis normal) undergruppe i gruppen $(G,\cdot)$. Det er let at vise, at der ved

$$x' \underset{v}{\sim} x \iff x^{-1}x' \in H$$

og

$$x' \underset{h}{\sim} x \iff x'x^{-1} \in H$$

defineres to ækvivalensrelationer i G, kaldet

venstre- og højre-ækvivalens modulo H.

Ækvivalensklasserne m.h.t. $\overset{v}{\sim}$ er delmængderne af formen xH, $x \in G$; de kaldes venstresideklasser. Ækvivalensklasserne m.h.t. $\overset{h}{\sim}$ er delmængderne af formen Hx, $x \in G$; de kaldes højresideklasser [Huskeregel: hvis $ø \in G$, er $Hø$ en Højresideklasse].

Hvis H er en normal undergruppe, er de to ækvivalensrelationer identiske (begge er $\overset{H}{\equiv}$).

Hvis derimod H ikke er normal, er de to ækvivalensrelationer forskellige, og ingen af dem er kongruensrelationer.

Hvis $X \subseteq G$ er en venstresideklasse, så er

$$X^{-1} = \{x^{-1} \mid x \in X\}$$

en højresideklasse. Det er let at se, at afbildningen $X \mapsto X^{-1}$ er en bijektiv afbildning:

$$\{\text{venstresideklasser}\} \overset{\sim}{\to} \{\text{højresideklasser}\}$$

Antallet af venstresideklasser er altså det samme som antallet af højresideklasser. Dette antal kaldes undergruppens index i G og betegnes $|G:H|$.

Da alle sideklasser har samme antal elementer som sideklassen H [$h \mapsto xh$ er en bijektiv afbildning: $H \overset{\sim}{\to} xH$] får vi

LAGRANGES SÆTNING: $\boxed{|G| = |G:H| \cdot |H|}$

Hvis H er en normal undergruppe, kan vi skrive

$$\boxed{|G| = |G/H| \cdot |H|}$$

3.5. Det er nærliggende (?) at søge en beskrivelse af undergrupper og normale undergrupper i en given kvotientgruppe af en gruppe G. Lidt mere generelt kan vi betragte en surjektiv gruppehomomorfi

$$\varphi: G \to G'.$$

Vi ser lit, at der for en undergruppe H i G gælder, at billedet $\varphi(H)$ er en undergruppe i G', og at der for en undergruppe H' i G' gælder, at originalmængden $\varphi^{-1}(H')$ er en undergruppe i G, som indeholder homomorfiens kerne $\varphi^{-1}(e')$.

NOETHERS ISOMORFISÆTNING FOR GRUPPER. Lad $\varphi: G \to G'$ være en surjektiv homomorfi med kernen N_0. Ved

$$H \longmapsto \varphi(H)$$

og

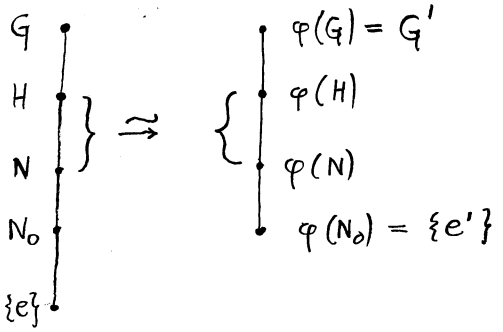
$$\varphi^{-1}(H') \longmapsto H'$$

etableres da en bijektiv ordenstro forbindelse:

$$\{H \mid H \text{ er undergruppe i } G,\ H \supseteq N_0\} \rightleftarrows \{H' \mid H' \text{ er undergruppe i } G'\}.$$

Er $H \supseteq N \supseteq N_0$ undergrupper i G, og er $\varphi(H) \supseteq \varphi(N)$ de tilsvarende undergrupper i G', så er N normal i H, hvis og kun hvis $\varphi(N)$ er normal i $\varphi(H)$. Er dette tilfældet, findes en naturlig isomorfi mellem de tilhørende kvotienter:

$$H/N \xrightarrow{\sim} \varphi(H)/\varphi(N).$$



Isomorfien $H/N \xrightarrow{\sim} \varphi(H)/\varphi(N)$ kaldes Noethers isomorfi.

Bevis. Mellem de betragtede mængder af undergrupper i G og G' har vi de to afbildninger: $H \mapsto \varphi(H)$ og $H' \mapsto \varphi^{-1}(H')$, som klart er ordenstro (dvs bevarer "$\subseteq$"). Vi ønsker at vise, at disse afbildninger er "hinandens inverse":

For en undergruppe H' i G' har vi

$$H' \longmapsto \varphi^{-1}(H') \longmapsto \varphi(\varphi^{-1}(H')),$$

og her er $\varphi(\varphi^{-1}(H')) = H'$, da φ er surjektiv.

For en undergruppe $H \supseteq N_0$ i G har vi

$$H \longmapsto \varphi(H) \longmapsto \varphi^{-1}(\varphi(H)).$$

Her er $\varphi^{-1}(\varphi(H)) = H$, thi "$\supseteq$" er klart, og betragter vi omvendt et element $x \in \varphi^{-1}(\varphi(H))$, kan vi skrive $\varphi(x) = \varphi(h)$, hvor $h \in H$. Vi ser, at $\varphi(xh^{-1}) = \varphi(x)\varphi(h)^{-1} = e'$, og dermed at $xh^{-1} \in N_0$. Da $N_0 \subseteq H$, har vi specielt $xh^{-1} \in H$, og vi slutter at $x = (xh^{-1})h \in H$.

Lad nu $H \supseteq N \supseteq N_0$ være undergrupper i G. Hvis N er normal i H, så er $hNh^{-1} = N$ for alle $h \in H$, og vi slutter, at $\varphi(h)\varphi(N)\varphi(h)^{-1} = \varphi(N)$ for alle $h \in H$, og dermed at $\varphi(N)$ er normal i $\varphi(H)$. Er omvendt $\varphi(N)$ normal i $\varphi(H)$, så er $\varphi(h)\varphi(N)\varphi(h)^{-1} = \varphi(N)$ for alle $h \in H$. Heraf slutter vi, at $\varphi(hNh^{-1}) = \varphi(N)$ for alle $h \in H$. Da hNh^{-1} er en undergruppe i G, og da vi har $hNh^{-1} \supseteq N_0$ (her bruges, at N_0 er normal), følger det af den bijektive forbindelse, at vi har $hNh^{-1} = N$.

For endelig at bestemme isomorfien $H/N \xrightarrow{\sim} \varphi(H)/\varphi(N)$, bemærker vi, at φ ved restriktion definerer en

surjektiv homomorfi : $H \longrightarrow \varphi(H)$. Sammensættes med den kanoniske homomorfi : $\varphi(H) \longrightarrow \varphi(H)/\varphi(N)$, får vi en surjektiv homomorfi :

$$H \longrightarrow \varphi(H) \longrightarrow \varphi(H)/\varphi(N).$$

Denne homomorfi har kernen $\varphi^{-1}(\varphi(N))$, og da vi har $\varphi^{-1}(\varphi(N)) = N$ ifølge det allerede viste, følger Noethers isomorfi af den generelle isomorfisætning 3.3 ▨

3.6. Isomorfien $H/N \xrightarrow{\sim} \varphi(H)/\varphi(N)$ vil vi kalde <u>Noethers isomorfi</u>. I specialtilfældet $N = N_0$ har vi $\varphi(N) = \{e'\}$, og Noethers isomorfi er isomorfien

$$H/N_0 \xrightarrow{\sim} \varphi(H)$$

fra isomorfisætningen 3.3.

I specialtilfældet $H = G$ har vi $\varphi(H) = G'$, og Noethers isomorfi er en isomorfi :

$$G/N \xrightarrow{\sim} G'/\varphi(N).$$

3.7. Betragter vi som surjektiv gruppehomomorfi en kvotienthomomorfi : $G \longrightarrow G/N_0$ ser vi, at undergrupperne i G/N_0 er af formen H/N_0, hvor $H \supseteq N_0$ er en entydigt bestemt undergruppe i G. Videre er $N \supseteq N_0$ normal i G, hvis og kun hvis N/N_0 er normal i G/N_0, og vi har i dette tilfælde en isomorfi

$$G/N \xrightarrow{\sim} (G/N_0)/(N/N_0).$$

4. Kongruensrelationer i en kommutativ gruppe

I en kommutativ (additivt skrevet) gruppe $(G,+)$ er enhver undergruppe øjensynlig normal. Der er altså en entydig forbindelse mellem kongruensrelationerne i $(G,+)$ og undergrupperne i $(G,+)$, idet kongruensrelationen $\underset{N}{\equiv}$ hørende til undergruppen N er bestemt ved

$$x' \underset{N}{\equiv} x \iff x' - x \in N.$$

Sideklasserne imodulo N er delmængderne af formen $x+N$, $x \in G$. Kvotientgruppen $(G,+)/N$ bliver igen kommutativ (og komposition skrives additivt).

En homomorfi $f: (G,+) \to (H,+)$ mellem kommutative (additivt skrevne) grupper forsvinder på N, hvis og kun hvis $f(x) = 0$ for alle $x \in N$. Kernen for en sådan homomorfi er $f^{-1}(0)$.

5. Kongruensrelationer i en ring

5.1. Lad M være en mængde med flere kompositioner $*, \top, \dots$. Hvis en ækvivalensrelation $\sim$ i M harmonerer med alle kompositionerne $*, \top, \dots$ i M, siger vi, at $\sim$ er en kongruensrelation i $(M, *, \top, \dots)$. Vi kan da definere kompositioner $\tilde{*}, \tilde{\top}, \dots$ i kvotientmængden $M/\sim$, således at den kanoniske afbildning $\sigma : M \to M/\sim$ bliver en homomorfi

$$\sigma : (M, *, \top, \dots) \to (M/\sim, \tilde{*}, \tilde{\top}, \dots).$$

$(M/\sim, \tilde{*}, \tilde{\top}, \dots)$ kaldes kvotienten af $(M, *, \top, \dots)$ m.h.t. $\sim$, og kan betegnes $(M, *, \top, \dots)/\sim$.

Hvis M m.h.t. kompositionen $*$ er en gruppe, svarer kongruensrelationerne i $(M, *, \top, \dots)$ til visse normale undergrupper i $(M, *)$, nemlig til de normale undergrupper N i $(M, *)$, for hvilke kongruensrelationen $\underset{N}{\equiv}$ i $(M, *)$ også harmonerer med $\top, \dots$.

Vi vil her betragte tilfældet, hvor vi har givet en <u>ring</u> $(A, +, \cdot)$.

DEFINITION. En ikke tom delmængde $\mathfrak{a}$ af A kaldes et <u>ideal</u>, hvis

I1) $\quad a_1 \in \mathfrak{a} \wedge a_2 \in \mathfrak{a} \Rightarrow a_1 - a_2 \in \mathfrak{a}$

I2) $\quad a \in \mathfrak{a} \wedge x \in A \Rightarrow xa \in \mathfrak{a} \wedge ax \in \mathfrak{a}.$

Betingelsen I1) i forbindelse med at $\mathfrak{a} \neq \emptyset$ udsiger, at $\mathfrak{a}$ er en undergruppe i $(A, +)$. Idealerne i $(A, +, \cdot)$ kan altså karakteriseres som de undergrupper i $(A, +)$, som er invariante over for multiplikation med ethvert $x \in A$. Vi får let:

SÆTNING. <u>Lad $\equiv$ være en kongruensrelation i ringen $(A, +, \cdot)$, og lad A_0 betegne den ækviva-</u>

lemsklasse, der indeholder nul-elementet, altså

$$A_0 = \mathfrak{O} - \{x \in A \mid x \equiv 0\}.$$

Da er A_0 et ideal i A, og kongruensrelationen er helt bestemt ved A_0, idet

$$x' \equiv x \iff x' - x \in A_0.$$

Omvendt, er der i $(A,+,\cdot)$ givet et ideal $\mathfrak{a}$, så defineres ved

$$x' \underset{\mathfrak{a}}{\equiv} x \iff x' - x \in \mathfrak{a}$$

en kongruensrelation $\underset{\mathfrak{a}}{\equiv}$ i $(A,+,\cdot)$, m.h.t. hvilken ækvivalensklassen, der indeholder nul-elementet, er $\mathfrak{a}$.

Bevis. □

Af denne sætning følger, at der er en entydig forbindelse mellem idealerne i $(A,+,\cdot)$ og kongruensrelationerne i $(A,+,\cdot)$. Kongruensrelationen $\underset{\mathfrak{a}}{\equiv}$, der hører til idealet $\mathfrak{a}$ i A, kaldes <u>kongruens modulo $\mathfrak{a}$</u>, og vi skriver ofte $x' \equiv x \pmod{\mathfrak{a}}$ eller $x' \equiv x \ (\mathfrak{a})$ for $x' \underset{\mathfrak{a}}{\equiv} x$. Det ses let, at kvotienten $(A,+,\cdot)/\underset{\mathfrak{a}}{\equiv}$ igen bliver en ring. Den kaldes <u>kvotientringen</u> af $(A,+,\cdot)$ m.h.t. $\mathfrak{a}$ og betegnes $(A,+,\cdot)/\mathfrak{a}$ eller $(A/\mathfrak{a},+,\cdot)$ eller blot $A/\mathfrak{a}$.

5.2. Lad $\mathfrak{a}$ være et ideal i ringen $(A,+,\cdot)$. Det er klart, at en ringhomomorfi $f: (A,+,\cdot) \to (B,+,\cdot)$ respekterer $\underset{\mathfrak{a}}{\equiv}$, hvis og kun hvis f forsvinder på $\mathfrak{a}$. Vi får nu let:

(ELLER UDVIDELSESSÆTNING)

HOMOMORFISÆTNING FOR RINGE. *Lad $\mathfrak{a}$ være et ideal i ringen $(A,+,\cdot)$, og lad $O: A \to A/\mathfrak{a}$ være den kanoniske homomorfi ind i kvotientringen. Til hver ringhomomorfi $f: A \to B$, som forsvinder på $\mathfrak{a}$, findes netop én homomorfi $\tilde{f}: A/\mathfrak{a} \to B$, således at $\tilde{f} \circ O = f$.*

$$\begin{array}{ccc} A & \xrightarrow{O} & A/\mathfrak{a} \\ & {\scriptstyle f}\searrow & \swarrow{\scriptstyle \tilde{f}} \\ & B & \end{array}$$

□

5.3 Lad $f: (A,+,\cdot) \to (B,+,\cdot)$ være en ringhomomorfi. Det er let at se, at billedmængden $f(A)$ er en delring af $(B,+,\cdot)$. Specielt er billedmængden selv en ring. Som tidligere nævnt er den til f hørende ækvivalensrelation $\tilde{f}$ en kongruensrelation i $(A,+,\cdot)$. Det tilhørende ideal i $(A,+,\cdot)$ er

$$\mathfrak{o}_f = \{ x \in A \mid f(x) = f(0) \} = f^{-1}(0),$$

som kaldes homomorfiens kerne. Det er klart, at f forsvinder på sin kerne, og f inducerer derfor en homomorfi $\tilde{f}: (A,+,\cdot)/f^{-1}(0) \to (B,+,\cdot)$. Vi får:

ISOMORFISÆTNING FOR RINGE. Lad $f: A \to B$ være en ringhomomorfi med kernen $f^{-1}(0)$. Den inducerede homomorfi $\tilde{f}: A/f^{-1}(0) \to B$ giver da en isomorfi af kvotientringen $A/f^{-1}(0)$ på billedringen $f(A)$.

$$\begin{array}{ccc} A & \xrightarrow{0} & A/f^{-1}(0) \\ \downarrow & & \downarrow\wr\ \tilde{f} \\ B & \hookleftarrow & f(A) \end{array}$$

Bevis □

5.4. Det er let at se, at der for en ringhomomorfi $f: A \to B$ gælder, at originalmængden $f^{-1}(b)$ af et ideal $b \subseteq B$ er et ideal i A. Derimod gælder i almindelighed ikke, at billedmængden $f(\mathfrak{a})$ af et ideal i A er et ideal i B, thi selv om $f(\mathfrak{a})$ er en additiv undergruppe i B, kan vi for $y \in B$ og $b = f(a) \in f(\mathfrak{a})$ ikke slutte at også $yf(a) \in f(\mathfrak{a})$. Er f imidlertid surjektiv, kan vi skrive $y = f(x)$, $x \in A$ og $b = f(a)$, $a \in \mathfrak{a}$, og ser, at $yb = f(x)f(a) = f(xa) \in f(\mathfrak{a})$, og tilsvarende, at $by \in f(\mathfrak{a})$. I dette tilfælde er altså $f(\mathfrak{a})$ et ideal i B.

Videre gælder nu

NOETHERS ISOMORFISÆTNING FOR RINGE. *Lad $f: A \to A'$ være en surjektiv ringhomomorfi med kerne $\mathfrak{a}_0$. Ved*

$$\mathfrak{a} \longmapsto f(\mathfrak{a}) \qquad \text{og} \qquad f^{-1}(\mathfrak{a}') \longleftarrow \mathfrak{a}'$$

etableres da en bijektiv, ordensbevarende forbindelse

$$\{\mathfrak{a} \mid \mathfrak{a} \text{ er ideal i } \mathfrak{o}, \mathfrak{a} \supseteq \mathfrak{a}_0\} \rightleftarrows \{\mathfrak{a}' \mid \mathfrak{a}' \text{ er ideal i } A'\}.$$

Er $\mathfrak{a} \supseteq \mathfrak{a}_0$ et ideal i A, og er $f(\mathfrak{a})$ det tilsvarende ideal i A', har vi en naturlig isomorfi

$$A/\mathfrak{a} \xrightarrow{\sim} A'/f(\mathfrak{a}),$$

kaldet Noethers isomorfi.

Bevis. Først vises, at de to angivne afbildninger er "hinandens inverse." Da f er surjektiv, gælder for idealer $\mathfrak{a}'$ i A', at $f(f^{-1}(\mathfrak{a}')) = \mathfrak{a}'$. Vi skal altså vise, at der for et ideal $\mathfrak{a} \supseteq \mathfrak{a}_0$ i A gælder

$$f^{-1}(f(\mathfrak{a})) = \mathfrak{a}.$$

Her er "$\supseteq$" klart, og for at vise "$\subseteq$" betragter vi et element $x \in f^{-1}(f(\mathfrak{a}))$. Vi har da $f(x) \in f(\mathfrak{a})$, og kan skrive $f(x) = f(a)$, hvor $a \in \mathfrak{a}$. Nu er $f(x-a) = f(x) - f(a) = 0$, så $x - a \in f^{-1}(0) = \mathfrak{a}_0$. Da $\mathfrak{a}_0 \subseteq \mathfrak{a}$, har vi $x - a \in \mathfrak{a}$, og da også $a \in \mathfrak{a}$ finder vi $x = (x-a) + a \in \mathfrak{a}$. For at bestemme Noethers isomorfi, bemærker vi, at $A \xrightarrow{f} A' \xrightarrow{0} A'/f(\mathfrak{a})$ er surjektiv med kerne $f^{-1}(f(\mathfrak{a})) = \mathfrak{a}$. Isomorfisætningen 5.3 giver derfor den søgte isomorfi. ∎

RINGE

1. Ring. Homomorfi. Delring.

1.1. DEFINITION. En ring er en mængde Λ forsynet med to kompositioner, en addition: $\Lambda \times \Lambda \to \Lambda$ betegnet $(\lambda, \mu) \mapsto \lambda + \mu$ og en multiplikation betegnet $(\lambda, \mu) \mapsto \lambda\mu$ således at følgende er opfyldt:

a) M.h.t. additionen er Λ en kommutativ gruppe. Det neutrale element for additionen kaldes ringens nul-element og betegnes 0. Hvert element $\lambda \in \Lambda$ har m.h.t. additionen et modsat betegnet $-\lambda$. Den additive gruppe betegnes ofte $(\Lambda, +)$ eller Λ^+. Betingelserne kan udtrykkes ved ligningerne:

a1) $\lambda + \mu = \mu + \lambda$

a2) $(\lambda + \mu) + \nu = \lambda + (\mu + \nu)$

a3) $\lambda + 0 = \lambda$

a4) $\lambda + (-\lambda) = 0$.

m) M.h.t. multiplikationen er Λ en semigruppe med neutralt element. Det neutrale element for multiplikationen kaldes ringens et-element og betegnes 1 (eller 1_Λ). Den multiplikative semigruppe betegnes ofte $(\Lambda, \cdot)$ eller $\Lambda^\times$. Betingelserne kan udtrykkes ved ligningerne

m1) $\lambda(\mu\nu) = (\lambda\mu)\nu$

m2) $\lambda 1 = 1\lambda = \lambda$.

d) Multiplikationen er distributiv m.h.t. additionen. Betingelsen kan udtrykkes ved ligningerne

d) $\lambda(\mu + \nu) = \lambda\mu + \lambda\nu$, $(\lambda + \mu)\nu = \lambda\nu + \mu\nu$.

1.2. DEFINITION. En afbildning $\varphi : \Gamma \to \Lambda$ mellem ringe Γ og Λ kaldes en (ring-)homomorfi, hvis den respekterer strukturen, d.v.s. hvis der gælder

$$\varphi(\lambda+\mu) = \varphi(\lambda) + \varphi(\mu)$$
$$\varphi(\lambda\mu) = \varphi(\lambda)\,\varphi(\mu)$$
$$\varphi(1) = 1.$$

Ved kernen for en ringhomomorfi $\varphi : \Gamma \to \Lambda$ forstås originalmængden $\varphi^{-1}(0)$. Ringhomomorfien φ er injektiv, hvis og kun hvis kernen $\varphi^{-1}(0) = \{0\}$.

En bijektiv ringhomomorfi kaldes også en isomorfi.

Det er klart, at man ved sammensætning af to ringhomomorfier $\varphi : \Gamma \to \Lambda$ og $\psi : \Delta \to \Gamma$ får en ringhomomorfi $\varphi \circ \psi : \Delta \to \Lambda$. Endvidere er for enhver ring Λ den identiske afbildning en ringhomomorfi (endda en isomorfi) $Id_\Lambda : \Lambda \to \Lambda$.

1.3. DEFINITION. Ved en delring af en ring Λ forstås en delmængde $\Delta \subseteq \Lambda$, der er stabil under kompositionerne, og således at Δ med de inducerede kompositioner er en ring med samme etelement som Λ. Denne sidste betingelse er nødvendig for at sikre, at inklusionsafbildningen er en ringhomomorfi : $\Delta \hookrightarrow \Lambda$.

1.4. Det er let at se, at billedmængden $\varphi(\Gamma)$ ved en ringhomomorfi $\varphi : \Gamma \to \Lambda$ er en delring af Λ, kaldet billedet eller billedringen for φ.

2. Eksempler

2.1. Nulringen er ringen med kun ét element, som altså er 0, og oplagte kompositioner. I denne ring er $1 = 0$. I alle andre ringe gælder $1 \neq 0$.

2.2. Talringene er delringe af ringen $\mathbb{C}$ af komplekse tal. Specielt har vi ringen $\mathbb{Z}$ af hele tal, ringen $\mathbb{Q}$ af rationale tal og ringen $\mathbb{R}$ af reelle tal. Disse ringe er alle kommutative. Til talringene medregnes af og til den ikke kommutative ring $\mathbb{H}$ af kvaternioner.

2.3. I mængden $\{0,1\}$ defineres ved kompositionstavlerne

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

en ring med to elementer.

2.4. Endomorfiringen $\mathrm{End}_L(V)$ for et vektorrum V over legemet L. En endomorfi i V er som bekendt en lineær afbildning $f: V \to V$; addition af to endomorfier f og g defineres argumentvis:

$$f + g : v \longmapsto f(v) + g(v),$$

og multiplikationen er sammensætning $(f, g) \longmapsto f \circ g$.

2.5. Endomorfiringen $\mathrm{End}(M)$ for en kommutativ gruppe M defineres tilsvarende.

Det ses, at endomorfiringen $End_L(V)$ for vektorrummet $(V,+,L)$ er en delring af endomorfiringen for den kommutative gruppe $(V,+)$.

2.6. Funktionsringe. Lad T være en mængde, og lad Λ være en ring. I mængden $Afb(T,\Lambda)$ af afbildninger $: T \to \Lambda$ defineres addition og multiplikation argumentvis, ved

$$f+g : t \longmapsto f(t)+g(t)$$
$$fg : t \longmapsto f(t)g(t).$$

Med disse kompositioner er $Afb(T,\Lambda)$ en ring. Nulelementet i denne ring er den konstante funktion $t \longmapsto 0$, og et-elementet er den konstante funktion $t \longmapsto 1$. Som eksempel på delringe af ringen $Afb([a,b],\mathbb{R})$ kan nævnes ringen $\mathcal{C}^n[a,b]$ af reelle $\mathcal{C}^n$-funktioner på intervallet $[a,b]$.

2.7. Ringen $\Lambda[X]$ af polynomier i én variabel med koefficienter i ringen Λ består af formelle udtryk af formen

$$p_0 + p_1X + p_2X^2 + \cdots + p_nX^n,$$

hvor $p_i \in \Lambda$, $i = 0,1,\cdots,n$. Addition og multiplikation af to sådanne udtryk udregnes efter regler, der er velkendte fra sædvanlige polynomiumsfunktioner. Størrelserne p_0, p_1X, p_2X^2, ... kaldes polynomiets led, og p_i siges at være koefficienten til det i-te led eller at være koefficienten til X^i. Led af formen $1X^i$ skrives sædvanligvis simpelthen X^i, og ofte undlader man at skrive led af formen $0X^i$.

To polynomier regnes for det samme, hvis de har de samme koefficienter.

2.8. En mere præcis definition af et polynomium fås derfor ved at definere et <u>polynomium</u> med koefficienter i ringen Λ som en følge

$$p = (p_0, p_1, p_2, \cdots)$$

af elementer $p_i \in \Lambda$, der <u>er 0 fra et vist trin</u>.*)
For sådanne følger $p = (p_0, p_1, \cdots)$, $q = (q_0, q_1, \cdots)$ defineres additionen ved

$$p + q = (p_0 + q_0, p_1 + q_1, p_2 + q_2, \cdots)$$

altså

$$p + q = (s_0, s_1, \cdots), \quad \text{hvor } s_i = p_i + q_i,$$

og multiplikationen ved

$$pq = (p_0 q_0, p_0 q_1 + p_1 q_0, p_0 q_2 + p_1 q_1 + p_2 q_0, \cdots)$$

altså

$$pq = (t_0, t_1, \cdots), \quad \text{hvor } t_i = \sum_{j+k=i} p_j q_k.$$

Med disse kompositioner organiseres mængden af sådanne følger til en ring, kaldet ringen af <u>polynomier i én variabel med koefficienter i Λ</u>.
og betegnet $\Lambda[X]$.

Polynomier af formen $(\lambda, 0, 0, \cdots)$, hvor $\lambda \in \Lambda$, kaldes <u>konstanter</u>. Ved $\lambda \mapsto (\lambda, 0, 0, \cdots)$ defineres en afbildning $\Lambda \to \Lambda[X]$, der let ses at være en injektiv ringhomomorfi. Ofte identificeres elementerne i Λ med de tilsvarende konstanter. Bemærk, at nul-elementet i $\Lambda[X]$ er konstanten

$$0 = (0, 0, 0, \cdots),$$

og at et-elementet i $\Lambda[X]$ er konstanten

$$1 = (1, 0, 0, \cdots).$$

---

*) At følgen er 0 fra et vist trin betyder, at den kan skrives $p = (p_0, p_1, \cdots, p_n, 0, 0, 0, \cdots)$

For produktet af en konstant $\lambda = (\lambda, 0, 0, \cdots)$ med et vilkårligt polynomium $p = (p_0, p_1, \cdots)$ finder vi

$$\lambda p = (\lambda p_0, \lambda p_1, \cdots) \quad \text{og}$$
$$p\lambda = (p_0\lambda, p_1\lambda, \cdots).$$

Det specielle polynomium $(0,1,0,0,0,\cdots)$ betegnes X. For produktet af $X = (0,1,0,0,\cdots)$ med et vilkårligt polynomium $p = (p_0, p_1, p_2, p_3, \cdots)$ finder vi

$$Xp = pX = (0, p_0, p_1, p_2, \cdots),$$

og for potenserne af X finder vi derfor

$$X = (0,1,0,0,\cdots)$$
$$X^2 = (0,0,1,0,\cdots)$$
$$\vdots$$
$$X^i = (\underbrace{0,0,\cdots,0}_{i \text{ 0'er}},1,0,\cdots$$
$$\vdots$$

Er $p_0, p_1, \cdots, p_n$ konstanter, kan vi i $\Lambda[X]$ betragte elementet $p_0 + p_1X + \cdots + p_nX^n$. Vi finder

$$p_0 + p_1X + \cdots + p_nX^n = (p_0, p_1, \cdots, p_n, 0, 0, \cdots).$$

Et polynomium af formen $p = (p_0, p_1, \cdots, p_n, 0, 0, \cdots)$ kan altså skrives

$$p = p_0 + p_1X + \cdots + p_nX^n.$$

Vi skriver ofte

$$p = \sum_{i \geq 0} p_iX^i,$$

idet jo kun endelig mange led i denne sum er $\neq 0$.

2.9. <u>Ringen $\Lambda[[X]]$ af formelle potensrækker med koefficienter i ringen Λ.</u> Mængden af alle følger

$$p = (p_0, p_1, \cdots)$$

af elementer $p_i \in \Lambda$ organiseres til en ring ved ganske de samme definitioner, som vi har givet for polynomier. Denne ring kaldes ringen af (formelle) potensrækker med koefficienter i Λ og betegnes $\Lambda[[X]]$. Polynomiumsringen $\Lambda[X]$ er en delring af $\Lambda[[X]]$:

$$\Lambda \subseteq \Lambda[X] \subseteq \Lambda[[X]].$$

Potensrækker skrives ofte på formen

$$p = \sum_{i \geq 0} p_i X^i$$

eller

$$p = p_0 + p_1 X + p_2 X^2 + \cdots$$

Denne skrivemåde er formel, og udtrykker blot, at

$$p = (p_0, p_1, p_2, \ldots).$$

2.10. Ringen $\Lambda[X_1, \ldots, X_k]$ af polynomier i k variable med koefficienter i ringen Λ. Vi indskrænker os her til en meget lös beskrivelse af polynomier i 2 variable. Eksempler på sådanne polynomier er

$$X_1 X_2 + X_1^3 X_2^5, \qquad \alpha + \beta X_1^2 + \gamma X_1^5 X_2^7, \quad \alpha, \beta, \gamma \in \Lambda.$$

Regning med sådanne udtryk udføres efter oplagte (!) regler. Mere systematisk kan sådanne polynomier skrives

$$p = p_{00} + (p_{10} X_1 + p_{01} X_2) + \cdots + (p_{n0} X_1^n + p_{n-1,1} X_1^{n-1} X_2 + \cdots + p_{0n} X_2^n)$$

Disse polynomier kan ordnes efter potenser af X_2:

$$p = (p_{00} + p_{10} X_1 + \cdots) + (p_{01} + \cdots + p_{n-1,1} X_1^{n-1}) X_2 + \cdots + (\ \ ) X_2^n.$$

Det ses, at $\Lambda[X_1, X_2]$ kan identificeres med

$$(\Lambda[X_1])[X_2].$$

2.11. Matrixringen $Mat_n(\Lambda)$ af $n\times n$-matricer med elementer fra Λ. Den fra legemer velkendte definition af matricer og deres sum og produkt overføres uden videre til en vilkårlig ring. Delringe af $Mat_n(\Lambda)$ er ringen $Tr_n(\Lambda)$ af øvre trekantsmatricer og ringen $Diag_n(\Lambda)$ af diagonalmatricer.

2.12. Produkt af ringe. Hvis $\Lambda_1, \dots, \Lambda_k$ er ringe, kan produktmængden $\Lambda = \Lambda_1 \times \cdots \times \Lambda_k$ organiseres til en ring ved for $\lambda = (\lambda_1, \dots, \lambda_k)$ og $\mu = (\mu_1, \dots, \mu_k)$ at sætte

$$\lambda + \mu = (\lambda_1 + \mu_1, \dots, \lambda_k + \mu_k)$$

$$\lambda\mu = (\lambda_1\mu_1, \dots, \lambda_k\mu_k).$$

Nul-elementet i denne ring er $0 = (0, \dots, 0)$ og et-elementet er $1 = (1, \dots, 1)$.

2.13. Ved til hvert polynomium $p = p_0 + p_1X + \cdots + p_nX^n$ i $\mathbb{C}[X]$ at lade svare den tilhørende polynomiumsfunktion : $\mathbb{C} \to \mathbb{C}$, $z \mapsto p_0 + p_1z + \cdots + p_nz^n$ defineres en ringhomomorfi : $\mathbb{C}[X] \to Afb(\mathbb{C},\mathbb{C})$. Den er injektiv.

I potensrækkeringen $\mathbb{C}[[X]]$ udgør de formelle potensrækker $p = \sum p_iX^i$, for hvilke den sædvanlige potensrække

$$\sum p_iz^i$$

har positiv konvergensradius, en delring $\mathbb{C}\{X\}$. Ligeledes udgør de formelle potensrækker $p = \sum p_iX^i$, for hvilke rækken $\sum p_iz^i$ er konvergent for alle $z \in \mathbb{C}$, en delring $\mathcal{H}$. Vi har

$$\mathbb{C} \subseteq \mathbb{C}[X] \subseteq \mathcal{H} \subseteq \mathbb{C}\{X\} \subseteq \mathbb{C}[[X]].$$

2.14. For hvert fast $t \in T$ er afbildningen

$$f \longmapsto f(t)$$

en ringhomomorfi : $Afb(T, \Lambda) \to \Lambda$. (jfr. 2.6.)

For hvert fast $i \in \{1, \dots, k\}$ er afbildningen

$$pr_i : \lambda = (\lambda_1, \dots, \lambda_k) \longmapsto \lambda_i$$

en ringhomomorfi : $\Lambda = \Lambda_1 \times \cdots \times \Lambda_k \to \Lambda_i$ (jfr. 2.12.)

2.15. Idet $\mathcal{C}^\infty$ betegner ringen af reelle $\mathcal{C}^\infty$-funktioner på $\mathbb{R}$, defineres ved

$$f \longmapsto \sum_{i \geq 0} \frac{D^i f(0)}{i!} X^i$$

en ringhomomorfi : $\mathcal{C}^\infty \to \mathbb{R}[[X]]$. Den er ikke injektiv. Man kan vise, at den er surjektiv.

2.16. <u>Den kanoniske ringhomomorfi : $\mathbb{Z} \to \Lambda$</u> Til hver ring Λ findes netop én ringhomomorfi : $\mathbb{Z} \to \Lambda$, thi en sådan skal afbilde $1 \in \mathbb{Z}$ over i et-elementet $1_\Lambda \in \Lambda$, og det må derfor være afbildningen

$$n \longmapsto n 1_\Lambda. \quad (= n\text{-te potens af } 1_\Lambda \text{ i } \Lambda^+)$$

Det ses let, at denne afbildning virkelig er en ringhomomorfi. Billedringen kaldes <u>primringen</u> i Λ.

2.17. Ringen D af <u>formelle Dirichletrækker</u> består af alle afbildninger $\alpha : \mathbb{N} \to \mathbb{C}$. Summen af to sådanne afbildninger α og β er den sædvanlige sum

$$\alpha + \beta : n \longmapsto \alpha(n) + \beta(n),$$

og produktet er foldningen

$$\alpha * \beta : n \longmapsto \sum_{d/n} \alpha(d)\beta\left(\frac{n}{d}\right).$$

Der summeres over divisorerne i n (incl. 1 og n). Nulelementet er den konstante funktion $n \mapsto 0$ og et-elementet er funktionen

$$1 : n \longmapsto \begin{cases} 1 & n = 1 \\ 0 & n > 1. \end{cases}$$

2.18. I en ring Λ kan en ny komposition $\Lambda \times \Lambda \to \Lambda$ betegnet $(\lambda, \mu) \mapsto \lambda \overset{op}{\cdot} \mu$ defineres ved

$$\lambda \overset{op}{\cdot} \mu = \mu\lambda, \quad \lambda, \mu \in \Lambda.$$

Med denne nye komposition som multiplikation fremkommer en ny ring $(\Lambda, +, \overset{op}{\cdot})$, der kaldes den <u>modsatte</u> ring, og betegnes Λ^{op}. Hvis Λ er kommutativ, har vi naturligvis $\Lambda = \Lambda^{op}$.

2.19. En afbildning $\varphi : \Gamma \to \Lambda$ mellem ringe kaldes en <u>antihomomorfi</u>, hvis der gælder

$$\varphi(\lambda + \mu) = \varphi(\lambda) + \varphi(\mu)$$
$$\varphi(\lambda\mu) = \varphi(\mu)\varphi(\lambda) \qquad \lambda, \mu \in \Gamma$$
$$\varphi(1) = 1$$

En antihomomorfi $\varphi : \Gamma \to \Lambda$ er således det samme som en ringhomomorfi : $\Gamma \to \Lambda^{op}$ (eller : $\Gamma^{op} \to \Lambda$).

F.eks. gælder for en kommutativ ring R, at transponering : $\alpha \mapsto {}^t\alpha$ er en isomorfi

$$Mat_n(R) \xrightarrow{\sim} Mat_n(R)^{op}$$

For en ikkekommutativ ring Λ er transponering en isomorfi: $Mat_n(\Lambda) \xrightarrow{\sim} Mat_n(\Lambda^{op})^{op}$

I kvaternionlegemet $\mathbb{H}$ (skævlegemet) er konjugering : $w \mapsto \bar{w}$ en isomorfi: $\mathbb{H} \xrightarrow{\sim} \mathbb{H}^{op}$.

3. Foldningsringe

3.1. Lad der være givet en ring Λ og en semigruppe $(S,*)$ med neutralt element e. Med $\Lambda[S]$ betegner vi mængden af de afbildninger $\varphi: S \to \Lambda$, for hvilke

$\varphi(s) \neq 0$ kun gælder for endelig mange $s \in S$.

Hvis S er endelig, er dette naturligvis altid opfyldt.

I $\Lambda[S]$ defineres en addition $+$ ved at summen $\varphi+\psi$ er den sædvanlige sum

$$\varphi+\psi : s \longmapsto \varphi(s)+\psi(s).$$

Endvidere defineres en komposition $*$ ved at foldningen $\varphi*\psi$ er afbildningen

$$\varphi*\psi : s \longmapsto \sum_{u*v=s} \varphi(u)\psi(v).$$

Med disse kompositioner er $(\Lambda[S],+,*)$ en ring, hvis et-element er afbildningen

$$\delta_e : s \longmapsto \begin{cases} 1 & \text{hvis } s=e \\ 0 & \text{hvis } s\neq e. \end{cases}$$

3.2. For hvert $\lambda \in \Lambda$ betegner vi med $\tilde{\lambda}$ den ved

$$\tilde{\lambda} : s \longmapsto \begin{cases} \lambda & \text{hvis } s=e \\ 0 & \text{hvis } s\neq e \end{cases}$$

definerede afbildning $\tilde{\lambda}: S \to \Lambda$. Det er klart, at $\tilde{\lambda} \in \Lambda[S]$, og $\lambda \longmapsto \tilde{\lambda}$ er en injektiv ringhomomorfi $: \Lambda \to \Lambda[S]$. Vi vil altid identificere elementerne $\lambda \in \Lambda$ med de tilsvarende elementer $\tilde{\lambda} \in \Lambda[S]$, altså opfatte Λ som en delring $\Lambda \subseteq \Lambda[S]$.

Med denne identifikation finder vi for "produktet" af et element $\lambda \in \Lambda$ med et element $\varphi \in \Lambda[S]$, at $\lambda * \varphi$ er afbildningen

$$s \longmapsto \lambda \varphi(s).$$

3.3. For hvert $u \in S$ betegner vi med $\delta_u \in \Lambda[S]$ den ved

$$\delta_u : s \longmapsto \begin{cases} 1 & \text{hvis } s = u \\ 0 & \text{hvis } s \neq u \end{cases}$$

definerede afbildning. Vi finder

$$\delta_u * \delta_v = \delta_{u*v},$$

og $u \longmapsto \delta_u$ er en injektiv homomorfi $(S,*) \to (\Lambda[S],*)$. Vi har

$$\begin{array}{ccc} \Lambda & \hookrightarrow & \Lambda[S] \\ & \nwarrow^{} & \uparrow \\ & & S \end{array}$$

Til et givet element $\varphi \in \Lambda[S]$ findes endelig mange elementer $u_1, \dots, u_k \in S$, således at $\varphi(s) = 0$ når $s \neq u_1, \dots, u_k$. Sætter vi $\lambda_i = \varphi(u_i)$, finder vi

$$\varphi = \lambda_1 * \delta_{u_1} + \dots + \lambda_k * \delta_{u_k}.$$

Hvert element $\varphi \in \Lambda[S]$ har en entydig fremstilling af denne art. Vi skriver også fremstillingen

$$\varphi = \sum_{u \in S} \lambda_u * \delta_u,$$

idet kun endelig mange elementer i summen er $\neq 0$.

3.4. Er komposition en i S betegnet multiplikativt, og undlader vi som sædvanlig tegnet for produktet i ringen $\Lambda[S]$, har vi

$$\delta_u \delta_v = \delta_{uv}.$$

Hvis misforståelser er udelukkede, identificerer

vi elementerne $u \in S$ med deres billeder $\delta_u \in \Lambda[S]$, opfatter altså S som en delmængde $S \subseteq \Lambda[S]$. Med denne identifikation består elementerne φ i $\Lambda[S]$ af endelige summer

$$\varphi = \lambda_1 u_1 + \cdots + \lambda_k u_k, \quad \lambda_i \in \Lambda, \ u_i \in S,$$

som også skrives

$$\varphi = \sum_{u \in S} \lambda_u u.$$

3.5. Er kompositionen i S additivt skrevet (og betegner 0 det neutrale element i S) skriver vi ofte X^u for δ_u. I ringen $\Lambda[S]$ har vi da

$$X^u X^v = X^{u+v}$$

og

$$X^0 = 1 \text{ er et-elementet i } \Lambda[S].$$

Elementerne i $\Lambda[S]$ er endelige summer

$$\varphi = \lambda_1 X^{u_1} + \cdots + \lambda_k X^{u_k},$$

som også skrives

$$\varphi = \sum_{u \in S} \lambda_u X^u.$$

3.6. Eksempel. $S = (\mathbb{N}_0, +)$ er semigruppen af hele tal $i \geqslant 0$. Vi har $X^0 = 1$, og sætter vi $X = X^1$, finder vi $X^i = X^{1+\cdots+1} = X^1 \cdots X^1 = X \cdots X$. Altså er X^i virkelig den i-te potens af elementet $X \in \Lambda[\mathbb{N}_0]$. Det ses, at $\Lambda[\mathbb{N}_0]$ er den tidligere definerede polynomiumsring $\Lambda[X]$.

3.7. Eksempel. $S = (\mathbb{N}_0^n, +)$ er semigruppen af n-sæt $i = (i_1, \cdots, i_n)$ af hele tal $i_\nu \geqslant 0$ (multiindices) med koordinatvis addition.

For $\nu = 1, \cdots, n$ sætter vi

$$X^{(0,\cdots,1,\cdots,0)} = X_\nu .$$

For et multiindex $i = (i_1, \cdots, i_n) \in \mathbb{N}_0^{\,n}$ har vi

$$i = i_1 (1,0,\cdots,0) + \cdots + i_n (0,0,\cdots,1),$$

så vi finder

$$X^i = X^{(i_1,\cdots,i_n)} = \left[X^{(1,0,\cdots,0)}\right]^{i_1} \cdots \left[X^{(0,0,\cdots,1)}\right]^{i_n}$$

$$= X_1^{i_1} \cdots X_n^{i_n},$$

et produkt af potenser af elementerne $X_1, \cdots, X_n$ i ringen $\Lambda[\mathbb{N}_0^{\,n}]$. Ringen $\Lambda[\mathbb{N}_0^{\,n}]$ betegnes også $\Lambda[X_1, \cdots, X_n]$ og dens elementer kaldes polynomier i n variable med koefficienter i Λ. Ethvert sådant kan entydigt skrives som en endelig sum

$$\sum_{i=(i_1,\cdots,i_n)} \lambda_i X^i = \sum \lambda_{i_1,\cdots,i_n} X_1^{i_1} \cdots X_n^{i_n}.$$

3.8. <u>Rækker</u>. Hvis semigruppen $(S,*)$ har den egenskab, at der for hvert element $s \in S$ kun findes endelig mange par $(u,v) \in S \times S$, således at $u * v = s$, kan foldningen

$$\varphi * \psi : s \longmapsto \sum_{u*v=s} \varphi(u)\,\psi(v)$$

defineres for vilkårlige afbildninger $\varphi, \psi : S \to \Lambda$. I dette tilfælde organiseres mængden af alle afbildninger $\varphi : S \to \Lambda$ med oplagt addition og foldning som multiplikation til en ring betegnet $\Lambda[[S]]$. Vi har

$$\Lambda \subseteq \Lambda[S] \subseteq \Lambda[[S]].$$

Specielt har vi $\delta_u \in \Lambda[[S]]$ for hvert $u \in S$,

men kun elementerne i $\Lambda[S]$ kan skrives som endelige summer

$$\varphi = \lambda_1 * \delta_{u_1} + \cdots + \lambda_k * \delta_{u_k}.$$

Alligevel skriver man ofte formelt for et element $\varphi \in \Lambda[[S]]$:

$$\varphi = \sum_{u \in S} \lambda_u * \delta_u,$$

som blot udtrykker, at $\varphi(u) = \lambda_u$ for alle $u \in S$.

3.9. Eksempel. $S = (\mathbb{N}_0, +)$ har den i 3.8. nævnte egenskab. Ringen $\Lambda[[\mathbb{N}_0]]$ betegnes også $\Lambda[[X]]$ og dens elementer kaldes <u>formelle potensrækker</u>. Disse kan skrives

$$\sum \lambda_i X^i = \lambda_0 + \lambda_1 X + \lambda_2 X^2 + \cdots$$

3.10. Eksempel. $S = (\mathbb{N}_0^n, +)$ har den i 3.8. nævnte egenskab. Ringen $\Lambda[[\mathbb{N}_0^n]]$ betegnes også $\Lambda[[X_1, \ldots, X_n]]$ og dens elementer kaldes <u>formelle potensrækker i n variable</u>. Disse kan skrives

$$\sum_{i=(i_1,\ldots,i_n)} \lambda_i X^i = \sum \lambda_{i_1,\ldots,i_n} X_1^{i_1} \cdots X_n^{i_n}.$$

3.11. Eksempel. $S = (\mathbb{N}, \cdot)$, semigruppen af naturlige tal med multiplikation som komposition, har den i 3.8. nævnte egenskab. Ringen $\Lambda[[\mathbb{N}]]$ kaldes ringen af <u>formelle Dirichlet rækker</u> (jfr. 2.17.).

4. Regulære og invertible elementer.

4.1. DEFINITION. Et element λ i ringen Λ kaldes invertibelt, hvis der findes et element $\mu \in \Lambda$, så at

$$\lambda\mu = \mu\lambda = 1.$$

og det betegnes λ^{-1}.

Et sådant element μ er da entydigt bestemt. De invertible elementer i Λ udgør (med multiplikation som komposition) en gruppe, der sædvanligvis betegnes Λ^*. Gruppen Λ^* er en undergruppe i semigruppen $(\Lambda, \cdot) = \Lambda^\times$.

4.2. DEFINITION. Et element λ i ringen Λ kaldes regulært, hvis der for alle $\xi \in \Lambda$ gælder

$$\xi \neq 0 \Rightarrow \lambda\xi \neq 0 \wedge \xi\lambda \neq 0$$

Det er klart, at de invertible elementer i Λ er regulære. De regulære elementer udgør en semiundergruppe i $(\Lambda, \cdot) = \Lambda^\times$.

4.3. DEFINITION. I ringen Λ siges nulreglen at gælde, hvis vi for alle $\lambda, \xi \in \Lambda$ har

$$\xi \neq 0 \wedge \lambda \neq 0 \Rightarrow \xi\lambda \neq 0.$$

Nulreglen udsiger altså, at alle elementer $\neq 0$ i Λ er regulære.

4.4. DEFINITION. Ringen Λ kaldes et skrivelegeme, hvis

$$\Lambda^* = \Lambda \setminus \{0\}.$$

Definitionen udsiger dels, at hvert element $\lambda \neq 0$ er invertibelt, dels at 0 ikke er invertibel. Herved udelukkes altså nulringen.

Et kommutativt skævlegeme kaldes også et <u>legeme</u>.

4.5. DEFINITION. En ring Λ kaldes et <u>integritetsområde</u>, hvis

$$\{\text{regulære elementer i } \Lambda\} = \Lambda \setminus \{0\}.$$

Definitionen udsiger dels, at nulreglen gælder i Λ, dels at 0 ikke er regulært. Herved udelukkes altså nulringen. Et skævlegeme er et integritetsområde.

4.6. Eksempler. I nulringen er alle (!) elementer invertible, men nulringen er ikke et integritetsområde. (jfr. 2.1.)

Talringene $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{H}$ er integritetsområder. $\mathbb{Q}, \mathbb{R}$ og $\mathbb{C}$ er legemer, og $\mathbb{H}$ er et skævlegeme. Det er klart, at $\mathbb{Z}^* = \{1, -1\}$. (jfr. 2.2.)

Ringen med elementerne 0 og 1 (jfr 2.3.) er et legeme.

De invertible elementer i ringen (jfr. 2.4.) $\Lambda = \mathrm{End}_L(V)$ er <u>automorfierne</u> : $V \to V$. Gruppen Λ^* betegnes også $\mathrm{Aut}_L(V)$. I ringen $\mathrm{End}_L(V)$ er de regulære elementer invertible. [I det endeligdimensionale tilfælde kan man f. eks. udnytte, at for et regulært element $f \in \mathrm{End}_L(V)$ er $g \mapsto g \circ f$ en lineær, injektiv afbildning mellem endeligdimensionale vektorrum]

Tilsvarende er de invertible elementer

i ringen $End(M)$, hvor $(M,+)$ er en kommutativ gruppe, netop automorfierne $: M \to M$. I almindelighed findes i $End(M)$ regulære elementer, der ikke er invertible.

Et element i en funktionsring $Afb(T, \Lambda)$ er invertibelt (resp. regulært), hvis og kun hvis $f(t)$ er invertibel (resp. regulær) i Λ for alle $t \in T$.

4.7. Ved en ringhomomorfi $\varphi: \Lambda \to \Gamma$ vil et invertibelt element $\lambda \in \Lambda$ afbildes på et invertibelt element i Γ (og $\varphi(\lambda)^{-1} = \varphi(\lambda^{-1})$). Der kan derimod intet siges om billedet af et regulært element.

4.8. Vi betragter ringen $\Lambda[X]$ af polynomier med koefficienter i ringen Λ. Det er klart, at invertible (resp. regulære) elementer i Λ opfattet som polynomier er invertible (resp. regulære) i $\Lambda[X]$. (jfr. 2.7., 2.8. eller 3.6.).

For et polynomium $p = p_0 + p_1 X + \cdots + p_n X^n \neq 0$ defineres <u>graden</u>, betegnet $\deg(p)$, som det største tal i, for hvilket $p_i \neq 0$. At

$$\deg(p) = d$$

betyder altså, at

$$p = p_0 + p_1 X + \cdots + p_d X^d, \quad p_d \neq 0.$$

eller en grad, der er $<$ alle andre grader

Nul-polynomiet 0 tillægges bekvemt graden $-\infty$.

For sum og produkt af polynomier p og q finder vi

$$\deg(p+q) \leqslant \max\{\deg(p), \deg(q)\}$$

$$\deg(pq) \leqslant \deg(p) + \deg(q).$$

(med oplagt konvention for regning med $-\infty$).

4.9. SÆTNING. *Lad Λ være et integritetsområde. For polynomier $p, q \in \Lambda[X]$ gælder da*

$$\deg(pq) = \deg(p) + \deg(q).$$

$\Lambda[X]$ er et integritetsområde, og de invertible polynomier er netop de invertible konstanter.

Bevis. Antag, at p og q er polynomier $\neq 0$, med $\deg(p) = n$, $\deg(q) = m$. Vi har så

$$p = p_0 + p_1 X + \cdots + p_n X^n \qquad p_n \neq 0$$

$$q = q_0 + q_1 X + \cdots + q_m X^m \qquad q_m \neq 0,$$

og for produktet pq finder vi

$$pq = p_0 q_0 + (p_0 q_1 + p_1 q_0) X + \cdots + p_n q_m X^{n+m}.$$

Her er $p_n q_m \neq 0$, da nulreglen gælder i Λ, og det følger, at $\deg(pq) = n + m$. Specielt er $pq \neq 0$.

Den sidste påstand følger let, thi hvis $pq = 1$, finder vi $\deg(p) + \deg(q) = \deg(1) = 0$, og så må $\deg(p) = 0$, dvs. p er en konstant. ▨

4.10. Eksempel. En potensrække $p = \sum p_i X^i$ med koefficienter i ringen Λ er invertibel (regulær) i $\Lambda[[X]]$, hvis og kun hvis konstantleddet p_0 er invertibelt i Λ.

Lad os vise, at en potensrække

$$p = p_0 + p_1 X + p_2 X^2 + \cdots,$$ hvor p_0 er invertibel i Λ, er invertibel i $\Lambda[[X]]$. Vi søger først en potensrække

$$q = q_0 + q_1 X + q_2 X^2 + \cdots$$

således at $pq = 1$. Hertil kræves, at

$$\begin{aligned} p_0 q_0 &= 1 \\ p_0 q_1 + p_1 q_0 &= 0 \\ p_0 q_2 + p_1 q_1 + p_2 q_0 &= 0 \\ &\vdots \\ p_0 q_i + \cdots + p_i q_0 &= 0 \\ &\vdots \end{aligned}$$

Da p_0 er invertibel i Λ, kan vi rekursivt bestemme først q_0, dernæst q_1, dernæst q_2 o.s.v. således at disse ligninger er opfyldt. Vi finder

$$q_0 = p_0^{-1},\ q_1 = p_0^{-1}(-p_1 q_0),\ q_2 = p_0^{-1}(-p_1 q_1 - p_2 q_0),\ \cdots$$

Tilsvarende indses, at der findes en potensrække $\tilde{q}$, således at $\tilde{q}p = 1$, men så følger det, at p er invertibel (og at $q = \tilde{q}$), thi

$$\tilde{q} = \tilde{q}\cdot 1 = \tilde{q}(pq) = (\tilde{q}p)q = 1q = q. \quad \square$$

Hvis Λ er et integritetsområde, bliver $\Lambda[[X]]$ ligeledes et integritetsområde. Dette følger ganske som for polynomier.

4.11. For kvadratiske matricer med koefficienter i en <u>kommutativ</u> ring R defineres <u>determinanten</u> ganske som for matricer med koefficienter i legemer.

Er $\alpha = (\alpha_{ij}) \in \mathrm{Mat}_n(R)$, sættes

$$\det(\alpha) = \sum_{\sigma \in S_n} (\operatorname{sgn}\sigma)\, \alpha_{1,\sigma(1)} \cdots \alpha_{n,\sigma(n)}.$$

En lang række velkendte egenskaber ved determinant af matricer overføres uden videre til denne større klasse af matricer.

<u>Kofaktormatricen</u> α^J defineres ved

$$\alpha^J : (i,j) \longmapsto (-1)^{i+j} \det(\alpha^{ji});$$

her er α^{ji} den $(n-1)\times(n-1)$ matrix, der fremgår af α ved at slette den j-te række og den i-te søjle. Der gælder

$$\alpha\,\alpha^J = \alpha^J \alpha = (\det\alpha)\, 1_n,$$

hvor $1_n = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$ er et-elementet i $\mathrm{Mat}_n(R)$.

Det følger, at en matrix α er invertibel i $Mat_n(R)$, hvis og kun hvis determinanten $\det\alpha$ er invertibel i R, thi er $\alpha\beta = 1_n$, får vi $\det(\alpha)\det(\beta) = \det(1_n) = 1$, og ser, at $\det\alpha$ er invertibel i R. Er omvendt $\det\alpha$ invertibel i R, følger det af formlen, at matricen

$$(\det\alpha)^{-1}\alpha^J$$

er invers til α.

Gruppen af invertible matricer i $Mat_n(R)$ betegnes $GL_n(R)$ og kaldes den generelle lineære gruppe med koefficienter i R. En undergruppe heri er gruppen $SL_n(R)$ af matricer med determinant $= 1$, kaldet den speciælle lineære gruppe med koefficienter i R.

4.12 De invertible (resp. regulære) elementer i en produktring $\Lambda = \Lambda_1 \times \cdots \times \Lambda_k$ er elementerne

$$\lambda = (\lambda_1, \ldots, \lambda_k),$$

hvor λ_i er invertibel (resp. regulær) i Λ_i, $i = 1, \ldots, k$. (jfr. 2.12.)

4.13. Gauske som for formelle potensrækker kan man indse, at en formel Dirichletrække $\alpha : \mathbb{N} \to \mathbb{C}$ er invertibel i D (jfr. 2.17 eller 3.11.), hvis og kun hvis $\alpha(1)$ er invertibel i $\mathbb{C}$ (d.v.s. $\neq 0$). En Dirichlet række $\alpha : \mathbb{N} \to \mathbb{C}$, som opfylder

$$\alpha(1) = 1 \quad \text{og} \quad \alpha(nm) = \alpha(n)\alpha(m), \text{ når } n, m \text{ er primiske},$$

kaldes multiplikativ. De multiplikative Dirichletrækker er invertible i D. De udgør endda en undergruppe i D^*.

Bemærk, at en multiplikativ Dirichletrække α er helt bestemt ved sine værdier $\alpha(p^\nu)$ på primtalspotenser p^ν.

Eksempel. Funktionen $\zeta: n \mapsto 1$ er multiplikativ. Dens inverse er Möbius' μ-funktion defineret ved

$$\mu(n) = \begin{cases} 1 & \text{hvis } n=1 \\ (-1)^r & \text{hvis } n = p_1 \cdots p_r \text{ er produkt af } r \text{ forsk. primtal.} \\ 0 & \text{ellers.} \end{cases}$$

For at vise, at $\zeta * \mu = 1$, skal vi vise, at

$$\zeta * \mu\,(n) = \begin{cases} 1 & n=1 \\ 0 & \text{ellers,} \end{cases}$$

og da μ er multiplikativ, er det nok at vise denne påstand når $n = p^\nu$ er en primtalspotens, og dette er let.

Funktionen $\tau = \zeta * \zeta$ er bestemt ved

$$\tau(n) = \sum_{d/n} 1 \cdot 1 = (\text{antal divisorer i } n);$$

denne funktion er altså multiplikativ.
Funktionen $\iota: n \mapsto n$ er klart multiplikativ, og følgelig er også funktionen $\sigma = \iota * \zeta$ multiplikativ. Vi finder

$$\sigma(n) = \sum_{d/n} d \cdot 1 = (\text{summen af divisorerne i } n).$$

Funktionen $\varphi(n) = \sum_{(a,n)=1} 1 = (\text{antal tal} \leq n \text{ og primiske med } n)$
er Eulers φ-funktion. Behændig summation giver $\varphi * \zeta = \iota$. (!). Det følger, at $\varphi = \iota * \mu$, så φ er multiplikativ. Vi finder nu

$$\varphi(p^\nu) = p^\nu - p^{\nu-1} = p^\nu\left(1 - \tfrac{1}{p}\right) \text{ og}$$

generelt

$$\varphi(n) = n\left(1-\tfrac{1}{p_1}\right)\cdots\left(1-\tfrac{1}{p_r}\right), \quad n = p_1^{\nu_1}\cdots p_r^{\nu_r}.$$

5. Ideal og kvotientring

5.1. DEFINITION. En delmængde $\mathfrak{a}$ af ringen Λ kaldes et *ideal* i Λ, hvis

i1) $\mathfrak{a}$ er en undergruppe i den additive gruppe Λ^+, d.v.s. $\mathfrak{a}$ er ikke tom, og

i1') $\alpha \in \mathfrak{a} \wedge \beta \in \mathfrak{a} \Rightarrow \alpha + \beta \in \mathfrak{a}$

i1") $\alpha \in \mathfrak{a} \Rightarrow -\alpha \in \mathfrak{a}$

og i2) $\mathfrak{a}$ er stabil over for multiplikation med elementer fra Λ, d.v.s. vi har

$$\lambda \in \Lambda \wedge \alpha \in \mathfrak{a} \Rightarrow \lambda\alpha \in \mathfrak{a} \wedge \alpha\lambda \in \mathfrak{a}.$$

5.2. De *trivielle* idealer i Λ er delmængderne $\{0\}$ (også betegnet (0)) og Λ.

5.3. Idealerne i ringen $\mathbb{Z}$ er delmængderne af formen

$$n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$$

med et entydigt bestemt $n \geqslant 0$. Mere generelt gælder i enhver ring Λ, at delmængderne

$$n\Lambda = \{n\lambda \mid \lambda \in \Lambda\}, \quad n \in \mathbb{Z}$$

er idealer i Λ.

5.4. Kernen $\varphi^{-1}(0)$ for en ringhomomorfi $\varphi : \Gamma \to \Lambda$ er et ideal i Γ. Mere generelt ses det let, at originalmængden $\varphi^{-1}(\mathfrak{a})$ af et ideal $\mathfrak{a}$ i Λ er et ideal i Γ.

5.5. Lad Λ være en ring. Kernen for den

kanoniske homomorfi : $\mathbb{Z} \to \Lambda$ (defineret ved $p \mapsto p1_\Lambda$) er et ideal i $\mathbb{Z}$, altså af formen $n\mathbb{Z}$ med et entydigt bestemt helt tal $\geqslant 0$. Dette tal kaldes ringens <u>karakteristik</u> og betegnes $\mathrm{Char}(\Lambda)$. At Λ har karakteristik 0 betyder, at vi i Λ har

$$p1 = 1 + \cdots + 1 \neq 0 \quad \text{for alle } p \geqslant 1.$$

At Λ har karakteristik $n \geqslant 1$ betyder, at vi i Λ har

$$p1 = 1 + \cdots + 1 \begin{cases} \neq 0 & \text{når } 1 \leqslant p < n \\ = 0 & \text{når } p = n. \end{cases}$$

5.6. <u>For et integritetsområde (specielt for et skævlegeme) Λ er karakteristikken 0 eller et primtal</u>, thi er karakteristikken n et sammensat tal:

$$n = n'n'', \quad 1 < n' < n, \quad 1 < n'' < n,$$

så er $n' \notin n\mathbb{Z}$, $n'' \notin n\mathbb{Z}$ og i ringen Λ har vi $n'1_\Lambda \neq 0$, $n''1_\Lambda \neq 0$. Men så er

$$(n'1_\Lambda)(n''1_\Lambda) = (n'n'')1_\Lambda = n1_\Lambda = 0,$$

og nulreglen gælder ikke i Λ ▨

5.7. <u>I en kommutativ ring Λ af primtalskarakteristik p gælder</u>

$$\underline{(\lambda+\mu)^p = \lambda^p + \mu^p}, \quad \lambda, \mu \in \Lambda$$

thi i en kommutativ ring Λ kan $(\lambda+\mu)^p$ udregnes ved binomialformlen

$$(\lambda+\mu)^p = \sum_{i=0}^{p} \binom{p}{i} \lambda^i \mu^{p-i}$$

$$= \lambda^p + \mu^p + \sum_{0<i<p} \binom{p}{i} \lambda^i \mu^{p-i}.$$

Hvis p er et primtal, er binomialkoefficienterne

$$\binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{i(i-1)\cdots 3\cdot 2\cdot 1}, \quad 0 < i < p$$

alle delelige med p (primfaktorerne i nævneren er alle $< p$, så primfaktoren p i tælleren kan ikke bortforkortes). Heraf følger påstanden.

Det følger, at afbildningen $\lambda \mapsto \lambda^p$ er en ringhomomorfi $\Lambda \to \Lambda$, idet vi for enhver kommutativ ring har $(\lambda\mu)^p = \lambda^p\mu^p$ og $1^p = 1$.

5.8. Som bekendt er der en entydig forbindelse mellem idealer i ringen Λ og kongruensrelationer i $(\Lambda, +, \cdot)$. Kongruensrelationen hørende til idealet $\mathfrak{a}$ kaldes "kongruens modulo $\mathfrak{a}$" og betegnes $\underset{\mathfrak{a}}{\equiv}$. Den er defineret ved

$$\lambda \underset{\mathfrak{a}}{\equiv} \mu \iff \mu - \lambda \in \mathfrak{a}.$$

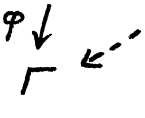
Den tilhørende kvotientring betegnes $\Lambda/\mathfrak{a}$. Ækvivalensklassen, der indeholder λ er delmængden

$$\lambda + \mathfrak{a} = \{\lambda + \alpha \mid \alpha \in \mathfrak{a}\} \subseteq \Lambda.$$

Opfattes den som element i $\Lambda/\mathfrak{a}$, betegnes den ofte $\textcircled{\lambda}$. Afbildningen $\lambda \mapsto \textcircled{\lambda}$ er den kanoniske homomorfi $O : \Lambda \to \Lambda/\mathfrak{a}$.

5.9. Som bekendt gælder følgende

UDVIDELSESSÆTNING. *En ringhomomorfi $\varphi : \Lambda \to \Gamma$, der forsvinder på idealet $\mathfrak{a}$ i Λ kan entydigt udvides til en homomorfi $\tilde{\varphi} : \Lambda/\mathfrak{a} \to \Gamma$.* Dette betyder, at der findes netop en homomorfi $\tilde{\varphi} : \Lambda/\mathfrak{a} \to \Gamma$, således at $\tilde{\varphi} \circ O = \varphi$.



Homomorfien $\tilde{\varphi}: \Lambda/\mathfrak{a} \to \Gamma$ siges at være <u>induceret</u> af homomorfien $\varphi: \Lambda \to \Gamma$.

5.10. Videre gælder

ISOMORFISÆTNINGEN. <u>Lad $\varphi: \Lambda \to \Gamma$ være en ringhomomorfi med kernen $\varphi^{-1}(0)$. Den inducerede homomorfi : $\Lambda/\varphi^{-1}(0) \to \Gamma$ giver da en isomorfi $\tilde{\varphi}: \Lambda/\varphi^{-1}(0) \xrightarrow{\sim} \varphi(\Lambda)$ mellem kvotienten $\Lambda/\varphi^{-1}(0)$ og billedet $\varphi(\Lambda)$.</u>

$$\begin{array}{ccc} \Lambda & \xrightarrow{0} & \Lambda/\varphi^{-1}(0) \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\tilde{\varphi}} \\ \Gamma & \longleftarrow & \varphi(\Lambda) \end{array}.$$

Hvis $\varphi: \Lambda \to \Gamma$ specielt er surjektiv, får vi en isomorfi : $\Lambda/\varphi^{-1}(0) \xrightarrow{\sim} \Gamma$.

5.11. Endelig minder vi om

NOETHERS ISOMORFISÆTNING. <u>Lad $\varphi: \Lambda \to \Lambda'$ være en surjektiv ringhomomorfi med kernen $\mathfrak{a}_0$. Ved</u>

$$\mathfrak{a} \longmapsto \varphi(\mathfrak{a})$$

<u>og</u>

$$\varphi^{-1}(\mathfrak{a}') \longmapsto \mathfrak{a}'$$

<u>etableres da en bijektiv, ordenstro forbindelse:</u>

<u>$\{\mathfrak{a} \mid \mathfrak{a}$ er ideal i Λ, $\mathfrak{a} \supseteq \mathfrak{a}_0\} \leftrightarrows \{\mathfrak{a}' \mid \mathfrak{a}'$ er ideal i $\Lambda'\}$.</u>

<u>Er $\mathfrak{a}$ et ideal i Λ og er $\varphi(\mathfrak{a})$ det tilsvarende ideal i Λ', så har vi en naturlig isomorfi:</u>

$$\Lambda/\mathfrak{a} \xrightarrow{\sim} \Lambda'/\mathfrak{a}'$$

Til et givet ideal $\mathfrak{a}_0$ i Λ kan denne isomorfisætning anvendes på den kanoniske homomorfi: $\Lambda \to \Lambda/\mathfrak{a}_0$. Herved fås en beskrivelse af idealerne i kvotienten $\Lambda/\mathfrak{a}_0$.

Er $\mathfrak{a} \supseteq \mathfrak{a}_0$ et ideal i Λ bruges ofte betegnelsen $\mathfrak{a}/\mathfrak{a}_0$ for det tilsvarende ideal i $\Lambda/\mathfrak{a}_0$. Den bijektive forbindelse udsigen altså, at hvert ideal i $\Lambda/\mathfrak{a}_0$ er af formen $\mathfrak{a}/\mathfrak{a}_0$, hvor $\mathfrak{a} \supseteq \mathfrak{a}_0$ er et entydigt bestemt ideal i Λ. Noethers isomorfi er her en isomorfi:

$$\Lambda/\mathfrak{a} \xrightarrow{\sim} (\Lambda/\mathfrak{a}_0)/(\mathfrak{a}/\mathfrak{a}_0).$$

5.12. Kvotienten $\Lambda/n\Lambda$ betegnes også Λ/n. Specielt har vi kvotienten $\mathbb{Z}/n$, kaldet restklasseringen modulo n. At $\textcircled{p} = \textcircled{r}$ i $\mathbb{Z}/n$ betyder, at $p - r \in n\mathbb{Z}$, altså at vi kan skrive

$$p = nq + r.$$

Det følger, at ringen $\mathbb{Z}/n\mathbb{Z}$ har de n elementer

$$\textcircled{0}, \textcircled{1}, \textcircled{2}, \dots, \textcircled{n-1}.$$

At $\textcircled{p} = \textcircled{r}$, med $0 \leqslant r < n$, betyder, at r er den principale rest af p ved division med n.

Lad Λ være en ring af karakteristik n. Den kanoniske homomorfi: $\mathbb{Z} \to \Lambda$ har da kernen $n\mathbb{Z}$, og billedet er primringen i Λ. Isomorfisætningen giver nu en isomorfi

$$\mathbb{Z}/n \xrightarrow{\sim} \text{primringen i } \Lambda.$$

Vi siger ofte, at en ring af karakteristik n indeholder $\mathbb{Z}/n$.

5.13. Lad $n = n_1 \cdots n_r$ være et produkt af parvis primiske tal $n_1, \dots, n_r$. Ringen $\mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_r$ har da karakteristik n, thi med oplagte betegnelser har vi

$$p1 = p(\textcircled{1}_1, \dots, \textcircled{1}_r) = (\textcircled{p}_1, \dots, \textcircled{p}_r) = 0 \Leftrightarrow n_i \mid p,\ i = 1, \dots, r$$
$$\Leftrightarrow n \mid p.$$

Følgelig har vi en injektiv ringhomo-

morfi: $\mathbb{Z}/n \longrightarrow \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_r$,
og da de to ringe har samme elementantal ($n = n_1 \cdots n_r$), er den en isomorfi. (Den kinesiske restklassesætning)

5.14. SÆTNING. *Enhver ring Λ med p elementer, hvor p er et primtal, er et legeme isomorft med $\mathbb{Z}/p$.*

Bevis. Lad $\lambda \neq 0$ være et element i Λ. Mængden

$$\{r\lambda \mid r \in \mathbb{Z}\} \subseteq \Lambda$$

af (additive) potenser af λ er da en undergruppe i $(\Lambda, +)$, og dens orden er følgelig en divisor i $p = |\Lambda|$. Da denne undergruppe ud over 0 indeholder elementet λ, kan ordenen ikke være 1, og den må følgelig være p, men så må vi have

$$\{r\lambda \mid r \in \mathbb{Z}\} = \Lambda;$$

specielt kan vi skrive

$$1 = r\lambda$$

med passende $r \in \mathbb{Z}$. Af $1 = r\lambda = (r1_\Lambda)\lambda = \lambda(r1_\Lambda)$ følger, at elementet $r1_\Lambda \in \Lambda$ er invers til λ. Altså er Λ et skævlegeme.

Anvendes argumentet på elementet $1_\Lambda \in \Lambda$, ses, at den kanoniske homomorfi $r \longmapsto r1_\Lambda$ af $\mathbb{Z} \to \Lambda$ er surjektiv. Heraf følger den sidste påstand, og vi ser specielt, at Λ er kommutativ, altså et legeme. ▨

Restklasseringen $\mathbb{Z}/p$, hvor p er et primtal, er altså et legeme. Dette legeme betegnes ofte $\mathbb{F}_p$.

5.15. SÆTNING. *Ethvert endeligt integritetsområde Λ er et skævlegeme. Dets karakteristik er et primtal p, og dets elementantal er en potens p^d af dette primtal.*

Bevis. Lad $\lambda \neq 0$ være et element i Λ. Afbildningen

$$\mu \longmapsto \mu\lambda$$

er da en homomorfi $\Lambda^+ \longrightarrow \Lambda^+$. Da nulreglen gælder i Λ, er denne homomorfi injektiv, og da Λ er en endelig mængde må den være bijektiv. Specielt er $1 \in \Lambda$ et billede ved denne afbildning, d.v.s. vi har

$$\mu\lambda = 1$$

med et passende $\mu \in \Lambda$. Tilsvarende findes et $\tilde{\mu} \in \Lambda$, således at $\lambda\tilde{\mu} = 1$, og nu slutter vi, at $\mu = \tilde{\mu}$ er invers til λ. Altså er Λ et skævlegeme.

At karakteristikken p for et integritetsområde er 0 eller et primtal, har vi allerede set, og her er 0 udelukket, da $|\Lambda|$ er endelig. Vi kan antage, at Λ indeholder legemet $\mathbb{Z}/p = \mathbb{F}_p$.

Ved multiplikationen i Λ har vi produktet

$$(\alpha, \lambda) \longmapsto \alpha\lambda, \quad \alpha \in \mathbb{F}_p\ (\subseteq \Lambda),\ \lambda \in \Lambda.$$

Herved organiseres Λ øjensynlig til et vektorrum over legemet $\mathbb{F}_p$. Dette vektorrum må være endeligdimensionalt, da det kun indeholder endelig mange elementer. Er $e_1, \dots, e_d$ en basis for $(\Lambda, +, \mathbb{F}_p)$, har hvert element $\lambda \in \Lambda$ en entydig fremstilling

$$\lambda = \alpha_1 e_1 + \cdots + \alpha_d e_d, \quad \alpha_i \in \mathbb{F}_p.$$

For hvert α_i er der p muligheder, så Λ må indeholde $p \cdots p = p^d$ elementer. ▨

Bemærk. Man kan vise, at ethvert endeligt skævlegeme er kommutativt.

5.16. SÆTNING. *De regulære elementer i ringen $\mathbb{Z}/n$ er restklasserne af formen $\overline{a}$, hvor a og n ikke har fælles divisorer. Disse elementer er alle invertible.*

Bevis. Et element $\lambda \in \mathbb{Z}/n$ kan skrives $\lambda = \overline{a}$, hvor $a \in \mathbb{Z}$. Hvis λ er regulær, er $\mu \mapsto \mu\lambda$ en injektiv afbildning $\mathbb{Z}/n \to \mathbb{Z}/n$, og den er derfor bijektiv. Specielt har vi $1 = \mu\lambda$ for et passende $\mu \in \mathbb{Z}/n$, og det følger, at λ er invertibel i $\mathbb{Z}/n$. Skriver vi $\mu = \overline{b}$, $b \in \mathbb{Z}$, har vi

$$\overline{ba} = \overline{b}\,\overline{a} = \mu\lambda = 1 = \overline{1},$$

altså $1 - ba \in n\mathbb{Z}$, og vi kan skrive

$$1 = ba + nx, \quad \text{hvor } x \in \mathbb{Z}.$$

En fælles divisor i a og n går også op i $ba + nx = 1$, og den må derfor være 1 (eller -1). Altså har a og n kun denne trivielle divisor fælles.

Antager vi omvendt, at $\lambda = \overline{a}$ ikke er regulær, findes et $\mu = \overline{b} \neq 0$, så at $0 = \mu\lambda = \overline{b}\,\overline{a} = \overline{ba}$. Vi har da $ba \in n\mathbb{Z}$ og $b \notin n\mathbb{Z}$, og heraf følger som bekendt, at a og n har en primdivisor fælles. ▨

Hvis a og n ikke har fælles divisorer, siger vi at *a og n er primiske*, og vi skriver $(a, n) = 1$. Restklassen $\overline{a}$ kaldes da en *primisk restklasse* i $\mathbb{Z}/n$.

Eksempel. Hvis $n = p$ er et primtal, er restklasserne $\overline{1}, \overline{2}, \ldots, \overline{p-1}$ øjensynlig primiske i $\mathbb{Z}/p$. I følge sætningen er de derfor invertible i $\mathbb{Z}/p$ og da de udgør samtlige elementer $\neq 0$ i $\mathbb{Z}/p$ har vi på ny bevist, at $\mathbb{Z}/p$ (p primtal) er et legeme.

KOROLLAR. *Hvis $(a, n) = 1$, findes hele tal b og x således at $ab + nx = 1$.* □

5.17. Gruppen $(\mathbb{Z}/n)^*$ af invertible elementer i ringen $\mathbb{Z}/n$ er gruppen af primiske restklasser @. Dens orden er

$$\varphi(n) = \sum_{(a,n)=1} 1$$

hvor der summeres over naturlige tal $\leqslant n$, primiske med n. Funktionen $n \longmapsto \varphi(n)$ er Eulers φ-funktion (jfr. 4.13.). For hvert element λ i gruppen $(\mathbb{Z}/n)^*$ er $\lambda^{\varphi(n)}$ det neutrale element i $(\mathbb{Z}/n)^*$, altså

$$\lambda^{\varphi(n)} = 1,$$

og vi får

<u>Hvis a og $n \geqslant 1$ er primiske hele tal, så er $a^{\varphi(n)} - 1$ delelig med n.</u>

Hvis $n = p$ er et primtal, finder vi $\varphi(p) = p-1$, og får

"FERMAT'S LILLE SÆTNING". <u>Lad p være et primtal. Hvis $a \in \mathbb{Z}$ ikke er delelig med p, så er $a^{p-1} - 1$ delelig med p.</u>

Er $n = n_1 \cdots n_r$ et produkt af parvis primiske tal $n_1, \ldots, n_r$, så har vi en ringisomorfi (jfr 5.13): $\mathbb{Z}/n \xrightarrow{\sim} \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_r$. Heraf får vi en gruppeisomorfi

$$(\mathbb{Z}/n)^* \xrightarrow{\sim} (\mathbb{Z}/n_1)^* \times \cdots \times (\mathbb{Z}/n_r)^*$$

mellem gruppene af invertible elementer. Sammenlignes elementantallene, ser vi, at

$$\varphi(n) = \varphi(n_1) \cdots \varphi(n_r),$$

og vi har således endnu en gang (jfr. 4.13) vist, at Eulers φ-funktion er multiplikativ.

5.18. Lad Λ være en ring, og betragt matrixringen $\Gamma = Mat_n(\Lambda)$. Hvis $\mathfrak{o} \subseteq \Lambda$ er et ideal, så udgør de matricer $\alpha \in \Gamma$, for hvilke $\alpha_{\nu\mu} \in \mathfrak{o}$ for alle ν, μ, et ideal i Γ, som vi naturligt betegner $Mat_n(\mathfrak{o})$. Det ses, at $Mat_n(\mathfrak{o})$ er kernen for ringhomomorfien $Mat_n(\Lambda) \to Mat_n(\Lambda/\mathfrak{o})$. Der gælder nu omvendt

<u>Ethvert ideal $\mathfrak{A}$ i $Mat_n(\Lambda)$ er af formen $Mat_n(\mathfrak{o})$, hvor $\mathfrak{o}$ er et (entydigt bestemt) ideal i Λ.</u>

Bevis. For $p, q = 1, \dots, n$ betegner vi med $\varepsilon^{pq} \in Mat_n(\Lambda)$ den matrix, der har 1 på den (p,q)-te plads, og 0 på de øvrige pladser. Er $\gamma \in Mat_n(\Lambda)$ en vilkårlig matrix, finder vi let

$$\varepsilon^{pq} \gamma \varepsilon^{rs} = \gamma_{qr} \varepsilon^{ps}$$

Lad nu $\mathfrak{A} \subseteq Mat_n(\Lambda)$ være et ideal, og sæt

$$\mathfrak{o} = \{ \lambda \in \Lambda \mid \exists \alpha \in \mathfrak{A} : \alpha_{11} = \lambda \}.$$

Det er let at se, at $\mathfrak{o}$ er et ideal i Λ.

Vi påstår, at $\mathfrak{A} = Mat_n(\mathfrak{o})$. Er $\alpha \in \mathfrak{A}$, finder vi, at $\alpha_{qr} \varepsilon^{11} = \varepsilon^{1q} \alpha \varepsilon^{r1} \in \mathfrak{A}$, og slutter, at $\alpha_{qr} \in \mathfrak{o}$, $q, r = 1, \dots, n$. Vi har således $\mathfrak{A} \subseteq Mat_n(\mathfrak{o})$.

For at vise den omvendte inklusion er det nok at vise, at der for enhver matrix $\lambda \varepsilon^{ps}$ med $\lambda \in \mathfrak{o}$ gælder $\lambda \varepsilon^{ps} \in \mathfrak{A}$. Dette følger tilsvarende, thi der findes en matrix $\alpha \in \mathfrak{A}$ med $\alpha_{11} = \lambda$, og vi finder

$$\lambda \varepsilon^{ps} = \varepsilon^{p1} \alpha \varepsilon^{1s} \in \mathfrak{A}. \quad \blacksquare$$

Specielt fremhæves følgende

KOROLLAR. <u>Matrixringen $Mat_n(D)$ med koefficienter i et skævlegeme D har kun (de to) trivielle idealer.</u>

6. Kommutation. Centrum.

6.1. DEFINITION. Lad Λ være en ring og lad $T \subseteq \Lambda$ være en delmængde. Mængden af elementer $\lambda \in \Lambda$, der kommuterer med alle elementer i T kaldes T's <u>kommutant</u> i Λ og betegnes T^c, altså

$$T^c = \{\lambda \in \Lambda \mid \forall \gamma \in T : \lambda\gamma = \gamma\lambda\}.$$

SÆTNING. <u>Lad T være en delmængde af ringen Λ. Kommutanten T^c er en delring af Λ, $T \subseteq T^{cc}$ og $T^{ccc} = T^c$.</u>

Bevis. At T^c er en delring af Λ vises let. At $T \subseteq T^{cc}$ følger let af definitionen. Anvendes dette resultat på delmængden T^c, får vi $T^c \subseteq T^{ccc}$; den omvendte inklusion følger af at der generelt gælder

$$S \subseteq T \Rightarrow T^c \subseteq S^c. \quad \blacksquare$$

6.2. Kommutantens kommutant T^{cc} kaldes også <u>bikommutanten</u>

6.3. DEFINITION. Lad Λ være en ring. Kommutanten for Λ selv kaldes Λ's <u>centrum</u> og betegnes $\mathrm{Cent}(\Lambda)$, altså

$$\mathrm{Cent}(\Lambda) = \Lambda^c = \{\lambda \in \Lambda \mid \forall \gamma \in \Lambda : \lambda\gamma = \gamma\lambda\}.$$

Det er klart, at centret for Λ er en kommutativ delring af Λ. Elementer, der ligger i centret, siges at være <u>centrale</u>.

6.4. Elementerne i primringen for Λ er centrale, thi disse elementer er af formen $n1_\Lambda$, $n \in \mathbb{Z}$. For et fast $\lambda \in \Lambda$ kan vi betragte afbildningerne

$$n \longmapsto (n1_\Lambda)\lambda \,, \quad n \longmapsto \lambda(n1_\Lambda) \,, \quad n \longmapsto n\lambda.$$

Disse afbildninger er homomorfier: $(\mathbb{Z},+) \to (\Lambda,+)$, og da de stemmer overens, når $n=1$, stemmer de overens for alle $n \in \mathbb{Z}$.

6.5 Elementet X er centralt i polynomiumsringen $\Lambda[X]$. Derimod er konstanterne i $\Lambda[X]$ ikke nødvendigvis centrale.

6.6. Ringen Λ kan opfattes som delring af ringen $\mathrm{Mat}_n(\Lambda)$ af $(n \times n)$-matricer $(n \geqslant 1)$ med koefficienter i Λ v.h.a. af afbildningen

$$\lambda \longmapsto \begin{pmatrix} \lambda & & 0 \\ & \lambda & \\ 0 & & \lambda \end{pmatrix}.$$

For en kommutativ ring R gælder, at R er centret i $\mathrm{Mat}_n(R)$. For $r,s = 1,\dots,n$ betegner vi med $\delta^{r,s}$ matricen $\delta^{r,s} = (\delta^{r,s}_{i,j})$, hvor

$$\delta^{r,s}_{i,j} = \begin{cases} 1 & \text{hvis } (i,j) = (r,s) \\ 0 & \text{ellers.} \end{cases}$$

Hvis matricen $\alpha = (\alpha_{kl})$ ligger i centret for $\mathrm{Mat}_n(R)$, har vi $\alpha\delta^{r,s} = \delta^{r,s}\alpha$, som ved udregning giver ligningerne

$$\alpha_{rr} = \alpha_{ss} \,, \quad \alpha_{kr} = \alpha_{sl} = 0, \text{ når } \begin{matrix} r \neq k \\ s \neq l, \end{matrix}$$

hvoraf følger, at $\alpha \in R$. Omvendt er det klart, at elementerne i R er centrale i $\mathrm{Mat}_n(R)$.

6.7. Eksempel. Lad V være et endeligtdimensionalt vektorrum over legemet L. I ringen $\Lambda = End(V)$ af (additive) endomorfier $: (V,+) \to (V,+)$ kan vi betragte delringen $End_L(V)$ af lineære endomorfier $: (V,+,L) \to (V,+,L)$. For hvert $\lambda \in L$ kan vi betragte homotetien $\lambda_V : v \mapsto \lambda v$,

$$\lambda_V : V \to V;$$

disse homotetier udgør ligeledes en delring L_V af $End(V)$.

I ringen $End(V)$ gælder

$$L_V{}^c = End_L(V), \quad End_L(V)^c = L_V$$

Bevis. Den første påstand er triviel, thi at en additiv homomorfi $: V \to V$ kommuterer med alle homotetierne, betyder netop, at den er lineær. Lad os vise den anden påstand: Vi har $End_L(V) \supseteq L_V$. En additiv homomorfi, der kommuterer med elementerne i $End_L(V)$, vil altså specielt kommutere med elementerne i L_V, og vil altså være lineær. Heraf følger, at kommutanten $End_L(V)^c$ for $End_L(V)$ i $End(V)$ netop er centret af $End_L(V)$. At dette centrum består af homotetierne fås som konsekvens af 6.6. ved at vælge en basis for V. Efter dette valg kan endomorfiringen $End_L(V)$ som bekendt identificeres med matrixringen $Mat_n(L)$, hvor $n = \dim V$.

6.8. DEFINITION. En ringhomomorfi $\varphi : \Gamma \to \Lambda$ kaldes <u>central</u> hvis elementerne $\varphi(\gamma)$, $\gamma \in \Gamma$ er centrale i Λ, altså hvis

$$\varphi(\Gamma) \subseteq Cent(\Lambda).$$

6.9. Eksempler. Den kanoniske homomorfi: $\mathbb{Z} \to \Lambda$ er altid central. (jfr. 6.4.)

Inklusionshomomorfien

$$\mathrm{Cent}(\Lambda) \hookrightarrow \Lambda$$

er central.

Hvis Λ er en kommutativ ring, er enhver ringhomomorfi $\Gamma \to \Lambda$ central.

Afbildningen $R \hookrightarrow \mathrm{Mat}_n(R)$, hvor R er en kommutativ ring, er central (trivielt). Tilsvarende er den ved homotetierne i et vektorrum $(V,+,L)$ bestemte afbildning $\lambda \longmapsto \lambda_V$ en central ringhomomorfi: $L \to \mathrm{End}_L(V)$.

Hvis R er en kommutativ ring, og $R[S]$ er foldningsringen over en semigruppe S med neutralt element, er afbildningen

$$R \hookrightarrow R[S] \qquad \text{(jfr. 3.2.)}$$

en central ringhomomorfi.

7. Associative algebraer over en kommutativ ring.

7.1. I det følgende betegner R en kommutativ ring.

7.2. DEFINITION. Ved en <u>associativ algebra over R</u> forstås en ring A forsynet med en central ringhomomorfi $\varphi: R \to A$.

At φ er central, betyder som bekendt, at elementerne $\varphi(r)$, $r \in R$ er centrale i ringen A, altså at der gælder

$$\varphi(r)\, a = a\, \varphi(r) \quad , \quad r \in R \, , \; a \in A.$$

En associativ algebra over R kaldes i det følgende en <u>R-algebra</u> (eller en algebra over R)

7.3. Enhver ring A kan opfattes som en $\mathbb{Z}$-algebra via den kanoniske ringhomomorfi: $\mathbb{Z} \to A$.

En ring A kan opfattes som algebra over enhver delring af centret for A. Specielt kan en ring opfattes som algebra over sin primring.

Matrixringene $\mathrm{Mat}_n(R)$ er R-algebraer; afbildningen $R \to \mathrm{Mat}_n(R)$ er givet ved $r \longmapsto \begin{pmatrix} r & & 0 \\ & r & \\ & & \ddots \\ 0 & & r \end{pmatrix}$.

Funktionsringene $\mathrm{Afb}(T, R)$ er R-algebraer; afbildningen $R \to \mathrm{Afb}(T, R)$ er givet ved

$$r \longmapsto (\text{konstante funktion } t \mapsto r).$$

Polynomiumsringen $R[X]$ er en R-algebra; afbildningen $R \to R[X]$ er inklusionen $R \hookrightarrow R[X]$.

Mere generelt er foldningsringen $R[S]$, hvor S er en semigruppe med neutralt element, en R-algebra

7.4. Mere udførligt kan vi for R-algebra A skrive $(A,+,\cdot,R)$ eller $(A,+,\cdot,\varphi)$ eller (A,φ).

7.5. Hvis (A,φ) er en R-algebra, defineres en ydre komposition $R\times A \to A$, betegnet $(r;a) \longmapsto ra$, ved

$$ra = \varphi(r)a.$$

Der gælder

$$\text{(I)} \begin{cases} r(a_1+a_2) = ra_1 + ra_2, & r\in R,\ a_1,a_2\in A \\ (r_1+r_2)a = r_1a + r_2a, & r_1,r_2\in R \quad a\in A \\ (r_1r_2)a = r_1(r_2a), & r_1,r_2\in R \quad a\in A \\ 1a = a, & (1 \text{ er et-elementet i } R),\ a\in A \end{cases}$$

samt

$$\text{(II)} \qquad r(a_1a_2) = (ra_1)\cdot a_2 = a_1\cdot(ra_2), \quad r\in R,\ a_1,a_2\in A.$$

De første ligninger er netop de betingelser vi kræver for multiplikation med skalarer i et vektorrum. Det følger, at en algebra over et legeme specielt kan opfattes som et vektorrum over dette legeme.
Bemærk, at $\varphi(r) = r1$, (1 er et-elementet i A).

7.6 Har vi omvendt givet en mængde A forsynet med to kompositioner: en <u>addition</u>: $A\times A \to A$ betegnet

$$(a,b) \longmapsto a+b,$$

en <u>multiplikation</u>: $A\times A \to A$ betegnet

$$(a,b) \longmapsto a\cdot b$$

og en <u>(ydre) multiplikation</u>: $R\times A \to A$ betegnet

$$(r,a) \longmapsto ra$$

således at følgende betingelser er opfyldt:

(0) $(A,+)$ er en kommutativ gruppe
(I) som ovenfor
(II) som oven for
(III) $\cdot$ er distributiv m.h.t. $+$
(IV) $(A,\cdot)$ er en semigruppe med neutralt element,

så kan A opfattes som en associativ algebra over R. Betingelserne (0), (III) og (IV) udsiger jo, at $(A,+,\cdot)$ er en ring, og at (I) og (II) udledes let, at afbildningen $r \longmapsto r1$ er en central homomorfi $: (R,+,\cdot) \to (A,+,\cdot)$.

Bemærkning. Betingelsen (IV) udsiger, at

(IV) $a\cdot(b\cdot c) = (a\cdot b)\cdot c$, $a,b,c \in A$,

samt at der findes et neutralt element for multiplikationen. Erstattes betingelsen IV med andre betingelser, defineres andre typer af (ikke-associative) algebraer. Ved betingelsen

(IV') $\begin{cases} a\cdot a = 0 \\ a\cdot(b\cdot c) + b\cdot(c\cdot a) + c\cdot(a\cdot b) = 0 \end{cases}$ $a,b,c \in A$

defineres således en <u>Lie-algebra</u>, ved betingelsen

IV'' $\begin{cases} a\cdot b = b\cdot a \\ (a\cdot b)\cdot(a\cdot a) = a\cdot[b\cdot(a\cdot a)] \end{cases}$ $a,b \in A$

defineres en <u>Jordan-algebra</u> og ved betingelsen

IV''' $\begin{cases} (a\cdot a)\cdot b = a\cdot(a\cdot b) \\ a\cdot(b\cdot b) = (a\cdot b)\cdot b \end{cases}$

defineres en <u>alternativ algebra</u>. Som nævnt reserverer vi betegnelsen <u>algebra</u> til de i 7.2. definerede associative algebraer.

7.7. DEFINITION. En <u>delalgebra</u> af R-algebraen (A,φ) er en delring $C \subseteq A$, således at $\varphi(R) \subseteq C$. Vi har da $\varphi : R \to C$ og kan opfatte C som R-algebra. Tilsvarende defineres for et ideal $\mathfrak{a} \subseteq A$ <u>kvotientalgebraen</u> $A/\mathfrak{a}$.

7.8. DEFINITION. Lad (A', φ') og (A'', φ'') være R-algebraer. Ved en <u>algebrahomomorfi</u> $f: A' \to A''$ forstås en ringhomomorfi $f: A' \to A''$, for hvilken $f \circ \varphi' = \varphi''$:

$$\begin{array}{ccc} A' & \xrightarrow{f} & A'' \\ & {\scriptstyle\varphi'}\nwarrow \quad \nearrow{\scriptstyle\varphi''} & \\ & R & \end{array}$$

At $f \circ \varphi' = \varphi''$, kan også udtrykkes ved at

$$f(ra) = r f(a), \qquad r \in R,\ a \in A'.$$

Det er klart, at identiteten er en algebrahomomorfi $Id_A: A \to A$, og at vi ved sammensætning af to algebrahomomorfier, $f: A' \to A''$, $g: A'' \to A'''$, får en algebrahomomorfi $g \circ f: A' \to A'''$.

For en delalgebra $C \subseteq A$ er inklusionsafbildningen en algebrahomomorfi $: C \hookrightarrow A$.

For en kvotientalgebra A/σ er den kanoniske homomorfi en algebrahomomorfi $: A \to A/\sigma$.

For en algebrahomomorfi $f: A' \to A''$ er billedet $f(A') \subseteq A''$ en delalgebra.

7.9. DEFINITION. Lad a være et element i R-algebraen A, og lad

$$p = p_0 + p_1 X + p_2 X^2 + \cdots + p_n X^n$$

være et polynomium i $R[X]$. Elementet $p_0 1 + p_1 a + \cdots + p_n a^n$ i A betegnes $p(a)$, altså

$$p(a) = p_0 1 + p_1 a + p_2 a^2 + \cdots + p_n a^n \in A,$$

og det siges at fremkomme ved at <u>indsætte elementet a i polynomiet p</u>.

Hvis $p(a) = 0$, siger vi, at p i algebraen A har <u>roden</u> a.

Indsættes i polynomiet $p = p_0 + \cdots + p_n X^n$ elementet $X \in R[X]$, får vi naturligvis polynomiet p igen. Der gælder altså $p = p(X)$.

7.10. Eksempel. Polynomiet $X^2+1 \in \mathbb{Z}[X]$ har ingen rødder i $\mathbb{Z}$, ingen rødder i $\mathbb{Q}$ og ingen rødder i $\mathbb{R}$. Det har rødderne i og $-i$ i $\mathbb{C}$, og det har uendelig mange rødder i $\mathbb{H}$. Det har "dobbeltroden" 1 i legemet $\mathbb{F}_2 = \mathbb{Z}/2$, og det har rødderne (8), (18), (47) og (57) i ringen $\mathbb{Z}/65$.

7.11. Lad V være et k-dimensionalt vektorrum over legemet L. Endomorfiringen $\mathrm{End}_L(V)$ er en L-algebra, idet homomorfien $L \to \mathrm{End}_L(V)$ er givet ved

$$\lambda \longmapsto \text{homoteti med } \lambda.$$

Som bekendt har $\mathrm{End}_L(V)$, som vektorrum over L, dimensionen k^2. Er $f \in \mathrm{End}_L(V)$, findes derfor en egentlig lineær relation, mellem de k^2+1 elementer

$$1, f, f^2, \ldots, f^{k^2} \text{ i } \mathrm{End}_L(V);$$

Dette betyder imidlertid, at f er rod i et polynomium af grad $\leqslant k^2$ i $L[X]$.

Man kan vise, at enhver endomorfi f i $\mathrm{End}_L(V)$ er rod i sit karakteristiske polynomium p_f, der er af grad k. (Hamilton-Cayley's sætning; vist for $L=\mathbb{R}$ og $L=\mathbb{C}$).

7.12. SÆTNING. Lad a være et element i R-algebraen A. Der findes da netop én R-algebra homomorfi

$$R[X] \to A, \quad \text{så at } X \longmapsto a,$$

nemlig afbildningen

$$p \longmapsto p(a).$$

Billedalgebraen ved denne homomorfi er den mindste delalgebra af A, som indeholder a, og kernen består af de polynomier i $R[X]$, der har a som rod.

Bevis. Trivielt. □

7.13. Den mindste delalgebra af A, som indeholder et givet element $a \in A$ kaldes <u>delalgebraen frembragt af a</u>, og betegnes $R[a]$. Vi har altså

$$R[a] = \{ p_0 1 + p_1 a + \cdots + p_n a^n \mid n \geqslant 0;\ p_0, \ldots, p_n \in R \}.$$

I følge isomorfisætningen inducerer homomorfien

$$p \longmapsto p(a)$$

en isomorfi

$$R[X]/\text{kernen} \xrightarrow{\sim} R[a] \quad (\subseteq A).$$

Delalgebraen $R[a]$ er altså isomorf med en kvotient af $R[X]$. Specielt er altså $R[a]$ en kommutativ ring. Vi giver nu en nærmere beskrivelse af visse kvotienter af $R[X]$.

7.14 SÆTNING OM DIVISION MED REST. <u>Lad</u>

$$\underline{d = d_n X^n + \cdots + d_0}$$

<u>være et polynomium i $R[X]$ af grad n, således at højestegradskoefficienten d_n er invertibel i R. Til hvert polynomium $p \in R[X]$ findes da entydigt bestemte polynomier $q, r \in R[X]$, så at</u>

$$\underline{p = qd + r \ , \quad \deg(r) < \deg(d) (= n).}$$

Bevis. Vi skal vise, at der til et givet polynomium p findes netop ét polynomium q, så at

$$\deg(p - qd) < \deg(d).$$

Hvis $\deg(p) < \deg(d)$, så er dette øjensynlig kun opfyldt for $q = 0$. Hvis $\deg(p) = k \geqslant \deg(d) = n$, må vi have $\deg(q) = k - n$, altså

$$q = q_{k-n} X^{k-n} + \ldots$$

og sammenligning af højestegradskoefficienterne giver

$$p_k = q_{k-n} d_n, \quad \text{altså } q_{k-n} = p_k d_n^{-1}$$

Vi ser nu, at polynomiet $p(X) - p_k d_n^{-1} X^{k-n} d(X)$ har grad $< k$. Idet vi bruger fuldstændig induktion efter k, kan vi altså skrive

$$p(X) - p_k d_n^{-1} X^{k-n} d(X) = \tilde{q}(X) d(X) + r(X)$$

hvor $\deg(r) < \deg(d)$. Følgelig har vi

$$p(X) = q(X) d(X) + r(X),$$

med

$$q(X) = p_k d_n^{-1} X^{k-n} + \tilde{q}(X).$$

Entydigheden følger ligeledes, idet det entydigt bestemte polynomium $\tilde{q}(X)$ åbenbart har grad $< n-k$. □

7.15. Hvis R er et legeme, ser vi, at divisionssætningen kan anvendes på ethvert polynomium $d \neq 0$. For en vilkårlig ring R kan divisionssætningen specielt anvendes på ethvert normeret polynomium, d.v.s. et polynomium $d \neq 0$, hvor højestegrads-koefficienten er 1.

7.16. For et givet polynomium $d \in R[X]$ ser vi let, at delmængden

$$\{ qd \mid q \in R[X] \} \subseteq R[X]$$

er et ideal. Det betegnes (d), (og kaldes hovedidealet frembragt af polynomiet d.)

KOROLLAR. *Lad $d = X^n + d_{n-1} X^{n-1} + \cdots + d_0 \in R[X]$ være et normeret polynomium, og lad $\textcircled{X}$ betegne billedet af X i kvotientalgebraen $R[X]/(d)$. Hvert element λ i kvotientalgebraen $R[X]/(d)$ har da en fremstilling*

$$\lambda = r_0 \textcircled{1} + r_1 \textcircled{X} + \cdots + r_{n-1} \textcircled{X}^{n-1},$$

og koefficienterne $r_0, \ldots, r_{n-1} \in R$ er entydigt bestemte.

Vi har $\textcircled{X}^n = -d_0 \textcircled{1} - d_1 \textcircled{X} - \cdots - d_{n-1} \textcircled{X}^{n-1}$.

Bevis. Hvert element $\lambda \in R[X]/(d)$ er af formen $\lambda = \overline{p(X)}$. Nu kan vi bestemme polynomier $q, r \in R[X]$, så at $p = qd + r$, $\deg(r) < n$. Men så er $p - r = qd$, altså $p - r \in (d)$, og vi har $\overline{p(X)} = \overline{r(X)}$ i $R[X]/(d)$. Da $\deg(r) < n$, kan vi skrive

$$r(X) = r_0 + r_1 X + \cdots + r_{n-1} X^{n-1},$$

og vi finder så

$$\lambda = \overline{r(X)} = \overline{r_0} + \overline{r_1}\,\overline{X} + \cdots + \overline{r_{n-1}}\,\overline{X}^{n-1}$$
$$= r_0\overline{1} + r_1\overline{X} + \cdots + r_{n-1}\overline{X}^{n-1}.$$

Entydigheden af $r_0, \ldots, r_{n-1}$ følger af entydigheden i divisionssætningen.
Den sidste ligning følger af at vi i $R[X]/(d)$ har $\overline{d(X)} = 0$, altså

$$\overline{X}^n + d_{n-1}\overline{X}^{n-1} + \cdots + d_0\overline{1} = 0. \quad \square$$

Bemærk, at kvotientalgebraen $R[X]/(d)$ er helt bestemt ved denne beskrivelse.

7.17. For hvert element $a \in R$ kan vi betragte 1ste grads polynomiet $X - a$. Anvendes divisionssætningen herpå, ser vi, at ethvert polynomium $p(X) \in R[X]$ entydigt kan skrives

$$p(X) = q(X)(X - a) + r(X)$$

hvor $\deg(r) < 1$. At $\deg(r) < 1$ betyder imidlertid, at $r(X)$ er konstant, og ved indsættelse af a ser vi, at denne konstant må være $p(a)$. Vi har altså

$$p(X) = q(X)(X - a) + p(a),$$

og vi udleder:

SÆTNING. *Polynomiet $p \in R[X]$ har i R roden a, hvis og kun hvis det kan skrives på formen*

$$p(X) = q(X)(X-a).$$ ∎

KOROLLAR. *Hvert polynomium $p \neq 0$ af grad n i $R[X]$ har en fremstilling*

$$p(X) = \tilde{p}(X)(X-a_1)\cdots(X-a_k)$$

hvor $a_1, \ldots, a_k \in R$, og hvor polynomiet $\tilde{p}$ ikke har rødder i R. Hvis R er et integritetsområde, så er fremstillingen entydig, og

$$\{a_1, \ldots, a_k\} = \{a \in R \mid p(a) = 0\}.$$

Bevis. Hvis p ikke har rødder i R, har vi den ønskede fremstilling med $\tilde{p} = p$ (og $r = 0$). Hvis p har en rod $a_1 \in R$, kan vi skrive $p(X) = p_1(X)(X-a_1)$, og her er $\deg(p_1) = \deg(p) - 1 = n-1$. Idet vi fortsætter således med p_1, får vi efter højst n skridt den ønskede fremstilling.

Lad nu R være et integritetsområde. Ud fra en fremstilling $p(X) = \tilde{p}(X)(X-a_1)\cdots(X-a_k)$, hvor $\tilde{p}(X)$ ikke har rødder i R, får vi

$$\{a_1, \ldots, a_k\} = \{a \in R \mid p(a) = 0\},$$

thi "$\subseteq$" er oplagt, og omvendt: er $p(a) = 0$, så har vi

$$0 = \tilde{p}(a)(a-a_1)\cdots(a-a_k);$$

her er $\tilde{p}(a) \neq 0$, og da nulreglen gælder, må en af de øvrige faktorer være 0.

Entydigheden vises nu ved induktion efter $n = \deg(p)$. Den er klar, hvis $n = 0$, idet p så er en konstant. Er $n > 0$, og har vi endnu en fremstilling

$$p(X) = \tilde{q}(X)\,(X-b_1)\cdots(X-b_\ell),$$

hvor $\tilde{q}$ ikke har rødder i R, så er b rod i p, altså ifølge det viste b_ℓ = et af a_i'erne. Vi kan antage, at $b_\ell = a_k$. Af

$$p(X) = \tilde{p}(X)(X-a_1)\cdots(X-a_k) = \tilde{q}(X)(X-b_1)\cdots(X-b_{\ell-1})(X-a_k)$$

følger imidlertid (entydigheden i divisionssætningen), at

$$\tilde{p}(X)(X-a_1)\cdots(X-a_{k-1}) = \tilde{q}(X)(X-b_1)\cdots(X-b_{\ell-1});$$

dette er fremstillingen af et polynomium af grad $n-1$, og induktionsforadsætningen viser derfor, at $\tilde{p} = \tilde{q}$, $k-1 = \ell-1$, og at vi (eventuelt efter permutation) har $a_1 = b_1, \ldots, a_{k-1} = b_{k-1}$. ▨

7.18 Eksempel. ① For $R = \mathbb{C}$ gælder som bekendt, at hvert polynomium af grad ≥ 1 har en rod. I fremstillingen

$$p(X) = \tilde{p}(X)\,(X-a_1)\cdots(X-a_k),$$

hvor $\tilde{p}$ ikke har rødder, af et polynomium $p \neq 0$ i $\mathbb{C}[X]$, må $\tilde{p}$ altså være en konstant. Er

$$p(X) = p_n X^n + \cdots + p_0, \quad p_n \neq 0$$

ser vi ved sammenligning af højstegradsleddene, at denne konstant er p_n, og at $k = n$. Fremstillingen er altså

$$p(X) = p_n\,(X-a_1)\cdots(X-a_n).$$

② Hvis p er et primtal, så er $\mathbb{Z}/p = \mathbb{F}_p$ et legeme med de p elementer $\textcircled{0}, \textcircled{1}, \ldots, \textcircled{p-1}$. Gruppen $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$ har orden $p-1$, så for hvert element $\lambda \in \mathbb{F}_p^*$ gælder $\lambda^{p-1} = \textcircled{1}$. (jfr. 5.17). Dette betyder imidlertid, at hvert af de $p-1$ elementer $\textcircled{1}, \textcircled{2}, \ldots, \textcircled{p-1}$ i $\mathbb{F}_p^*$ er rod i polynomiet

$$X^{p-1} - \textcircled{1} \in \mathbb{F}_p[X];$$

hvaf følger klart, at fremstillingen af dette er

$$X^{p-1} - ① = (X-①)(X-②)\cdots(X-(p-1)).$$

Sammenlignes koefficienterne på begge sider får vi en række ligninger. F.eks. finder vi for konstantleddet

$$-① = (-1)^{p-1}①②\cdots(p-1) = (-1)^{p-1}(p-1)!,$$

der for et ulige primtal p viser, at $(p-1)!+1$ er delelig med p (Wilsons sætning).

7.19. Bemærkning. I beviset for at afbildningen $p \mapsto p(a)$ er en ringhomomorfi : $R[X] \to A$ er det essentielt, at elementet a kommuterer med elementerne $\varphi(r)$, $r \in R$. Det benyttes altså afgørende, at $\varphi : R \to A$ er en central homomorfi.

Lad os mere generelt betragte en vilkårlig ringhomomorfi $\varphi : \Gamma \to \Lambda$ og et element $\lambda \in \Lambda$. I denne situation kan vi stadig indsætte λ i et polynomium

$$p = p_0 + p_1 X + \cdots + p_m X^m \in \Gamma[X],$$

og vi får herved elementet

$$p(\lambda) = \varphi(p_0) + \varphi(p_1)\lambda + \cdots + \varphi(p_m)\lambda^m \in \Lambda.$$

Det ses let, at den ved $p \mapsto p(\lambda)$ definerede afbildning : $\Gamma[X] \to \Lambda$ er additiv. Er altså

$$q = q_0 + q_1 X + \cdots + q_m X^m \in \Gamma[X]$$

endnu et polynomium, gælder

$$(p+q)(\lambda) = p(\lambda) + q(\lambda).$$

Afbildningen er derimod generelt ikke mul-

tiplikativ.

Eksempel. I kvaternionskrevlegemet $\mathbb{H}$ med "kvaternionenhederne" i, j og k betragtes polynomierne

$$p = X - i, \quad q \in X + i \quad \in \mathbb{H}[X].$$

Vi finder $pq = X^2 + 1$. Ved indsættelse af j finder vi

$$(pq)(j) = j^2 + 1 = 0$$

$$p(j)q(j) = (j-i)(j+i) \neq 0.$$

I den generelle situation gælder imidlertid

$$(pq)(\lambda) = p(\lambda)q(\lambda),$$

hvis λ kommuterer med elementerne $\varphi(q_0), \ldots, \varphi(q_m)$ (eller, som vi kort siger, hvis λ kommuterer med koefficienterne i polynomiet q). Dette verificeres ved udregning.

7.20. Lad os som anvendelse af resultatet i 7.19. vise Hamilton - Cayley's sætning.

Lad $\alpha \in \mathrm{Mat}_n(R)$ være en matrix med koefficienter i den kommutative ring R. Matrixringen $\mathrm{Mat}_n(R)$ kan opfattes som delring af matrixringen $\mathrm{Mat}_n(R[X])$. I ringen $\mathrm{Mat}_n(R[X])$ kan vi betragte matricen

$$\underline{\underline{X}} = \begin{pmatrix} X & & 0 \\ & \ddots & \\ 0 & & X \end{pmatrix}.$$

Det karakteristiske polynomium $p_\alpha(X)$ for α defineres nu som polynomiet

$$p_\alpha(X) = \det(\alpha - \underline{\underline{X}}) \in R[X].$$

Vi har

$$p_\alpha(X) = p_0 + \cdots + p_{n-1}X^{n-1} + p_n X^n, \quad \text{hvor}$$

$$p_0 = \det(\alpha), \quad p_{n-1} = (-1)^{n-1}\mathrm{Tr}(\alpha), \quad p_n = (-1)^n.$$

Er $A \in Mat_n(R[X])$ kofaktormatricen for $\alpha - \underline{\underline{X}}$, har vi

$$A(\alpha - \underline{\underline{X}}) = \det(\alpha - \underline{\underline{X}})\, 1_n$$

(jfr. 4.11.). Denne ligning i $Mat_n(R[X])$ kan skrives

$$A(\alpha - \underline{\underline{X}}) = p_0 + p_1 \underline{\underline{X}} + \cdots + p_{n-1} \underline{\underline{X}}^{n-1} + p_n \underline{\underline{X}}^n.$$

Nu er det let at se, at matrixringen $Mat_n(R[X])$ kan identificeres med polynomiumsringen $Mat_n(R)[X]$. Ved denne identifikation svarer matricen A til et polynomium $A(X)$ (hvis koefficienter er matricer), $\alpha - \underline{\underline{X}}$ svarer til polynomiet $\alpha - X$ og $\det(\alpha - \underline{\underline{X}})\, 1_n$ svarer til polynomiet $p_0 + p_1 X + \cdots + p_{n-1} X^{n-1} + p_n X^n$. I polynomiumsringen $Mat_n(R)[X]$ får vi derfor ligningen

$$A(X)(\alpha - X) = p_0 + \cdots + p_{n-1} X^{n-1} + p_n X^n.$$

Vi ønsker at indsætte α i dette polynomium. Dette kan gøres ved at indsætte α i hver af faktorerne og dernæst udregne produktet, thi herfor kræves, (jfr. 7.19) at α kommuterer med koefficienterne i polynomiet $\alpha - X$, og da disse koefficienter er α og -1, er denne betingelse opfyldt. Vi får derfor

$$p_0 + \cdots + p_{n-1} \alpha^{n-1} + p_n \alpha^n = A(\alpha)(\alpha - \alpha) = 0,$$

og ser, at <u>matricen $\alpha \in Mat_n(R)$ er rod i sit karakteristiske polynomium $p_\alpha(X) \in R[X]$.</u>

IDEALER I KOMMUTATIVE RINGE

I det følgende betegner R en kommutativ ring.

1. Ideal og kvotient.

1.1. Vi minder om, at et <u>ideal</u> i R er en ikke-tom delmængde $\mathfrak{a} \subseteq R$, for hvilken der gælder

id 1) $a_1, a_2 \in \mathfrak{a} \Rightarrow a_1 + a_2 \in \mathfrak{a} \wedge -a_1 \in \mathfrak{a}$

id 2) $r \in R \wedge a \in \mathfrak{a} \Rightarrow ra \in \mathfrak{a}$.

Betingelsen id 1) udsiger, at $\mathfrak{a}$ er en undergruppe i ringens additive gruppe R^+. At $a \in \mathfrak{a} \Rightarrow -a \in \mathfrak{a}$ følger i øvrigt af id 2), idet $-a = (-1)a$. De <u>trivielle</u> idealer i R er idealet $\{0\}$, der også betegnes (0), og idealet R.

1.2. Som bekendt er der en bijektiv forbindelse mellem idealer i R og kongruensrelationer i ringen R. Den til et ideal $\mathfrak{a}$ svarende kongruensrelation $\equiv$ er defineret ved

$$x \equiv y \quad \Leftrightarrow \quad y - x \in \mathfrak{a}.$$

Den kaldes "<u>kongruens modulo $\mathfrak{a}$</u>". Den tilhørende kvotient kan organiseres som en ring, kaldet <u>kvotientringen</u>, og betegnet $R/\mathfrak{a}$. Den kanoniske afbildning $x \mapsto \textcircled{x}$ er en surjektiv ringhomomorfi:

$$R \longrightarrow R/\mathfrak{a}.$$

1.3. Som bekendt gælder den såkaldte UDVIDELSESSÆTNING. <u>En ringhomomorfi $\varphi : R \to R'$, der forsvinder på idealet $\mathfrak{a} \subseteq R$, kan entydigt udvides</u>

til en ringhomomorfi fra kvotienten $\tilde{\varphi}: R/\mathfrak{a} \to R'$.

Homomorfien $\tilde{\varphi}: R/\mathfrak{a} \to R'$ siges at være induceret af φ.

1.4. Kernen for en ringhomomorfi $\varphi: R \to R'$, altså originalmængden $\varphi^{-1}(0)$, er et ideal i R, og billedet, altså $\varphi(R)$, er en delring af R'. Homomorfien φ forsvinder ógensynlig på sin kerne, og der gælder den såkaldte ISOMORFISÆTNING. En ringhomomorfi $\varphi: R \to R'$ inducerer en isomorfi

$$\tilde{\varphi}: R/\varphi^{-1}(0) \xrightarrow{\sim} \varphi(R)$$

af kvotienten på billedet.

1.5. Endelig gælder

NOETHERS ISOMORFISÆTNING. Lad $\varphi: R \to R'$ være en surjektiv ringhomomorfi med kernen $\mathfrak{a}_0$. Ved

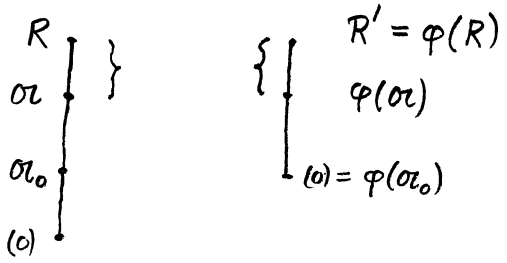
$$\mathfrak{a}' \longmapsto \varphi^{-1}(\mathfrak{a}') \quad \text{og} \quad \mathfrak{a} \longmapsto \varphi(\mathfrak{a})$$

etableres da en bijektiv, ordenstro forbindelse

$$\{\text{idealer } \mathfrak{a}' \text{ i } R'\} \leftrightarrows \{\text{idealer } \mathfrak{a} \text{ i } R, \text{ så at } \mathfrak{a} \supseteq \mathfrak{a}_0\}.$$

Er $\mathfrak{a} \supseteq \mathfrak{a}_0$ et ideal i R, findes en naturlig isomorfi

$$R/\mathfrak{a} \xrightarrow{\sim} R'/\varphi(\mathfrak{a}).$$



1.6. Betragter vi den kanoniske surjektive ringhomomorfi $O: R \to R/\mathfrak{a}_0$, og et ideal $\mathfrak{a} \supseteq \mathfrak{a}_0$, bruges

betegnelsen $\mathfrak{a}/\mathfrak{a}_0$ for (billed-) idealet $\overline{\mathfrak{a}} \subseteq R/\mathfrak{a}_0$. Isomorfien er da en isomorfi

$$R/\mathfrak{a} \xrightarrow{\sim} (R/\mathfrak{a}_0)/(\mathfrak{a}/\mathfrak{a}_0).$$

2. Ideal frembragt af en delmængde

2.1. Er der i R givet en delmængde M, betegner vi med RM (eller MR) delmængden af R bestående af elementer, der kan skrives som endelige summer af elementer af formen rx, $r \in R$, $x \in M$, altså

$$RM = \{ r_1 x_1 + \cdots + r_p x_p \mid r_1, \ldots, r_p \in R, x_1, \ldots, x_p \in M \}.$$

Det er let at se, at RM er et ideal i R. Idealet RM er endda det mindste ideal, som indeholder delmængden M, thi et ideal, som indeholder M, må indeholde alle elementer af formen rx, $r \in R$, $x \in M$ (id 2) og dermed alle summer af sådanne elementer (id 1).

DEFINITION. Idealet RM kaldes idealet <u>frembragt</u> af delmængden M.

2.2. For en endelig delmængde $M = \{a_1, \ldots, a_m\} \subseteq R$ ser vi let, at der gælder

$$R\{a_1, \ldots, a_m\} = \{ r_1 a_1 + \cdots + r_m a_m \mid r_1, \ldots, r_m \in R \}.$$

For idealet $R\{a_1, \ldots, a_m\}$ bruges betegnelsen $Ra_1 + \cdots + Ra_m$ (eller $a_1 R + \cdots + a_m R$). Ofte anvender også betegnelsen $(a_1, \ldots, a_m)$. Indeholder $M = \{a\}$ kun ét element, får vi betegnelserne Ra (eller aR) eller (a) for idealet $R\{a\}$.

DEFINITION. Idealer i R, der er frembragt af en endelig delmængde, kaldes <u>endeligt frembragte</u> idealer. Idealer i R, der er frembragt af et enkelt element, kaldes <u>hovedidealer</u>.

De endeligt frembragte idealer er altså idealer af formen $Ra_1 + \cdots + Ra_m$. Hovedidealerne er idealerne

af formen Ra.

Elementer af formen ra kaldes <u>multipla</u> af a. Hovedidealet Ra består altså af samtlige multipla af a.

Vi har $R1 = R$, og ser let, at der for et element $u \in R$ gælder

$$Ru = R \Leftrightarrow u \text{ er invertibel.}$$

2.3. Eksempler. ① I gruppen $\mathbb{Z}^+$ gælder som bekendt, at samtlige undergrupper har formen $\mathbb{Z}a$ (hvor $a \geq 0$ er entydigt bestemt). Undergrupperne er altså idealer i ringen $\mathbb{Z}$, endda hovedidealer. Alle idealer i ringen $\mathbb{Z}$ er altså hovedidealer.

② Lad $t_0 \in [0,1]$, og betragt i ringen $C^0[0,1]$ af kontinuerte funktioner på $[0,1]$ delmængden $\mathfrak{o}_{t_0}$ bestående af funktioner $f \in C^0[0,1]$, for hvilke

$$f = 0 \text{ i en omegn (afhængig af } f) \text{ af } t_0.$$

Det er let at se, at $\mathfrak{o}_{t_0}$ er et ideal i $C^0[0,1]$. Også delmængden $\mathfrak{m}_{t_0}$ bestående af funktioner $f \in C^0[0,1]$, for hvilke

$$f(t_0) = 0$$

er et ideal i $C^0[0,1]$ (Det er kernen for homomorfien $C^0[0,1] \to \mathbb{R}$ givet ved $f \mapsto f(t_0)$)

Det er let at se, at idealet $\mathfrak{o}_{t_0}$ ikke er endeligt frembragt. Heller ikke idealet $\mathfrak{m}_{t_0}$ er endeligt frembragt. □

③ I en polynomiumsring $R = K[X,Y]$ består idealet $RX + RY = (X,Y)$ af de polynomier $p \in R$, for hvilke $p(0,0) = 0$. Dette ideal er endeligt frembragt, men det er ikke et hovedideal □

④ Delmængden $R \subseteq \mathbb{Q}[X]$ bestående af polynomier

$$p = r_0 + p_1 X + \cdots + p_n X^n \in \mathbb{Q}[X] \quad \text{med } r_0 \in \mathbb{Z}$$

er en delring. I denne ring R er delmængden $\mathfrak{a}$ bestående af polynomier p, for hvilke $p(0) = r_0 = 0$, et ideal, der ikke er endeligt frembragt. [Er nemlig $p_1, \cdots, p_k \in \mathfrak{a}$,

$$p_i = \frac{a_i}{n_i} X + \cdots \quad , \quad a_i \in \mathbb{Z}, n_i \in \mathbb{N},$$

vil idealet $Rp_1 + \cdots + Rp_k \subseteq \mathfrak{a}$ ikke indeholde elementet $\frac{1}{(n_1 \cdots n_k)^2} X$ □]

2.4. Kvadratiske talringe. Vi betragter et irrationalt tal $\xi \in \mathbb{C}$, der er rod i et 2den grads polynomium $X^2 - AX - B$, hvor $A, B \in \mathbb{Z}$.

[Eks. $\xi = i$ er rod i X^2+1, $\xi = \sqrt{5}$ er rod i X^2-5, $\xi = \sqrt{-5}\,(= i\sqrt{5})$ er rod i X^2+5, $\xi = \frac{-1}{2} + i\frac{\sqrt{3}}{2}$ er rod i X^2+X+1].

Delringen $R = \mathbb{Z}[\xi] \subseteq \mathbb{C}$ består da af alle elementer af formen

$$r = r_1 + r_2 \xi \quad , \quad \text{hvor } r_1, r_2 \in \mathbb{Z}.$$

Under brug af at $\xi^2 = A\xi + B$ vises nemlig let, at elementer af denne form udgør en ring.

Da $\xi \notin \mathbb{Q}$, ser vi let, at i fremstillingen $r = r_1 + r_2 \xi$ af et element $r \in R$ er $r_1, r_2 \in \mathbb{Z}$ entydigt bestemte.

Er ξ' den anden rod i $X^2 - AX - B$, så er $\xi\xi' = -B$ og $\xi + \xi' = A$. Specielt er altså også $\xi' = A - \xi \in R$.

Det er ikke svært at vise, at den ved

$$r = r_1 + r_2 \xi \longmapsto r' = r_1 + r_2 \xi'$$

definerer en ringhomomorfi: $R \to R$ $\square$. Vi har $(r')' = r$, og $r' = r \Leftrightarrow r \in \mathbb{Z}$.

For et element $r = r_1 + r_2\xi \in R$ sætter vi

$$N(r) = rr' = (r_1 + r_2\xi)(r_1 + r_2\xi') = r_1^2 - Br_2^2 + Ar_1r_2.$$

[$N(r)$ kaldes "normen" af r]

Vi har da

$$N(r) \in \mathbb{Z}, \quad N(0) = 0, \quad N(r) \neq 0 \text{ hvis } r \neq 0$$
$$N(ra) = N(r)N(a).$$

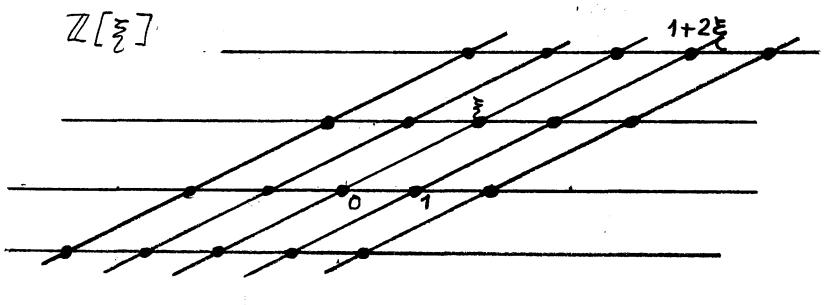
Normen er altså en multiplikativ homomorfi: $R \to \mathbb{Z}$.

Et element $x = x_1 + x_2\xi \in R$ er invertibelt, hvis og kun hvis $N(x) = \pm 1$.

Er nemlig $xy = 1$, så er $N(x)N(y) = N(xy) = N(1) = 1$ i $\mathbb{Z}$, og det følger, at $N(x) = \pm 1$, og er omvendt $N(x) = \pm 1$, altså $xx' = \pm 1$, så er $\pm x'$ invers i R til x.

Af den multiplikative egenskab kan vi f.eks. udlede, at hvis $b \in Ra$, så gælder i $\mathbb{Z}$, at $N(a)$ er divisor i $N(b)$.

Vi bemærker endelig, at hvis $\xi \notin \mathbb{R}$, så er $\xi' = \overline{\xi}$ og $r' = \overline{r}$ (kompleks konjugering) for alle $r \in R$. I dette tilfælde er altså $N(r) = r\overline{r} = |r|^2$ kvadratet på den sædvanlige absolutværdi. Ydertigere er $1, \xi \in \mathbb{C}$ lineært uafhængige over $\mathbb{R}$, så elementerne i $\mathbb{Z}[\xi]$ kan anskueliggøres som gitterpunkter i et Wesseldiagram:



2.5. Eksempel. I ringen $R = \mathbb{Z}[\sqrt{-5}]$ har vi

$$N(x_1 + x_2\sqrt{-5}) = x_1^2 + 5x_2^2 \geqslant 0.$$

De invertible elementer i R svarer til løsninger $(x_1, x_2) \in \mathbb{Z} \times \mathbb{Z}$ til ligningen

$$x_1^2 + 5x_2^2 = 1.$$

Vi ser, at 1 og -1 er de eneste invertible elementer i $\mathbb{Z}[\sqrt{-5}]$ (svarende til løsningerne $(1,0)$ og $(-1,0)$). Ingen elementer $x \in R$ opfylder $N(x) = 3$. Samtlige elementer i $x \in R$, som opfylder $N(x) = 9$ er ± 3, $\pm(2+\sqrt{-5})$, $\pm(2-\sqrt{-5})$. Lad os vise, at idealet

$$R3 + R(2+\sqrt{-5})$$

ikke er et hovedideal. Vi bemærker først, at der for hvert $x \in R3 + R(2+\sqrt{-5})$ gælder $N(x) \equiv 0 \bmod 3$. Sættes nemlig $a = 2+\sqrt{-5}$ finder vi $N(r3 + sa) = (r3 + sa)(\bar{r}3 + \bar{s}\bar{a}) = 9N(r) + 9N(s) + 3(r\bar{s}\bar{a} + \bar{r}sa) \equiv 0 \bmod 3$, idet $r\bar{s}\bar{a} + \bar{r}sa$ er 2·realdelen af et element i $\mathbb{Z}[\sqrt{-5}]$, og dermed $\in \mathbb{Z}$ (endda $\in 2\mathbb{Z}$). Var nu $R3 + R(2+\sqrt{-5})$ et hovedideal:

$$R3 + R(2+\sqrt{-5}) = Rd,$$

måtte $3 = ud$, $2+\sqrt{-5} = vd$ med $u, v \in R$, og følgelig

$$9 = N(3) = N(u)N(d) \qquad 9 = N(2+\sqrt{-5}) = N(v)N(d).$$

Specielt ville $N(d)$ være divisor i 9, altså $N(d) = 1, 3$ eller 9. Her er $N(d) = 1$ udelukket ifølge bemærkningen, $N(d) = 3$ kan ikke gælde for nogit $d \in R$, og var $N(d) = 9$, måtte $N(u) = N(v) = 1$; u og v ville altså være invertible, og vi ville have $uv^{-1} = \pm 1$. Men

$$3 = ud = uv^{-1}(2+\sqrt{-5}) = \pm(2+\sqrt{-5})$$

er også udelukket.

3. Noetherske ringe og hovedidealringe.

3.1. DEFINITION. Ringen R kaldes *noetherske*, hvis alle dens idealer er endeligt frembragte.

3.2. Eksempler. Ringen $\mathbb{Z}$ er noetherske, idet alle dens idealer er frembragt af ét element. Et hvert legeme er en noetherske ring. Ringene i eksemplerne 2.3.② og 2.3.④ er ikke noetherske.

3.3. SÆTNING. *For en ring R er følgende betingelser ækvivalente:*

(i) *Ethvert ideal i R er endeligt frembragt* (d: R er noetherske)

(ii) *I enhver opstigende kæde*
$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots$$
af idealer i R gælder "=" fra et vist trin (den opstigende kædes egenskab)

(iii) *I enhver ikke-tom mængde $\mathcal{S}$ af idealer i R findes maksimale elementer (m.h.t. $\subseteq$)*, d.v.s. der findes et ideal $\mathfrak{a}_0 \in \mathcal{S}$ med egenskaben:
$$\mathfrak{a} \in \mathcal{S} \wedge \mathfrak{a}_0 \subseteq \mathfrak{a} \Rightarrow \mathfrak{a}_0 = \mathfrak{a}.$$
(maksimalitetsegenskaben).

Bevis. *(i) ⇒ (ii)*: Er der givet en stigende følge
$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots$$
af idealer, vises det let, at foreningsmængden
$$\mathfrak{a} = \bigcup_{i=1}^{\infty} \mathfrak{a}_i$$
er et ideal, og dermed af formen
$$\mathfrak{a} = Ra_1 + \cdots + Ra_m.$$
Hver af frembringerne $a_1, \ldots, a_m$ tilhører foreningsmængden,

og dermed et af $\mathfrak{a}_i$'erne. Da der kun er endelig mange frembringere, slutter vi, at der findes et N (= "det største i"), så at alle frembringerne tilhører $\mathfrak{a}_N$. Men så har vi

$$\mathfrak{a} = Rx_1 + \cdots + Rx_m \subseteq \mathfrak{a}_N \subseteq \mathfrak{a}_{N+1} \subseteq \cdots \subseteq \bigcup_i \mathfrak{a}_i = \mathfrak{a},$$

og altså $\mathfrak{a}_N = \mathfrak{a}_{N+1} = \cdots$.

(ii) ⇒ (i): Indirekte. Er $\mathfrak{a}$ et ikke-endeligt frembragt ideal i R, kan vi vælge $a_1 \in \mathfrak{a}$, og få $Ra_1 \subseteq \mathfrak{a}$. Her må endda gælde $Ra_1 \subset \mathfrak{a}$, så vi kan vælge $a_2 \in \mathfrak{a} \setminus Ra_1$, og få $Ra_1 + Ra_2 \subseteq \mathfrak{a}$. Her må endda gælde $Ra_1 + Ra_2 \subset \mathfrak{a}$, så vi kan vælge $a_3 \in \mathfrak{a} \setminus (Ra_1 + Ra_2)$ og få $Ra_1 + Ra_2 + Ra_3 \subseteq \mathfrak{a}$. Idet vi fortsætter således, får vi en kæde

$$Ra_1 \subset Ra_1 + Ra_2 \subset Ra_1 + Ra_2 + Ra_3 \subset \cdots$$

i modstrid med (ii).

(ii) ⇒ (iii): Indirekte. Er $\mathcal{S}$ en ikke-tom mængde af idealer, der ikke har noget maksimalt element, kan vi – da $\mathcal{S} \neq \emptyset$ – vælge $\mathfrak{a}_1 \in \mathcal{S}$. Da $\mathfrak{a}_1$ ikke er maksimalt element i $\mathcal{S}$, findes $\mathfrak{a}_2 \in \mathcal{S}$, så at $\mathfrak{a}_1 \subset \mathfrak{a}_2$. Da $\mathfrak{a}_2$ ikke er maksimalt element i $\mathcal{S}$, findes $\mathfrak{a}_3 \in \mathcal{S}$, så at $\mathfrak{a}_2 \subset \mathfrak{a}_3$. Fortsættes således, fås en kæde af idealer

$$\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \mathfrak{a}_3 \subset \cdots,$$

i modstrid med (ii).

(iii') ⇒ (ii). Er der givet en opstigende kæde af idealer

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots,$$

findes i mængden $\mathcal{S} = \{\mathfrak{a}_1, \mathfrak{a}_2, \ldots\}$ et maksimalt element $\mathfrak{a}_N$. Vi har $\mathfrak{a}_N \subseteq \mathfrak{a}_{N+1} \subseteq \cdots$, og maksimaliteten sikrer, at $\mathfrak{a}_N = \mathfrak{a}_{N+1} = \cdots$.

▨

3.4. SÆTNING. *Enhver kvotient $R/\mathfrak{a}_0$ af en noethersk ring R, er igen noethersk.*

Bevis. Ifølge Noethers isomorfisætning er ethvert ideal i kvotienten $\bar{R} = R/\mathfrak{a}_0$ af formen

$$\bar{\mathfrak{a}} = \{\bar{a} \mid a \in \mathfrak{a}\},$$

hvor $\mathfrak{a}$ er et ideal i R. Er $\mathfrak{a}$ endeligt frembragt:

$$\mathfrak{a} = Ra_1 + \cdots + Ra_m,$$

finder vi let

$$\bar{\mathfrak{a}} = \bar{R}\bar{a}_1 + \cdots + \bar{R}\bar{a}_m. \quad \square$$

3.5. HILBERTS BASISSÆTNING. *Hvis R er en noethersk ring, så er enhver polynomiumsring $R[X_1, \cdots, X_n]$ ligeledes noethersk.*

Bevis. Idet $R[X_1, \cdots, X_n] = R[X_1, \cdots, X_{n-1}][X_n]$, ser vi - ved induktion - at det er nok at vise påstanden for $n = 1$. Vi skal altså for en noethersk ring R vise, at polynomiumsringen $R[X]$ er noethersk.

Er $\mathfrak{a}$ et ideal i $R[X]$, kan vi for $n = 0, 1, 2, \cdots$ betragte mængden af de elementer $a \in R$, for hvilke der *i* $\mathfrak{a}$ findes et polynomium af formen

$$aX^n + a_1X^{n-1} + \cdots + a_n,$$

altså

$$\mathfrak{a}^{(n)} = \{a \in R \mid \exists a_1, \cdots, a_n \in R : aX^n + a_1X^{n-1} + \cdots + a_n \in \mathfrak{a}\}.$$

Det er let at se, at $\mathfrak{a}^{(n)}$ er et ideal i R, at $\mathfrak{a}^{(0)} \subseteq \mathfrak{a}^{(1)} \subseteq \mathfrak{a}^{(2)} \subseteq \cdots$, og at der for et ideal $\mathfrak{B} \subseteq \mathfrak{a}$ gælder $\mathfrak{B}^{(n)} \subseteq \mathfrak{a}^{(n)}$, $n = 0, 1, 2, \cdots$.

Vi indskyder nu et

LEMMA. *Er $\mathfrak{B} \subseteq \mathfrak{a}$ idealer i $R[X]$, således at $\mathfrak{B}^{(n)} = \mathfrak{a}^{(n)}$, $n = 0, 1, \cdots$, så er $\mathfrak{B} = \mathfrak{a}$.*

Bevis for lemma. Var $\mathfrak{B} \subset \mathfrak{a}$ kunne vi i $\mathfrak{a} \setminus \mathfrak{B}$

finde et polynomium af lavest mulig grad n:

$$p = aX^n + a_1X^{n-1} + \cdots + a_n.$$

Her er $a \in A^{(n)}$, altså også $a \in B^{(n)}$, så der i B et polynomium q af formen

$$q = aX^n + b_1X^{n-1} + \cdots + b_n.$$

Nu er $q \in B \subseteq A$, og altså også $p-q \in A$, og yderligere er $p-q \notin B$, idet vi ellers ville have $p = (p-q)+q \in B$. Vi har altså

$$p-q \in A \setminus B,$$

men da dette polynomium har lavere grad end p, er dette en modstrid ▨

Idet vi vender tilbage til beviset for basissætningen, betragter vi en opstigende kæde af idealer i $R[X]$:

$$A_1 \subseteq A_2 \subseteq \cdots$$

Heraf får vi idealer i R:

$$\begin{array}{ccccc}
A_1^{(0)} & \subseteq & A_2^{(0)} & \subseteq & A_3^{(0)} \subseteq \cdots \\
\cap| & & \cap| & & \cap| \\
A_1^{(1)} & \subseteq & A_2^{(1)} & \subseteq & A_3^{(1)} \subseteq \cdots \\
\cap| & & \cap| & & \cap| \\
A_1^{(2)} & \subseteq & A_2^{(2)} & \subseteq & A_3^{(2)} \subseteq \cdots \\
\cap| & & \cap| & & \cap| \\
\vdots & & \vdots & & \vdots
\end{array}$$

Vi ser, at "diagonalfølgen" er en opstigende kæde

$$A_1^{(0)} \subseteq A_2^{(1)} \subseteq \cdots,$$

og slutter, at der gælder "=" fra et vist trin N:

$$A_{N+1}^{(N)} = A_{N+2}^{(N+1)} = \cdots$$

Vi har nu inklusionerne

$$\begin{array}{ccccc}
A_{N+1}^{(N)} & \subseteq & A_{N+2}^{(N)} & \subseteq & \cdots \\
\cap| & \diagdown & \cap| & & \\
A_{N+1}^{(N+1)} & \subseteq & A_{N+2}^{(N+1)} & \subseteq & \cdots \\
\cap| & & \cap| & \diagdown & \\
\vdots & & \vdots & & \ddots
\end{array}$$

og ser, at der her overalt må gælde "=". For hvert $n \geqslant N$ har vi altså

$$a_{N+1}^{(n)} = a_{N+2}^{(n)} = \cdots \qquad n \geqslant N$$

Vi betragter nu de endelig mange følger

$$a_1^{(n)} \subseteq a_2^{(n)} \subseteq \cdots , \qquad n = 0, \cdots, N-1.$$

I hver af disse følger gælder "=" fra et vist trin, og da der her kun er endelig mange følger, gælder endda fra et vist trin "=" i dem alle. Der findes altså et M, således at

$$a_M^{(n)} = a_{M+1}^{(n)} = \cdots \qquad n = 0, \cdots, N-1.$$

Vi kan antage, at $M > N$, og har så

$$a_M^{(n)} = a_{M+1}^{(n)} = \cdots \qquad n = 0,1,2, \cdots .$$

Af lemmaet følger nu, at

$$a_M = a_{M+1} = \cdots \quad \blacksquare$$

3.6. Eksempler. Ringene $\mathbb{Z}[X_1, \cdots, X_n]$ (specielt $\mathbb{Z}[X]$) er noetherske ringe.

Ringene $L[X_1, \cdots, X_n]$, hvor L er et legeme, er noetherske ringe.

3.7. Eksempel. En kvadratisk talring $\mathbb{Z}[\xi]$ er en noetherisk ring, nemlig (isomorf med) en kvotient af $\mathbb{Z}[X]$.

3.8. Eksempel. En delring af en noetherisk ring behøver ikke at være noetherisk. F.eks. var den ikke-noetherske ring R fra eksempel 2.3.④ en delring af $\mathbb{Q}[X]$.

3.9. DEFINITION. Ringen R kaldes en <u>hovedidealring</u>, hvis alle dens idealer er hovedidealer. Er R desuden et integritetsområde, kaldes R et <u>hovedidealområde</u>.

3.10. Ringen $\mathbb{Z}$ er et hovedideal område. Videre gælder følgende vigtige

SÆTNING. <u>Polynomiumsringen $L[X]$, hvor L er et legeme, er et hovedidealområde</u>.

Bevis. Lad $\mathfrak{a} \subseteq L[X]$ være et ideal. $\neq (0)$. Blandt polynomierne $\neq 0$ i $\mathfrak{a}$ kan vi vælge et, d, af lavest mulig grad. Da er $\mathfrak{a} = (d)$, thi $\mathfrak{a} \supseteq (d)$ er klart, og er omvendt $a \in \mathfrak{a}$, kan vi bestemme et polynomium q således at

$$\deg(a - qd) < \deg d$$

("division med rest"). Nu er $qd \in (d) \subseteq \mathfrak{a}$, og altså også $a - qd \in \mathfrak{a}$. Da dette polynomium i $\mathfrak{a}$ har lavere grad end d, må det være nul-polynomiet. Vi har altså $a = qd \in (d)$. ▨

3.11. Vi ser let, at det essentielle i ovenstående bevis er følgende: <u>Er der i ringen R givet en funktion $v: R \to \mathbb{Z}$, der er nedad begrænset, og således at der for alle $a, d \in R$, $d \neq 0$ findes et $q \in R$, så at</u>

$$\underline{v(a - qd) < v(d)},$$

<u>så er R en hovedidealring.</u>

Således har vi i beviset for sætning 3.10 betragtet funktionen $v: L[X] \to \mathbb{Z}$ defineret ved $v(p) = \deg(p)$.

Tilsvarende ser vi, at $\mathbb{Z}$ er en hovedidealring ved at betragte funktionen $v: \mathbb{Z} \to \mathbb{Z}$ defineret ved $v(p) = |p|$.

3.12. Gauß' talring er den kvadratiske talring $\mathbb{Z}[i] \subseteq \mathbb{C}$.

Gauß' talring er et hovedidealområde. Vi viser, at funktionen $v: R = \mathbb{Z}[i] \to \mathbb{Z}$ defineret ved

$$v(r) = N(r) = |r|^2,$$

har egenskaberne nævnt i 3.11. Er altså $a, d \in R$, $d \neq 0$, skal vi vise, at der findes $q \in R$, så at $v(a - qd) < v(d)$, eller ensbetydende hermed:

$$\left| \frac{a}{d} - q \right| < 1.$$

Vi kan fortolke elementerne i R som gitterpunkter i $\mathbb{C}$ ($\mathbb{Z}[i] = \{ r_1 + r_2 i \mid r_1, r_2 \in \mathbb{Z} \}$), og ser, at der for hvert $\alpha \in \mathbb{C}$ (og specielt for $\alpha = \frac{a}{d}$), findes et $q \in R$, så at vi endda har

$$|\alpha - q| \leq \frac{1}{\sqrt{2}} \quad \blacksquare$$

Tilsvarende vises, at den kvadratiske talring $\mathbb{Z}[\rho]$, hvor $\rho = \frac{-1}{2} + i\frac{\sqrt{3}}{2}$ er rod i $X^2 + X + 1$, er et hovedidealområde.

3.13. En hovedidealring er specielt en noethersk ring. Vi får derfor følgende

SÆTNING. For idealerne i en hovedidealring gælder den opstigende kædes egenskab og maksimalitetsegenskaben, jfr. 3.3.

4. Maksimalideal og primideal.

4.1. SÆTNING. Ringen R er et legeme, hvis og kun hvis den indeholder netop to idealer (som så må være de trivielle: $(0) \subset (1)$).
Bevis. Et element $r \in R$ er invertibelt, hvis og kun hvis $Rr = R$. Heraf følger påstanden let □

4.2. DEFINITION. Et ideal $\mathfrak{M}$ i ringen R kaldes et maksimalideal, hvis det er maksimalt blandt idealerne $\subset R$. Dette betyder altså, at $\mathfrak{M} \subset R$, og at der for ideal $\mathfrak{a}$ i R gælder

$$\mathfrak{M} \subseteq \mathfrak{a} \subset R \Rightarrow \mathfrak{M} = \mathfrak{a}.$$

4.3. Betingelsen kan også udtrykkes ved at der af ideal $\mathfrak{a}$ i R, som opfylder

$$\mathfrak{M} \subseteq \mathfrak{a} \subseteq R$$

findes netop to (som så må være $\mathfrak{a} = \mathfrak{M}$ og $\mathfrak{a} = R$).
Ifølge Noethers isomorfisætning svarer idealerne $\mathfrak{a}$ i R, som opfylder $\mathfrak{M} \subseteq \mathfrak{a} \subseteq R$ netop til idealerne i kvotienten $R/\mathfrak{M}$. Kombinerer vi med sætning 4.1, får vi derfor følgende
SÆTNING. Idealet $\mathfrak{M}$ i R er et maksimalideal, hvis og kun hvis kvotienten $R/\mathfrak{M}$ er et legeme. ▨

4.4. Eksempel. I ringen $\mathbb{Z}$ er hovedidealet (p) frembragt af et primtal p et maksimalideal, thi vi har $(p) \subset \mathbb{Z}$, og er $(p) \subseteq (a) \subset \mathbb{Z}$, med $a \geqslant 0$, må vi have $a \geqslant 2$ og a er divisor i p. Følgelig er $p = a$ og dermed $(p) = (a)$.

kvotienten $\mathbb{Z}/p = \mathbb{F}_p$ er altså et legeme.

4.5. Eksempel. I ringen $R = C^0[0,1]$ er idealet

$$\mathfrak{m}_{t_0} = \{ f \in R \mid f(t_0) = 0 \},$$

(jfr. eksempel 2.3 ②) et maksimalvdeal, thi $\mathfrak{m}_{t_0}$ er kerne for den surjektive homomorfi : $R \to \mathbb{R}$, defineret ved $f \longmapsto f(t_0)$, således at $R/\mathfrak{m}_{t_0} \cong \mathbb{R}$ er et legeme.

4.6. Lad os vise, at i ringen $R = \mathbb{Z}[\sqrt{-5}]$ (jfr. eksempel 2.5) er idealet

$$R3 + R(2+\sqrt{-5})$$

et maksimalideal. Vi betragter afbildningen $R \to \mathbb{Z}/3$ defineret ved $r = r_1 + r_2\sqrt{-5} \longmapsto \hat{r} = \overline{r_1} + \overline{r_2} \in \mathbb{Z}/3$. Denne afbildning er en ringhomomorfi, thi den er klart additiv, og den er multiplikativ, idet vi for $s = s_1 + s_2\sqrt{-5}$ finder

$$\begin{aligned}
\widehat{rs} &= \overline{r_1 s_1 - 5 r_2 s_2 + (r_1 s_2 + r_2 s_1)\sqrt{-5}} \\
&= \overline{r_1 s_1 - 5 r_2 s_2} + \overline{r_1 s_2 + r_2 s_1} \\
&= \overline{r_1}\,\overline{s_1} + \overline{r_2}\,\overline{s_2} + \overline{r_1}\,\overline{s_2} + \overline{r_2}\,\overline{s_1} \\
&= (\overline{r_1} + \overline{r_2})(\overline{s_1} + \overline{s_2}) \\
&= \hat{r}\,\hat{s}.
\end{aligned}$$

Denne homomorfi : $R \to \mathbb{Z}/3$ er klart surjektiv, og da $\mathbb{Z}/3$ er et legeme, er dens kerne

$$\mathfrak{m} = \{ r_1 + r_2\sqrt{-5} \mid r_1 + r_2 \equiv 0 \pmod 3 \}$$

et maksimalideal i R. Nu er

$$R3 + R(2+\sqrt{-5}) = \mathfrak{m},$$

thi "$\subseteq$" er klart, da hver af de to frembringere åbenbart tilhører $\mathfrak{m}$, og er omvendt $r = r_1 + r_2\sqrt{-5} \in \mathfrak{m}$,

så er $r_1 + r_2 \equiv 0 \pmod 3$, altså $r_1 + r_2 = 3n$, og vi får

$$\begin{aligned} r = r_1 + r_2\sqrt{-5} &= r_1 + (3n - r_1)\sqrt{-5} \\ &= (r_1 + n\sqrt{-5})\,3 - r_1(2 + \sqrt{-5}) \\ &\in R3 + R(2+\sqrt{-5}). \end{aligned}$$

Tilsvarende ser vi, at idealet

$$\overline{w} = R3 + R(2-\sqrt{-5})$$

er et maksimalideal i R, kerne for homomorfien

$$r = r_1 + r_2\sqrt{-5} \longmapsto \overline{r_1} - \overline{r_2} \in \mathbb{Z}/3.$$

4.7 DEFINITION. Et ideal $\mathfrak{p}$ i ringen R kaldes et <u>primideal</u>, hvis $\mathfrak{p} \subset R$, og hvis den for alle $x, y \in R$ gælder

$$xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p} \vee y \in \mathfrak{p}.$$

4.8. For idealet (0) i R, er den sidste betingelse, at nulreglen gælder i R. At (0) er et primideal, udsiger altså at $(0) \subset R$ og at nulreglen gælder i R, altså alt i alt, at R er et integritetsområde.

Mere generelt får vi let følgende

SÆTNING. <u>Idealet $\mathfrak{p}$ i R er et primideal, hvis og kun hvis kvotienten $R/\mathfrak{p}$ er et integritetsområde.</u> □

4.9 Da et legeme specielt er et integritetsområde, følger det af de givne karakteriseringer, at vi har

SÆTNING. <u>Ethvert maksimalideal i ringen R er et primideal.</u> ▨

4.10 SÆTNING. *Kernen for en ringhomomorfi $\varphi: R \to R'$, hvor R' er et integritetsområde, er et primideal i R.*

Bevis. I følge isomorfisætningen har vi en isomorfi

$$R/\text{kernen} \xrightarrow{\sim} \text{billedet},$$

og her er billedet en delring af integritetsområdet R', og dermed selv et integritetsområde. ▨

4.11. Eksempler. Kernen for homomorfien $\mathbb{Z}[X] \to \mathbb{Z}$ givet ved

$$f = a_0 + a_1X + \cdots + a_mX^m \longmapsto f(0) = a_0$$

er hovedidealet $(X) \subseteq \mathbb{Z}[X]$. Det er et primideal. Kernen for homomorfien $\mathbb{Z}[X] \to \mathbb{Z}/p\,[X]$ defineret ved

$$f = a_0 + a_1X + \cdots + a_mX^m \longmapsto \overline{a_0} + \overline{a_1}X + \cdots + \overline{a_m}X^m$$

er hovedidealet $(p) \subseteq \mathbb{Z}[X]$. Hvis p er et primtal, bliver dette ideal et primideal, idet $\mathbb{Z}/p\,[X]$ da er et integritetsområde. I dette tilfælde bliver idealet $(X, p) \subseteq \mathbb{Z}[X]$ et maksimalideal. (kerne for homomorfien $f \longmapsto \overline{a_0} \in \mathbb{Z}/p = \mathbb{F}_p$.

4.12. Eksempel. Ringen $\mathbb{Z}$ er et integritetsområde, så $(0) \subset \mathbb{Z}$ er et primideal. Et primideal i $\mathbb{Z}$ har formen (p), hvor $p \geqslant 2$, og her må p være et primtal, thi var $p = xy$, $x > 1$, $y > 1$, ville vi have

$$xy \in (p),\quad x \notin (p),\quad y \notin (p).$$

Omvendt har vi set, at hvis p er et primtal, så er (p) et maksimalidealer. Primidealerne $\neq (0)$ i $\mathbb{Z}$ er altså maksimalidealer.

4.13. Eksempel. Som bekendt gælder, at en endelig (kommutativ) ✓

ring er et legeme, hvis og kun hvis den er et integritetsområde. Har idealet $\mathfrak{a} \subseteq R$ altså endeligt index, d.v.s. er $R/\mathfrak{a}$ endelig, så er $\mathfrak{a}$ et maksimalideal, hvis og kun hvis det er et primideal.

Som anvendelse heraf kan vi vise, at i en kvadratisk talring $R = \mathbb{Z}[\xi]$ er ethvert primideal $\neq (0)$ et maksimalideal. Det er nok at vise, at der for hvert ideal $\mathfrak{a} \neq (0)$ gælder, at $R/\mathfrak{a}$ er en endelig ring. Er $\mathfrak{a} = Rn$, hvor $n \in \mathbb{Z}$, $n \neq 0$, er dette klart, thi Rn består af elementer $r_1 + r_2\xi$, hvor $r_1, r_2 \in \mathbb{Z}n$, så elementerne $r_1 + r_2\xi$, hvor $0 \leqslant r_1 < |n|$, $0 \leqslant r_2 < |n|$ er et repræsentantsystem for R/Rn (og $|R/Rn| = n^2$). Det almindelige tilfælde reduceres hertil, thi der findes $a \neq 0$ i $\mathfrak{a}$, og så er $An = N(a) = a'a \in \mathfrak{a}$, og vi har $Rn \subseteq Ra \subseteq \mathfrak{a}$, så $|R/\mathfrak{a}|$ er endelig (endda divisor i $|R/nR| = N(a)^2$).

I $R = \mathbb{Z}[\sqrt{-5}]$ er $R11$ et maksimalideal (og $R/R11$ er et legeme med $11^2 = 121$ elementer). Det er nok at vise, at $R11$ er et primideal, altså at der af

$$(r_1 + r_2\sqrt{-5})(x_1 + x_2\sqrt{-5}) \in R11, \quad r_1 + r_2\sqrt{-5} \notin R11$$

følger $x_1 + x_2\sqrt{-5} \in R11$.

Nu består $R11$ af de elementer $z = z_1 + z_2\sqrt{-5} \in R$, hvor $z_1, z_2 \in \mathbb{Z} \cdot 11$, altså $\overline{z_1} = \overline{z_2} = 0 \in \mathbb{Z}/11$. Vi har $(r_1 + r_2\sqrt{-5})(x_1 + x_2\sqrt{-5}) = (r_1x_1 - 5r_2x_2) + (r_1x_2 + r_2x_1)\sqrt{-5}$, altså i $\mathbb{F}_{11} = \mathbb{Z}/11$

$$\overline{r_1}\,\overline{x_1} - 5\,\overline{r_2}\,\overline{x_2} = 0$$

$$\overline{r_2}\,\overline{x_1} + \overline{r_1}\,\overline{x_2} = 0.$$

For her at kunne slutte, at $\overline{x_1} = \overline{x_2} = 0$, må vi for determinanten have

$$\overline{r_1}^2 + 5\,\overline{r_2}^2 \neq 0.$$

At dette virkelig er opfyldt, når $\overline{r_1}$ og $\overline{r_2}$ ikke begge er 0 følger let (er $\overline{r_2} = 0$, har vi $\overline{r_1}^2 + \overline{5}\,\overline{r_2}^2 = \overline{r_1}^2 \neq 0$, og er $\overline{r_2} \neq 0$, er $\overline{r_1}^2 + \overline{5}\,\overline{r_2}^2 = \overline{r_2}^2\left([\overline{r_1}\,\overline{r_2}^{-1}]^2 + \overline{5}\right) \neq 0$, idet der for intet element $\lambda \in \mathbb{Z}/11$ kan gælde $\lambda^2 + \overline{5} = 0$.).

5. Idealoperationerne. Den kinesiske restklassesætning.

5.1. Er $\mathfrak{a}$ og $\mathfrak{b}$ idealer i ringen R, kan vi betragte fællesmængden

$$\mathfrak{a} \cap \mathfrak{b},$$

som øjensynlig igen er et ideal. Videre kan vi betragte summen

$$\mathfrak{a} + \mathfrak{b}$$

bestående af alle elementer i R af formen

$$a + b, \quad a \in \mathfrak{a}, \quad b \in \mathfrak{b},$$

og produktet

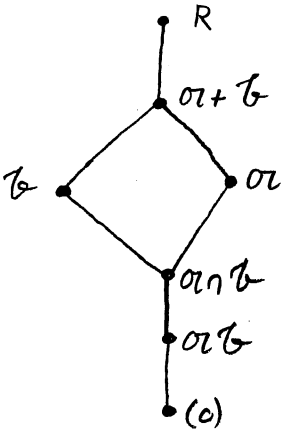
$$\mathfrak{a}\mathfrak{b}$$

bestående af elementer i R af formen

$$a_1 b_1 + \cdots + a_k b_k, \quad a_1, \ldots, a_k \in \mathfrak{a}; \; b_1, \ldots, b_k \in \mathfrak{b}.$$

Det ses let, at også $\mathfrak{a} + \mathfrak{b}$ og $\mathfrak{a}\mathfrak{b}$ er idealer i R.

Fællesmængden $\mathfrak{a} \cap \mathfrak{b}$ er det største ideal, som er indeholdt i både $\mathfrak{a}$ og $\mathfrak{b}$, summen $\mathfrak{a} + \mathfrak{b}$ er det mindste ideal, som indeholder både $\mathfrak{a}$ og $\mathfrak{b}$, og produktet $\mathfrak{a}\mathfrak{b}$ er det mindste ideal, som indeholder alle produkter ab, $a \in \mathfrak{a}$, $b \in \mathfrak{b}$. Det er klart, at $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$.



5.2. For idealer $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ i R ses det let, at

$$\mathfrak{a} \cap (\mathfrak{b} \cap \mathfrak{c}) = (\mathfrak{a} \cap \mathfrak{b}) \cap \mathfrak{c}$$
$$\mathfrak{a} + \mathfrak{b} = \mathfrak{b} + \mathfrak{a}, \quad (\mathfrak{a} + \mathfrak{b}) + \mathfrak{c} = \mathfrak{a} + (\mathfrak{b} + \mathfrak{c})$$
$$(\mathfrak{a}\mathfrak{b})\mathfrak{c} = \mathfrak{a}(\mathfrak{b}\mathfrak{c}), \quad \mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a}$$
$$(\mathfrak{a} + \mathfrak{b})\mathfrak{c} = \mathfrak{a}\mathfrak{c} + \mathfrak{b}\mathfrak{c}.$$

5.3. Analogt - eller induktivt - kan vi til idealer $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ i R definere <u>fællesmængden</u> $\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n$, <u>summen</u> $\mathfrak{a}_1 + \cdots + \mathfrak{a}_n$ og <u>produktet</u> $\mathfrak{a}_1 \cdots \mathfrak{a}_n$.

For hovedidealer $Ra_1, \ldots, Ra_n$ bliver produktet hovedidealet frembragt af $a_1 \cdots a_n$ (og summen bliver idealet frembragt af $a_1, \ldots, a_n$, således at den tidligere indførte betegnelse hvfor harmonerer med den ovenfor indførte)

5.4 Eksempel. For hovedidealer (a) og (b) i $\mathbb{Z}$ ser vi let, at

$(a) \cap (b) = (m)$, hvor m er mindste fælles multiplum af a og b.

$(a) + (b) = (d)$, hvor d er største fælles divisor i a og b

$(a)(b) = (c)$, hvor $c = ab$.

5.5. Eksempel. I ringen $R = \mathbb{Z}[\sqrt{-5}]$ er idealerne

$$\mathfrak{m} = R3 + R(2+\sqrt{-5}), \quad \overline{\mathfrak{m}} = R3 + R(2-\sqrt{-5})$$

maksimalidealer. For produktet finder vi

$$\mathfrak{m}\,\overline{\mathfrak{m}} = R3,$$

thi "$\subseteq$" følger af, at vi har $3 \cdot 3 \in R3$, $3(2-\sqrt{-5}) \in R3$ $(2+\sqrt{-5})3 \in R3$ og $(2+\sqrt{-5})(2-\sqrt{-5}) = 9 \in R3$, og "$\supseteq$"

følger af at $3 = (-3)3 + (2+\sqrt{-5})3 + 3(2-\sqrt{-5}) \in \mathfrak{m}\overline{\mathfrak{m}}$.

5.6 DEFINITION. Er $\mathfrak{a}$ og $\mathfrak{b}$ idealer i R, siger vi, at $\mathfrak{a}$ er <u>komaksimal med</u> $\mathfrak{b}$, eller at $\mathfrak{a}$ og $\mathfrak{b}$ er <u>komaksimale</u>, hvis $\mathfrak{a}+\mathfrak{b} = R$. Idealer $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ kaldes <u>parvis komaksimale</u>, hvis $\mathfrak{a}_i + \mathfrak{a}_j = R$, $i \neq j$. $i,j = 1, \dots, n$.

Det er klart, at forskellige maksimalidealer $\mathfrak{m}_1, \dots, \mathfrak{m}_n$ er parvis komaksimale, thi er $\mathfrak{m}$ og $\tilde{\mathfrak{m}}$ to forskellige maksimalidealer, så er $\mathfrak{m} \not\subset \tilde{\mathfrak{m}}$, og altså $\tilde{\mathfrak{m}} \subset \tilde{\mathfrak{m}} + \mathfrak{m}$, og dermed $\tilde{\mathfrak{m}} + \mathfrak{m} = R$.

5.7 SÆTNING. <u>Er $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ idealer i R, således at $\mathfrak{a}$ er komaksimal med $\mathfrak{b}$ og komaksimal med $\mathfrak{c}$, så er $\mathfrak{a}$ komaksimal med $\mathfrak{b}\mathfrak{c}$.</u>

Bevis. Vi har $\mathfrak{a}+\mathfrak{b} = R$ og $\mathfrak{a}+\mathfrak{c} = R$, og skal vise, at $\mathfrak{a}+\mathfrak{b}\mathfrak{c} = R$. Nu er idealerne $\mathfrak{a}\mathfrak{a}$, $\mathfrak{b}\mathfrak{a}$ og $\mathfrak{a}\mathfrak{c}$ alle indeholdt i $\mathfrak{a}$, og påstanden følger af at vi har

$$R = RR = (\mathfrak{a}+\mathfrak{b})(\mathfrak{a}+\mathfrak{c}) = (\mathfrak{a}\mathfrak{a} + \mathfrak{b}\mathfrak{a} + \mathfrak{a}\mathfrak{c}) + \mathfrak{b}\mathfrak{c}$$
$$\subseteq \mathfrak{a} + \mathfrak{b}\mathfrak{c} = R \quad \blacksquare$$

Sætningen kan specielt anvendes når $\mathfrak{b} = \mathfrak{c}$, og ved gentagen anvendelse ser vi, at hvis $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ er parvis komaksimale, så er også potenser $\mathfrak{a}_1^{\nu_1}, \dots, \mathfrak{a}_n^{\nu_n}$ parvis komaksimale. Specielt er altså potenser $\mathfrak{m}_1^{\nu_1}, \dots, \mathfrak{m}_n^{\nu_n}$, af forskellige maksimalidealer $\mathfrak{m}_1, \dots, \mathfrak{m}_n$, altid parvis komaksimale.

5.8. Eksempel. For idealer (a) og (b) i $\mathbb{Z}$ har vi som nævnt $(a)+(b)=(c)$, hvor c er en største fælles divisor for a og b. At (a) og (b) er komaksimale betyder altså, at 1 er største fælles divisor for a og b. Vi siger da også, at a og b er primiske.

For hvert primtal p er $(p) \subset \mathbb{Z}$ et maksimalideal. Af 5.7 følger derfor, at potenser $p_1^{\nu_1}, \ldots, p_n^{\nu_n}$ af forskellige primtal $p_1, \ldots, p_n$ altid er parvis primiske.

5.9. DEN KINESISKE RESTKLASSESÆTNING. *Lad $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ være parvis komaksimale idealer i ringen R. Da er*

$$\mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n = \mathfrak{a}_1 \cdots \mathfrak{a}_n,$$

og ringhomomorfien

$$R \to R/\mathfrak{a}_1 \times \cdots \times R/\mathfrak{a}_n$$

inducerer en isomorfi

$$R/\mathfrak{a}_1 \cdots \mathfrak{a}_n \xrightarrow{\sim} R/\mathfrak{a}_1 \times \cdots \times R/\mathfrak{a}_n.$$

Bevis. Vi viser først den første påstand for $n=2$: Vi har $\mathfrak{a}_1 + \mathfrak{a}_2 = R$, og finder derfor

$$\begin{aligned} \mathfrak{a}_1 \cap \mathfrak{a}_2 &= (\mathfrak{a}_1 \cap \mathfrak{a}_2) R = (\mathfrak{a}_1 \cap \mathfrak{a}_2)(\mathfrak{a}_1 + \mathfrak{a}_2) \\ &= (\mathfrak{a}_1 \cap \mathfrak{a}_2)\mathfrak{a}_1 + (\mathfrak{a}_1 \cap \mathfrak{a}_2)\mathfrak{a}_2 \\ &\subseteq \mathfrak{a}_2\mathfrak{a}_1 + \mathfrak{a}_1\mathfrak{a}_2 \\ &= \mathfrak{a}_1\mathfrak{a}_2 \\ &\subseteq \mathfrak{a}_1 \cap \mathfrak{a}_2, \end{aligned}$$

hvoraf det ønskede fremgår.

Vi kan nu vise den første påstand ved induktion: Gentagen anvendelse af sætning 5.7 viser, at $\mathfrak{a}_1$ er komaksimal med $\mathfrak{a}_2 \cdots \mathfrak{a}_n$, således at vi får:

$$\mathfrak{a}_1(\mathfrak{a}_2 \cdots \mathfrak{a}_n) = \mathfrak{a}_1 \cap (\mathfrak{a}_2 \cdots \mathfrak{a}_n) = \mathfrak{a}_1 \cap (\mathfrak{a}_2 \cap \cdots \cap \mathfrak{a}_n).$$

Idet vi med φ_i betegner den kanoniske homomorfi: $R \to R/\mathfrak{a}_i$, $i = 1, \cdots, n$, er homomorfien:

$$R \to R/\mathfrak{a}_1 \times \cdots \times R/\mathfrak{a}_n$$

givet ved

$$x \longmapsto (\varphi_1, \cdots, \varphi_n).$$

Den inducerer en isomorfi:

$$R/(\text{kernen}) \xrightarrow{\sim} (\text{billedet})$$

Kernen er øjensynlig $\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n$, altså ifølge det allerede viste $= \mathfrak{a}_1 \cdots \mathfrak{a}_n$, så vi mangler kun at vise, at homomorfien er surjektiv. Hertil er det nok for $i = 1, \cdots, n$ at finde et element $e_i \in R$, som afbildes på $(0, \cdots, 1, \cdots, 0) \in R/\mathfrak{a}_1 \times \cdots \times R/\mathfrak{a}_n$, thi et vilkårligt element i $R/\mathfrak{a}_1 \times \cdots \times R/\mathfrak{a}_n$ er af formen $(\varphi_1 x_1, \cdots, \varphi_n x_n)$, og dette element vil da være billede af $x_1 e_1 + \cdots + x_n e_n \in R$.

For at finde e_i bemærker vi, at gentagen anvendelse af sætning 5.7 viser, at $\mathfrak{a}_i$ er komaksimal med produktet $\prod_{j \neq i} \mathfrak{a}_j$. Vi har altså $R = \mathfrak{a}_i + \prod_{j \neq i} \mathfrak{a}_j$, og kan skrive

$$1 = a_i + e_i, \quad \text{hvor } a_i \in \mathfrak{a}_i, e_i \in \prod_{j \neq i} \mathfrak{a}_j.$$

Specielt har vi $e_i \in \mathfrak{a}_j$ for $j \neq i$, og da vi har $e_i - 1 = a_i \in \mathfrak{a}_i$, finder vi for billedet af e_i:

$$(\varphi_1 e_i, \cdots, \varphi_i e_i, \cdots, \varphi_n e_i) = (0, \cdots, 1, \cdots, 0),$$

som ønsket ▨

5.10. Eksempel. Er $p_1, \cdots, p_k$ forskellige primtal, så

er idealerne $(p_1^{\nu_1}), \ldots, (p_k^{\nu_k})$ som nævnt parvis komaksimale. Sættes

$$a = p_1^{\nu_1} \cdots p_k^{\nu_k},$$

så giver restklassesætningen en isomorfi

$$\mathbb{Z}/a \xrightarrow{\sim} \mathbb{Z}/p_1^{\nu_1} \times \cdots \times \mathbb{Z}/p_k^{\nu_k}$$

5.11 Eksempel. For et element $\lambda \in L$, hvor L er et legeme, kan vi betragte homomorfien $L[X] \to L$ defineret ved

$$p = a_0 + a_1 X + \cdots + a_m X^m \mapsto p(\lambda) = a_0 + a_1\lambda + \cdots + a_m\lambda^m.$$

Da L er et legeme, og da homomorfien er surjektiv, bliver kernen et maksimalideal. Det er let at se, at kernen bliver hovedidealet $(X-\lambda)$ [Skriv for et polynomium p (ved division med rest)

$$p(X) = q(X)(X-\lambda) + r$$

hvor r er konstant. Vi har $p(\lambda) = 0 \Leftrightarrow r = 0 \Leftrightarrow p \in (X-\lambda)$] Af 5.7 følger, at når $\lambda_1, \ldots, \lambda_m$ er forskellige elementer i L, så er potenserne $(X-\lambda_1)^{\nu_1}, \ldots, (X-\lambda_m)^{\nu_m}$ parvis komaksimale. Sættes

$$f(X) = (X-\lambda_1)^{\nu_1} \cdots (X-\lambda_m)^{\nu_m},$$

så giver restklassesætningen en isomorfi

$$L[X]/(f) \xrightarrow{\sim} L[X]/(X-\lambda_1)^{\nu_1} \times \cdots \times L[X]/(X-\lambda_m)^{\nu_m}.$$

5.12. Eksempel. I talringen $R = \mathbb{Z}[\sqrt{-5}]$ er (jfr. 4.6 og 5.5). $\mathfrak{m} = R3 + R(2+\sqrt{-5})$ og $\overline{\mathfrak{m}} = R3 + R(2-\sqrt{-5})$ maksimalidealer, og $\mathfrak{m}\overline{\mathfrak{m}} = R3$. Vi har $R/\mathfrak{m} \xrightarrow{\sim} \mathbb{Z}/3$, $R/\overline{\mathfrak{m}} \xrightarrow{\sim} \mathbb{Z}/3$, og får en isomorfi

$$R/R3 \xrightarrow{\sim} \mathbb{Z}/3 \times \mathbb{Z}/3.$$

FAKTORIELLE RINGE

I det følgende betegner R et kommutativt integritetsområde. Nulreglen gælder altså i R: Af en ligning $rx = ry$, hvor $r \neq 0$, følger $x = y$.

1. Irreducible elementer og primelementer.

1.1. DEFINITION. De invertible elementer i R kaldes også <u>enheder</u>. Et element $a \in R$ kaldes <u>associeret med</u> et element $b \in R$, hvis der findes en enhed u, så at $b = ua$. Det er klart, at "associeret med" er en ækvivalensrelation.

1.2. I ringen $\mathbb{Z}$ er enhederne ± 1. Elementerne associerede med et tal $a \neq 0$ er a og $-a$. Heriblandt findes netop et positivt tal.
I ringen $L[X]$ af polynomier med koefficienter i et legeme L er enhederne netop konstanterne $\neq 0$. Elementerne associerede med et polynomium $A(X) \neq 0$ er polynomierne $cA(X)$, hvor $c \in L^*$. Heriblandt findes netop et normeret polynomium.

1.3. DEFINITION. Er d og a elementer i R, siger vi, at <u>d er divisor i a</u> eller at <u>d går op i a</u> eller at <u>a er et multiplum af d</u>, og vi skriver

$$d \mid a,$$

hvis der findes et element $x \in R$, så at

$$dx = a.$$

De <u>trivielle divisorer</u> i a er enhederne og de elementer, der er associerede med a.

1.4. DEFINITION. Ved et <u>irreducibelt</u> element i R forstås et element $p \neq \{$enhed, der kun har trivielle divisorer.

At et element $p \neq \{$enhed er irreducibelt, betyder altså, at de eneste fremstillinger af p som et produkt $p = dx$ er de trivielle, hvor en af faktorerne er en enhed (og hvor den anden faktor så er associeret med p).

1.5. I ringen $\mathbb{Z}$ er de irreducible elementer $\pm$ primtallene.

I ringen $L[X]$, hvor L er et legeme, følger af $a(X) = r(X)\,d(X)$, at

$$\deg a = \deg r + \deg d.$$

Konstanterne $\neq 0$, altså enhederne i $L[X]$ har grad 0. Polynomierne associerede med $a(X) \neq 0$ har samme grad som $a(X)$. For en ikke-triviel divisor $d(X)$ i $a(X)$ gælder altså

$$0 < \deg d < \deg a.$$

Specielt ser vi, at alle 1ste grads polynomier er irreducible.

Det følger let af algebraens fundamentalsætning, at de irreducible polynomier i $\mathbb{C}[X]$ netop er 1ste grads polynomierne.

Polynomiet X^2+1 er derimod et irreducibelt polynomium i $\mathbb{R}[X]$, thi en ikke-triviel

divisor i dette 2^{den} grads polynomium måtte være et 1ste grads polynomium i $\mathbb{R}[X]$, og ville altså have en rod i $\mathbb{R}$, men så ville denne rod også være rod i X^2+1 i modstrid med at X^2+1 ikke har reelle rødder. Det er ikke svært ud fra algebraens fundamentalsætning at vise, at de irreducible polynomier i $\mathbb{R}[X]$ er 1ste grads polynomierne samt de 2^{den} grads polynomier, der ikke har reelle rødder.

Som vi senere skal se, er polynomiet X^n+2 et irreducibelt polynomium i $\mathbb{Q}[X]$, $n=1,2,\cdots$] $\mathbb{Q}[X]$ findes altså irreducible polynomier af enhver grad.

1.6. I en kvadratisk talring $R=\mathbb{Z}[\xi]$, hvor ξ er en irrational rod i $X^2-AX-B \in \mathbb{Z}[X]$, har vi homomorfien: $R \to R$ defineret ved

$$r = r_1 + r_2\xi \longmapsto r' = r_1 + r_2\xi',$$

hvor ξ' er den anden rod i X^2-AX-B. Videre har vi sat $N(r) = rr' = r_1^2 - Br_2^2 + Ar_1r_2 \in \mathbb{Z}$, og vi har set, at $N(0)=0$, $N(r)\neq 0$, hvis $r\neq 0$,

$$N(rd) = N(r)N(d).$$

Endelig har vi set, at $u\in R$ er en enhed, hvis og kun hvis $N(u) = \pm 1$. Det følger nu viden, at hvis d i R er en ikke-triviel divisor i a, så er $N(d)$ i $\mathbb{Z}$ en ikke-triviel divisor i $N(a)$.

Gauß' talring $\mathbb{Z}[i]$ har enhederne $\pm 1, \pm i$. Elementet 2 er reducibelt, idet $2 = (1+i)(1-i)$. Men $1+i$ og $1-i$ er irreducible, idet $N(1\pm i) = 2$ er irreducibel i $\mathbb{Z}$. Elementet 3 er irreducibelt,

thi da $N(3) = 3^2$, måtte vi for en ikke-triviel divisor d i 3 have $N(d) = \pm 3$, men der findes ingen elementer $d = d_1 + id_2 \in \mathbb{Z}[i]$ med $N(d) = d_1^2 + d_2^2 = \pm 3$. Elementet 5 er reducibelt, idet $5 = (2+i)(2-i)$; og $2+i$ og $2-i$ er irreducible, idet $N(2 \pm i) = 5$.

Ringen $\mathbb{Z}[\sqrt{-5}]$ har enhederne ± 1. Elementet 2 er irreducibelt, da $N(2) = 2^2$, og da intet element $d = d_1 + d_2\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ opfylder $N(d) = d_1^2 + 5d_2^2 = \pm 2$. Tilsvarende ser vi, at 3 er irreducibelt, idet intet element d i $\mathbb{Z}[\sqrt{-5}]$ opfylder $N(d) = \pm 3$. Elementet $1+\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ har $N(1+\sqrt{-5}) = 6 = 2 \cdot 3$. Det følger, at $1+\sqrt{-5}$ er irreducibelt i $\mathbb{Z}[\sqrt{-5}]$. Bemærk, at

$$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5}).$$

Elementet $5 = -\sqrt{-5} \cdot \sqrt{-5}$ er reducibelt i $\mathbb{Z}[\sqrt{-5}]$, og $29 = (3+2\sqrt{-5})(3-2\sqrt{-5})$ er reducibelt i $\mathbb{Z}[\sqrt{-5}]$.

1.7. De indførte begreber spejler sig i relationer mellem de tilhørende hovedidealer. Vi får således:

u er enhed $\Leftrightarrow$ $(u) = R$ $(= (1))$
b er associeret med a $\Leftrightarrow$ $(b) = (a)$
d er divisor i a $\Leftrightarrow$ $a \in (d)$ $\Leftrightarrow$ $(a) \subseteq (d)$
d er triviel divisor i a $\Leftrightarrow$ $(d) = (1)$ eller $(d) = (a)$.

Divisorerne d i a svarer altså til hovedidealer (d) således at

$$(a) \subseteq (d) \subseteq R,$$

og de triviele divisorer svarer til hovedidealer, hvor et af de to mulige ligheds tegn $(a) = (d)$ eller $(d) = R$ forekommer.

Vi får derfor:

1.8. SÆTNING. *Et element $p \neq 0$ i R er irreducibelt, hvis og kun hvis hovedidealet (p) er maksimalt blandt hovedidealer $\subset R$.* ▨

1.9. DEFINITION. Ved et *primelement* i R forstås et element $p \neq$ {enhed}, således at der for alle elementer $a, b \in R$ gælder

$$p/ab \Rightarrow p/a \vee p/b.$$

Betingelsen kan skrives

$$ab \in (p) \Rightarrow a \in (p) \vee b \in (p),$$

så vi får:

1.10 SÆTNING. *Et element $p \neq 0$ i R er et primelement, hvis og kun hvis hovedidealet (p) er et primideal i R.* ▨

1.11. SÆTNING. *Ethvert primelement p i R er irreducibelt.*

Bevis. Vi antager, at $p = d_1 d_2$, og skal vise, at en af faktorerne er en enhed. Vi har specielt $p/d_1 d_2$, og det følger, at p går op i en af faktorerne, f.eks. p/d_1. Vi kan altså skrive $d_1 = pu$, og får $p = d_1 d_2 = pud_2$, men så er $1 = ud_2$, og d_2 er altså en enhed ▨

1.12. Eksempel. Det omvendte gælder i almindelighed ikke. Således er (jfr. eks. 1.6) elementet 2 irreducibelt i $\mathbb{Z}[\sqrt{-5}]$, og da

$$2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

har vi $2 \mid (1+\sqrt{-5})(1-\sqrt{-5})$. Men 2 er ikke divisor i nogen af faktorerne. (idet de to faktorer som nævnt i 1.6 ligeledes er irreducible).

1.13. ± primtallene er definerede som de irreducible elementer i ringen $\mathbb{Z}$. Det er velkendt, at primtallene er primelementer i $\mathbb{Z}$ ("et primtal, der går op i et produkt, går op i en af faktorerne"). Det følger af at $\mathbb{Z}$ er en hovedidealring, idet vi har følgende almindelige

1.14 SÆTNING. Hvis R er et hovedidealområde, så er et element $p \neq 0$ irreducibelt, hvis og kun hvis det er et primelement. Hovedidealet (p) frembragt af et sådant element er et maksimalideal i R

Bevis. "hvis" gælder generelt
"kun hvis". At $p \neq 0$ er irreducibelt, er ensbetydende med at hovedidealet (p) er maksimalt blandt hovedidealer $\subset R$ (sætning 1.8). Når R er en hovedidealring, er dette ensbetydende med at (p) er et maksimalideal, og dette medfører at (p) er et primideal. Følgelig er p et primelement (sætning 1.10).
Den sidste påstand så vi undervejs ▨

1.15. Er $p \in \mathbb{Z}$ et primtal, er $(p) \subset \mathbb{Z}$ et maksimalideal, og kvotienten $\mathbb{Z}/p$ altså et legeme.

Elementet 3 er irreducibelt i $\mathbb{Z}[i]$, så (3) er et maksimalideal i $\mathbb{Z}[i]$, og kvotienten $\mathbb{Z}[i]/(3)$ bliver et legeme. (Det får $9 = 3^2$ elementer!)

2. Faktorielle ringe

2.1. DEFINITION. Er der i R givet elementer $a, d_1, \dots, d_r$, således at $a = d_1 \cdots d_r$, siger vi kort, at $a = d_1 \cdots d_r$ er en opløsning (af a i faktorerne $d_1, \dots, d_r$). En opløsning $a = p_1 \cdots p_r$ kaldes irreducibel, hvis faktorerne $p_1, \dots, p_r$ er irreducible, og den kaldes en primopløsning, hvis faktorerne $p_1, \dots, p_r$ er primelementer.

2.2. SÆTNING. Primopløsninger er entydige i følgende forstand: Er $p_1 \cdots p_r$ og $q_1 \cdots q_s$ primopløsninger, og er

$$p_1 \cdots p_r \text{ associeret med } q_1 \cdots q_s,$$

så er $s = r$, og der gælder (eventuelt efter en passende permutation af indices), at p_i er associeret med q_i, $i = 1, \dots, r$.

Bevis. Der findes en enhed u, så at

$$u p_1 \cdots p_r = q_1 \cdots q_s.$$

Da primelementet p_r således er divisor i produktet $q_1 \cdots q_s$, må p_r gå op i en af faktorerne; vi kan antage, at $p_r \mid q_s$, altså at $p_r v = q_s$, med $v \in R$. Da q_s er et primelement, og dermed irreducibelt, følger det af $q_s = p_r v$, at en af faktorerne må være en enhed. Da p_r ikke er en enhed, må altså v være en enhed. Vi har

$$u p_1 \cdots p_{r-1} p_r = v q_1 \cdots q_{s-1} p_r$$

og får ved forkortning

$$u p_1 \cdots p_{r-1} = v q_1 \cdots q_{s-1},$$

men så er

$$p_1 \cdots p_{r-1} \text{ associeret med } q_1 \cdots q_{s-1}.$$

Idet vi fortsætter således, får vi det ønskede ▨

2.3. Den tilsvarende sætning gælder ikke i almindelighed for irreducible opløsninger. F.eks. har vi i $\mathbb{Z}[\sqrt{-5}]$ irreducible opløsningen $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$, og 2 er ikke associeret med nogen faktor på højre side.

2.4. DEFINITION. Ringen R kaldes <u>faktoriel</u>, hvis der til hvert $a \neq \{^0_{\text{enhed}}$ i R findes en primopløsning $a = p_1 \cdots p_r$.

I en faktoriel ring R har altså hvert element $a \neq \{^0_{\text{enhed}}$ en primopløsning $a = p_1 \cdots p_r$ og af sætning 2.2 følger at disse primopløsninger er entydige i den forstand, at hvis $a = q_1 \cdots q_s$ er endnu en primopløsning af a, så er $s = r$ og (eventuelt efter permutation) p_i er associeret med q_i, $i = 1, \ldots, r$.

2.5. SÆTNING. <u>Hvis R er en faktoriel ring, så er et element $p \neq 0$ irreducibelt, hvis og kun hvis det er et primelement.</u>

Bevis. "hvis" gælder generelt.

"kun hvis". Et irreducibelt element p i R har (som alle elementer $\neq \{^0_{\text{enhed}}$) en primopløsning. Da et irreducibelt element kun har trivielle divisorer, kan en sådan primopløsning af p kun indeholde én faktor. Altså er p selv et primelement ▨

2.6. I en faktoriel ring er altså en irreducibel opløsning det samme som en primopløsning. Som vi nedenfor skal se, kan man i visse typer af ringe vise, at hvert element $\neq \{^0_{\text{enhed}}$ har en irreducibel opløsning. En sådan ring er altså faktoriel, hvis der desuden gælder, at ethvert irreducibelt element er et primelement. Men klassisk er følgende kriterium:

SÆTNING. En ring R er faktoriel, hvis og kun hvis der gælder

(1) Et hvert element $a \neq \{^0_{\text{enhed}}$ har en irreducibel opløsning.

(2) Irreducible opløsninger er entydige (bortset fra permutation og association, jfr. sætning 2.2).

Bevis. "kun hvis" er klart, da der i en faktoriel ring gælder at en irreducibel opløsning er det samme som en primopløsning, og primopløsningen findes (definitionen på "faktoriel") og er altid entydige (sætning 2.2).

"hvis". Det er nok at vise, at ethvert irreducibelt element p er et primelement. Antag altså at p går op i et produkt ab:

$$p r = ab$$

Indsætter vi heri irreducible opløsninger $r = r_1 \cdots r_n$, $a = a_1 \cdots a_k$, $b = b_1 \cdots b_\ell$ (her bruges (1)) får vi irreducible opløsninger

$$p r_1 \cdots r_n = a_1 \cdots a_k b_1 \cdots b_\ell .$$

Under brug af (2) slutter vi nu, at p er associeret med en af faktorerne på højre side. Er p f.eks. associeret med a_1, er p specielt divisor i a_1 og dermed i a ▨

2.7. For at angive betingelser, der sikrer, at ethvert element $\neq$ {enhed i en foreløbig ring har en irreducibel opløsning, betragter vi et øjeblik en ring R, i hvilken der findes et element $a \neq$ {enhed, der ikke har nogen irreducibel opløsning. Elementet a er specielt ikke selv irreducibelt, så vi kan skrive $a = bc$, hvor b, c er $\neq$ {enhed. Hvis begge faktorer havde en irreducibel opløsning, ville vi ved indsætning få en irreducibel opløsning af a. Vi slutter altså, at mindst en af faktorerne ikke har nogen irreducibel opløsning. Et element $a \neq$ {enhed, der ikke har nogen irreducibel opløsning, har altså en ikke-triviel divisor, der heller ikke har nogen irreducibel opløsning. Ved at fortsætte således ser vi, at der til et element $a \neq$ {enhed, der ikke har nogen irreducibel opløsning, findes en følge

(*) $a = a_1, a_2, \ldots$ så at a_{n+1} er ikke triviel divisor i a_n, $n = 1, 2, \ldots$

Betingelser, der sikrer, at der i en given ring R ikke kan findes nogen følge som (*), vil altså ligeledes sikre, at hvert element $\neq$ {enhed har en irreducibel opløsning.

2.8. Er der således givet en funktion $v : \mathbb{R} \to \mathbb{Z}$, som er nedad begrænset, og opfylder, at der for en ikke-triviel divisor d i $a \neq 0$ gælder

$$v(a) > v(d),$$

så ville en følge som (*) give anledning til en følge

$$v(a) = v(a_1) > v(a_2) > \ldots$$

i $\mathbb{Z}$, i modstrid med at v var nedad begrænset.

I en sådan ring R har altså ethvert element $\neq \{^0_{\text{enhed}}$ en irreducibel opløsning.

Eks. Ringen $\mathbb{Z}$ med funktionen $v: \mathbb{Z} \to \mathbb{Z}$ givet ved $v(a) = |a|$.

Ringen $L[X]$, L et legeme, med funktionen $v: L[X] \to \mathbb{Z}$ givet ved

$$v(p) = \deg p.$$

En kvadratisk talring $\mathbb{Z}[\xi]$ med funktionen $v: \mathbb{Z}[\xi] \to \mathbb{Z}$ givet ved

$$v(r) = |N(r)|.$$

2.9. En følge som (*) 2.7. af elementer i R svarer til en følge af hovedidealer

$$(a_1) \subset (a_2) \subset \cdots$$

Vi får derfor umiddelbart:

SÆTNING. <u>I en noethersk ring R har hvert element $a \neq \{^0_{\text{enhed}}$ en irreducibel opløsning.</u> ▨

2.10. Vi har nu næsten vist følgende

HOVEDSÆTNING. <u>Antag at R er et hovedidealområde. Da er R en faktoriel ring. Primidealerne $\neq (0)$ i R er netop idealerne af formen (p), hvor p er irreducibel. Disse primidealer er maksimalidealer. Primelementerne i R er netop de irreducible elementer.</u>

Bevis. Da R specielt er en noethersk ring, har hvert element $\neq \{^0_{\text{enhed}}$ en irreducibel opløsning. Da hvert irreducibelt element i en hovedidealring er et primelement (sætning 1.14), er en sådan opløs-

ning endda en primoplösning. Altså er R faktoriel. Et primideal $\neq (0)$ er – som alle andre idealer i R – et hovedideal, altså af formen (p), hvor $p \neq 0$. At (p) er et primideal, betyder imidlertid, at p er et primelement, men dette er ensbetydende med at p er irreducibel, og det medfører, at (p) er et maksimalideal (sætning 1.14). ▨

2.11. Ringen $\mathbb{Z}$ er faktoriel. Ethvert primideal $\neq (0)$ i $\mathbb{Z}$ har formen (p), hvor p er et primtal. Kvotientringen $\mathbb{Z}/p$ er et legeme.

Polynomiumsringen $L[X]$, hvor L er et legeme, er faktoriel. Ethvert primideal $\neq (0)$ i $L[X]$ har formen $(p(X))$, hvor $p(X)$ er et irreducibelt polynomium. Kvotienten $L[X]/(p(X))$ er et legeme.

2.12. Gauß' talring $\mathbb{Z}[i]$ er en hovedidealring, og altså faktoriel. Lad os prøve at skaffe os et overblik over primelementerne i $\mathbb{Z}[i]$. Vi har $\mathbb{Z} \subseteq \mathbb{Z}[i]$. Specielt har hvert sædvanligt primtal $p \in \mathbb{Z}$ en primoplösning i $\mathbb{Z}[i]$. For et sådant primtal $p \in \mathbb{Z}$ er der nu netop en af følgende tre muligheder:

0) $p = 2$ har primoplösningen $2 = (1+i)(1-i)$ og $1-i = (-i)(1+i)$ er associeret med $1+i$.

1) p er ulige og et primelement i $\mathbb{Z}[i]$

2) p er ulige og har i $\mathbb{Z}[i]$ en primoplösning

$$p = \pi\bar{\pi},$$

og π og $\bar{\pi}$ er ikke associerede i $\mathbb{Z}[i]$.

Det er klart, at de tre muligheder "udelukker hinanden", så vi skal vise, at et primtal p, der ikke er af type 0) eller 1) har primoplösningen angivet i 2): Et sådant primtal er ikke et primelement i $\mathbb{Z}[i]$, så der findes et primelement $\pi \in \mathbb{Z}[i]$, der er en ikke-triviel divisor i p: $p = \alpha\pi$. Heraf følger $p^2 = N(p) = N(\alpha)N(\pi)$, og vi slutter, at vi må have $p = N(\pi)$ (og $p = N(\alpha)$; vi udnytter, at $\mathbb{Z}$ er faktoriel), altså

$$p = \pi\bar{\pi}.$$

Med π er også $\bar{\pi}$ et primelement, og var $\bar{\pi}$ associeret med π ville vi have $\bar{\pi} = \pm\pi$ eller $= \pm i\pi$. Her er $\bar{\pi} = \pi$ udelukket, da vi ellers ville have $\pi = a \in \mathbb{Z}$, og dermed $p = a^2$ et kvadrat. Til svarende giver $\bar{\pi} = -\pi$, at $\pi = ib$, $b \in \mathbb{Z}$, $p = b^2$ en modstrid, og endelig er $\bar{\pi} = \pm i\pi$ udelukket, idet vi ellers ville have $\pi = a + ia$, $a \in \mathbb{Z}$, og dermed $p = \pi\bar{\pi} = a^2 + a^2 = 2a^2$ i modstrid med at $p \neq 2$ må være ulige.

Vi ser altså, at der (på nær associering) til $p = 2$ svarer ét primelement i $\mathbb{Z}[i]$ (nemlig $1+i$), at der til primtal p af type 1) svarer ét primelement (nemlig p selv) og at der til primtal p af type 2) svarer to primelementer (nemlig π og $\bar{\pi}$). Der gælder nu yderligere, at ethvert primelement i $\mathbb{Z}[i]$ kommer med ved denne inddeling. Er nemlig $\pi \in \mathbb{Z}[i]$ et primelement, har vi $\pi\bar{\pi} = N(\pi) \in \mathbb{Z}$; primoplöses $N(\pi)$ inden for $\mathbb{Z}$, ser vi, at π er divisor i et produkt af sædvanlige primtal, og slutter, at π er divisor i et sædvanligt primtal p, altså $\pi\delta = p$. Vi får $N(\pi)N(\delta) = N(p) = p^2$ og har følgelig $N(\pi) = p^2$ eller

$N(\pi) = p$. Er $N(\pi) = p^2$, altså $\pi\bar{\pi} = p \cdot p$, må p være et primelement i $\mathbb{Z}[i]$ (idet vi ellers kunne primoplose p i $\mathbb{Z}[i]$ og derved på højre side kunne få flere end de to primfaktorer på venstre-side), og π må være associeret med p, som altså er af type 1). Og er $N(\pi) = p$, altså $\pi\bar{\pi} = p$, ser vi at p er af type 0) eller af type 2).

2.13. For at afrunde oversigten over primelementer i $\mathbb{Z}[i]$ viser vi

SÆTNING. <u>For et (sædvanligt) ulige primtal p er følgende betingelser ækvivalente:</u>

(i) <u>p er af type 2)</u> (d: p er ikke primelement i $\mathbb{Z}[i]$)

(ii) <u>Ligningen $x^2 + y^2 = p$ har løsningen $(x,y) \in \mathbb{Z} \times \mathbb{Z}$</u>

(iii) <u>$p \equiv 1 \pmod 4$</u>

(iv) <u>Polynomiet $X^2 + 1$ har en rod i legemet $\mathbb{F}_p = \mathbb{Z}/p$</u>

(v) <u>Kongruensen $x^2 \equiv -1 \pmod p$ har en løsning $x \in \mathbb{Z}$.</u>

Bevis. <u>(i) $\Rightarrow$ (ii)</u>: Vi har $p = \pi\bar{\pi}$ i $\mathbb{Z}[i]$. Skrives $\pi = x + iy$, $x, y \in \mathbb{Z}$ har vi altså $x^2 + y^2 = N(x+iy) = p$.

<u>(ii) $\Rightarrow$ (iii)</u> Er $p = x^2 + y^2$, $x, y \in \mathbb{Z}$, kan x og y ikke begge være lige og ikke begge være ulige. Vi kan derfor antage, at x er lige og y er ulige, men så er $x^2 \equiv 0 \pmod 4$ og $y^2 \equiv 1 \pmod 4$, og altså $p = x^2 + y^2 \equiv 1 \pmod 4$.

<u>(iii) $\Rightarrow$ (iv)</u> Vi kan skrive $p - 1 = 4h$, $h \in \mathbb{N}$. Den multiplikative gruppe $\mathbb{F}_p^*$ har altså orden $4h$, så for hvert element $\lambda \in \mathbb{F}_p^*$ gælder $\lambda^{4h} = 1$. Polynomiet $X^{4h} - 1$ har altså $4h$ rødder i $\mathbb{F}_p$. Nu er

$$X^{4h} - 1 = (X^{2h} - 1)(X^{2h} + 1).$$

så hver af de $4h$ rødder i $X^{4h}-1$ må være rod i $X^{2h}-1$ eller $X^{2h}+1$. Da hvert af disse polynomier højst kan have $2h$ rødder, slutter vi, at de begge har netop $2h$ rødder. Specielt findes altså i $\mathbb{F}_p$ en rod i $X^{2h}+1$, altså et element λ således at $\lambda^{2h}+1=0$, men så er λ^h rod i polynomiet X^2+1.

(iv) $\Rightarrow$ (v): er klart

(v) $\Rightarrow$ (i): Vi kan skrive $x^2+1 = np$, $x\in\mathbb{Z}$, $n\in\mathbb{Z}$, og har altså i $\mathbb{Z}[i]$:

$$np = (x+i)(x-i).$$

Hvis p ikke var af type 2), ville p være af type 1), altså et primelement i $\mathbb{Z}[i]$; Af $p \mid (x+i)(x-i)$ ville derfor følge $p \mid x+i$ eller $p \mid x-i$, altså $p\delta = x+i$ eller $p\delta = x-i$ med et element $\delta\in\mathbb{Z}[i]$. Af $p\delta = x\pm i$ følger imidlertid

$$\delta = \frac{x}{p} \pm \frac{1}{p}i,$$

og dette element tilhører ikke $\mathbb{Z}[i]$, da $\pm\frac{1}{p}$ ikke tilhører $\mathbb{Z}$.

▨

2.14. I en faktoriel ring R tænkes ofte valgt en mængde $\mathcal{P}$ af primelementer i R med den egenskab, at ethvert primelement i R er associeret med netop ét af primelementerne i $\mathcal{P}$. Elementerne i $\mathcal{P}$ er altså repræsentanter for associeretklasserne af primelementer. Efter et sådant valg er primelementerne i R elementerne af formen

$$q = up, \quad \text{hvor } u \text{ er enhed}, \ p\in\mathcal{P}.$$

[I ringen $\mathbb{Z}$ vælges sædvanligvis for $\mathcal{P}$ mængden af (positive) primtal, i ringen $L[X]$, L et legeme, vælges sædvanligvis for $\mathcal{P}$ mængden af normerede, irreducible polynomier].

Er der i en faktoriel ring R valgt et sådant repræsentantsystem $\mathcal{P}$ for primelementerne, ser vi, at hvert element $a \neq$ enhed i R har en entydig opløsning

$$a = u p_1^{\nu_1} \cdots p_k^{\nu_k},$$

hvor u er en enhed, $p_1, \cdots, p_k$ er forskellige elementer i $\mathcal{P}$, og $\nu_1, \cdots, \nu_k \in \mathbb{N}$. I en sådan fremstilling kan vi eventuelt tilføje potenser med eksponent 0. Er $a \neq 0$ betegner vi for hvert $p \in \mathcal{P}$ med $v_p(a)$ den eksponent p forekommer i ved ovenstående opløsning af a. [vi sætter $v_p(a) = 0$, hvis a er en enhed]. Vi har altså $v_p(a) \geqslant 0$, og $v_p(a) > 0$ gælder kun for endelig mange $p \in \mathcal{P}$. Opløsningen kan nu skrives

$$a = u \prod_{p \in \mathcal{P}} p^{v_p(a)}$$

Er også $b \neq 0$, ser vi, at

$$v_p(ab) = v_p(a) + v_p(b)$$

og

$$v_p(a+b) \geqslant \min\{v_p(a), v_p(b)\}.$$

(med den oplagte konvention $v_p(0) = \infty$).

Vi ser, at d er divisor i a, hvis og kun hvis

$$v_p(d) \leqslant v_p(a) \text{ for alle } p \in \mathcal{P}.$$

Ofte vil vi tillade os at kalde opløsningen

$$a = u \prod_{p \in \mathcal{P}} p^{v_p(a)}$$

for primopløsningen af a. Ud fra denne opløsning kan altså samtlige divisorer i a bestemmes. Det er elementerne af formen

$$d = w \prod_{p \in \mathcal{P}} p^{\mu_p}, \quad \text{hvor } 0 \leqslant \mu_p \leqslant v_p(a)$$

På nær associering er altså antallet af divisorer $= \prod_{p \in \mathcal{P}} (v_p(a)+1)$.

2.15. Vi minder om at integritetsområdet R kan indlejres i sit brøklegeme K. Hvert element α i $K^* = K \setminus \{0\}$ er af formen $\alpha = \frac{a}{b} = a/b = ab^{-1}$, hvor $a, b \in R \setminus \{0\}$. Er R faktoriel, og har vi primopløsninger

$$a = up_1^{\nu_1} \cdots p_r^{\nu_r}, \quad b = vp_1^{\mu_1} \cdots p_r^{\mu_r}, \quad \nu_i, \mu_i \geqslant 0$$

hvor u, v er enheder og $p_1, \ldots, p_r \in \mathcal{P}$, får vi for α en fremstilling

$$\alpha = (uv^{-1})\, p_1^{\nu_1 - \mu_1} \cdots p_r^{\nu_r - \mu_r},$$

altså en fremstilling af formen

$$\alpha = w\, p_1^{\lambda_1} \cdots p_r^{\lambda_r}, \qquad \lambda_i \in \mathbb{Z}$$

hvor w er en enhed i R. Det er let at se, at denne fremstilling af et element $\alpha \in K^*$ er entydig.

Idet vi for hvert $p \in \mathcal{P}$ med $v_p(\alpha)$ betegner den eksponent p forekommer med ved denne fremstilling, kan vi altså skrive

$$\alpha = w \prod_{p \in \mathcal{P}} p^{v_p(\alpha)}, \quad w \text{ enhed i } R$$

Her er altså v_p en afbildning $v_p : K^* \to \mathbb{Z}$,

og vi finder som før:

$$v_p(\alpha\beta) = v_p(\alpha) + v_p(\beta)$$
$$v_p(\alpha+\beta) \geqslant \min\{v_p(\alpha), v_p(\beta)\}.$$

2.16. Som anvendelse af disse primopløsninger viser vi følgende

SÆTNING. *Lad der for tallet $n \in \mathbb{N}$ være givet primopløsningen*

$$n = 2^a p_1^{b_1} \cdots p_r^{b_r} q_1^{c_1} \cdots q_s^{c_s}$$

hvor primtallene p_i er $\equiv 3 \pmod 4$ og primtallene q_j er $\equiv 1 \pmod 4$. Ligningen

$$x^2 + y^2 = n, \quad (x,y) \in \mathbb{Z}\times\mathbb{Z}$$

har da løsninger, hvis og kun hvis $b_1 \equiv 0 \pmod 2, \ldots, b_r \equiv 0 \pmod 2$. Er dette opfyldt, bliver antallet af løsninger $4(c_1+1)\cdots(c_s+1)$.

Bevis. Elementer $(x,y) \in \mathbb{Z}\times\mathbb{Z}$ svarer til elementer $z = x+iy \in \mathbb{Z}[i]$. Vi har $N(z) = x^2+y^2$, så løsningerne til ligningen $x^2+y^2 = n$ svarer til de elementer $z \in \mathbb{Z}[i]$, for hvilke $N(z) = z\bar{z} = n$.
Nu er $\mathbb{Z}[i]$ faktoriel, og samtlige primelementer er (på nær association): primelementet $1+i$ svarende til primtallet 2, primelementer p svarende til hvert primtal $p \equiv 3 \pmod 4$ (d: af type 1)) og primelementer q', q'' med $q'' = \bar{q}'$ og $q'q'' = q$ svarende til primtal $q \equiv 1 \pmod 4$ (d: af type 2)) (jfr. 2.12 og 2.13).
Hvert element $z \neq 0$ i $\mathbb{Z}[i]$ har altså en entydig opløsning (u er en enhed, altså $= \pm 1, \pm i$)

$$z = u(1+i)^\alpha p_1^{\beta_1} \cdots p_r^{\beta_r} q_1'^{\gamma_1'} q_1''^{\gamma_1''} \cdots q_s'^{\gamma_s'} q_s''^{\gamma_s''}$$

Vi har $N(u) = 1$, $N(1+i) = 2$, $N(p_i) = p_i^2$, $N(q_j') = N(q_j'') = q_j$,

og finder altså

$$N(z) = 2^{\alpha} p_1^{2\beta_1} \cdots p_r^{2\beta_r} q_1^{\gamma_1' + \gamma_1''} \cdots q_s^{\gamma_s' + \gamma_s''}.$$

Sammenlignes med den givne primopløsning af n, ser vi, at $N(z) = n$,
hvis og kun hvis

$$\alpha = a, \quad 2\beta_1 = b_1, \ \ldots, \ 2\beta_r = b_r$$

$$\gamma_1' + \gamma_1'' = c_1, \ \ldots, \ \gamma_s' + \gamma_s'' = c_s.$$

Heraf følger påstandene. ▨

3. Største fælles divisor.

3.1 DEFINITION. Lad der være givet elementer a og b i R. Et element c i R kaldes en største fælles divisor for a og b (eller et største fælles mål), hvis c er en fælles divisor for a og b (d: divisor i både a og b), og hvis der for enhver anden fælles divisor d for a og b gælder, at d er divisor i c. Betingelsen kan skrives

$$c/a \wedge c/b \wedge \forall d \in R : d/a \wedge d/b \Rightarrow d/c.$$

Den kan også skrives:

$$\forall d \in R : d/a \wedge d/b \Leftrightarrow d/c.$$

De trivielle fælles divisorer for a og b er enhederne. At disse er de eneste fælles divisorer for a og b er ensbetydende med at 1 er største fælles divisor for a og b. Er dette tilfældet, siger vi at a og b er primiske.

Tilsvarende defineres "en største fælles divisor for $a_1, \ldots, a_n$" og "$a_1, \ldots, a_n$ er primiske".

3.2. Oversættes betingelsen til inklusioner mellem hovedidealer, får den udseendet

$$\forall d \in R : (a) \subseteq (d) \wedge (b) \subseteq (d) \Leftrightarrow (c) \subseteq (d).$$

At et ideal indeholder både (a) og (b) er ensbetydende med at det indeholder idealet $(a,b) = Ra + Rb$ frembragt af a og b. Betingelsen kan altså skrives

$$\forall d \in R : (a,b) \subseteq (d) \Leftrightarrow (c) \subseteq (d),$$

3.3. Vi ser således, at c er en største fælles divisor for a og b, hvis og kun hvis

$$(c) = \bigcap \{(d) \mid (a,b) \subseteq (d)\}$$

Vi bemærker, at for givne a,b er "højre side" en fællesmængde af idealer, og dermed selv et ideal. Det behøver imidlertid ikke at være et hovedideal. Elementerne a og b i R har altså en største fælles divisor, hvis og kun hvis fællesmængden

$$\bigcap \{(d) \mid (a,b) \subseteq (d)\}$$

er et hovedideal. Er dette tilfældet, er de største fælles divisorer for a og b netop frembringerne for dette hovedideal.

3.4. SÆTNING. <u>Hvis R er en hovedidealring, så har to elementer a,b i R altid en største fælles divisor. De største fælles divisorer for a og b er netop frembringerne for (hoved-)idealet $(a,b) = Ra + Rb$. Elementerne a og b er primiske, hvis og kun hvis der findes elementer $x,y \in R$, så at $xa + yb = 1$.</u>

Bevis. Fremgår umiddelbart af betingelsen i 3.2 under brug af at (a,b) er et hovedideal □

Tilsvarende ser vi, at de største fælles divisorer for elementer $a_1, \ldots, a_n$ i en hovedidealring R netop er frembringerne for (hoved-)idealet $(a_1, \ldots, a_n)$, og at elementer $a_1, \ldots, a_n$ i en sådan ring er primiske, hvis og kun hvis der findes elementer $x_1, \ldots, x_n \in R$, så at $x_1 a_1 + \cdots + x_n a_n = 1$.

I en hovedidealring R skrives ofte (ukorrekt) $(a,b) = c$, hvis c er en største fælles di-

visor for a og b (altså hvis $(a,b)=(c)$). Skrivemåden $(a,b)=1$ udtrykker altså at a og b er primiske.

3.5. Også i en vilkårlig faktoriel ring R gælder, at to elementer a og b altid har en største fælles divisor. Dette følger af at spørgsmål om delelighed kan afgøres ud fra primoplösningerne. Mere præcist har vi følgende

SÆTNING. *Er der i en faktoriel ring R valgt et repræsentantsystem $\mathcal{P}$ for primelementerne (jfr. 2.14), og er der for elementer $a, b \neq 0$ givet primoplösninger*

$$a = u p_1^{\alpha_1} \cdots p_r^{\alpha_r} \qquad b = v p_1^{\beta_1} \cdots p_r^{\beta_r}, \quad p_i \in \mathcal{P}$$

så er de største fælles divisorer for a og b netop elementerne af formen

$$c = w p_1^{\gamma_1} \cdots p_r^{\gamma_r},$$

hvor w er en enhed, og $\gamma_i = \min\{\alpha_i, \beta_i\}$, $i = 1, \ldots, r$. ▨

3.6 I en hovedidealring R kan vi kombinere sætningerne 3.4 og 3.5. At elementer $a_1, \ldots, a_n \in R$ er primiske er ensbetydende med at de ikke indeholder nogen fælles primfaktor. Dette kan afgøres ud fra primoplösninger, og det er på den anden side ensbetydende med at der findes elementer $x_1, \ldots, x_n \in R$, så at $x_1 a_1 + \cdots + x_n a_n = 1$.

4. Gauss' sætning.

4.1. Vi betragter ringen $R[X]$ af polynomier med koefficienter i ringen R. Enhederne i $R[X]$ er som bekendt de invertible konstanter, d.v.s. enhederne i R. At et polynomium $A \in R[X]$ er deleligt med en konstant $d \in R$, betyder, at alle A's koefficienter er delelige med d. Hovedidealet $dR[X]$ frembragt af d i $R[X]$ består altså af de polynomier, hvis koefficienter alle tilhører hovedidealet $dR \subseteq R$.

SÆTNING. *Hvis p er et primelement i R, så er p ligeledes et primelement i $R[X]$.*

Bevis. Den kanoniske homomorfi $: R \to R/pR$, der til et element $a \in R$ lader svare restklassen $\bar{a} \in R/pR$ kan udvides til en afbildning: $R[X] \to R/pR\,[X]$ betegnet $A \mapsto \bar{A}$, idet vi for et polynomium

$$A = a_0 + a_1X + \cdots + a_nX^n \in R[X]$$

sætter

$$\bar{A} = \bar{a}_0 + \bar{a}_1X + \cdots + \bar{a}_nX^n \in R/pR\,[X].$$

Det er klart, at $A \mapsto \bar{A}$ er en ringhomomorfi:

$$R[X] \longrightarrow R/pR\,[X],$$

hvis kerne er hovedidealet $pR[X]$.

Er p et primelement i R, altså pR et primideal i R, så er kvotienten R/pR et integritetsområde, og følgelig er også polynomiumsringen $R/pR\,[X]$ et integritetsområde. Homomorfiens kerne, altså $pR[X]$, er derfor et primideal i $R[X]$, men det betyder netop, at p er et primelement i $R[X]$. ▨

4.2 DEFINITION. Et polynomium $A \in R[X]$ kaldes *primitivt*, hvis dets koefficienter er primiske i R.

Dette betyder altså, at de eneste konstanter, der er divisorer i polynomiet A, er de trivielle, d.v.s. enhederne.

4.3. Gauß' LEMMA. *Lad R være en faktoriel ring. Hvis $A, B \in R[X]$ er primitive polynomier, så er også produktet AB et primitivt polynomium.*

Bevis. At elementer i en faktoriel ring er primiske, er ensbetydende med at intet primelement er divisor i dem alle. Var AB ikke et primitivt polynomium, ville der i R findes et primelement p, som var divisor i AB. Da p også er et primelement i $R[X]$ (sætning 4.1), kunne vi slutte, at p var divisor i A eller i B, i modstrid med at både A og B var primitive polynomier ▨

4.4. Udover integritetsområdet R betragter vi dets brøklegeme K og polynomiumsringen $K[X]$. Vi har da

$$\begin{array}{ccc} R & \subseteq & R[X] \\ \cap| & & \cap| \\ K & \subseteq & K[X] \end{array}$$

BEMÆRKNING. *Hvis R er faktoriel, så kan ethvert polynomium $\phi(X) \neq 0$ i $K[X]$ skrives*

$$\phi(X) = \frac{a}{s} F(X),$$

hvor $a, s \in R$ er primiske, og hvor $F(X)$ er et primitivt polynomium i $R[X]$.

Koefficienterne i $\phi(X)$ er jo endelig mange brøker. For disse kan vi finde en fælles nævner (f.eks. produk-

tet af alle naevnere), d.v.s. vi kan skrive

$$\phi(X) = \frac{a_0}{t} + \frac{a_1}{t}X + \cdots + \frac{a_n}{t}X^n = \frac{1}{t}(a_0 + a_1X + \cdots + a_nX^n),$$

hvor $a_0, \ldots, a_n \in R$. Er d en største fælles divisor for $a_0, \ldots, a_n$, kan vi skrive

$$a_0 + a_1X + \cdots + a_nX^n = d\,F(X),$$

hvor $F(X)$ er et primitivt polynomium. Vi får så

$$\phi(X) = \frac{d}{t}F(X),$$

og forkortes brøken $\frac{d}{t}$ men en største fælles divisor for d og t, får vi den ønskede fremstilling.

4.5. KOROLLAR TIL GAUSS' LEMMA. *Lad R være en faktoriel ring, lad $A(X) \in R[X]$ være et primitivt polynomium og lad $\phi(X) \in K[X]$ være et polynomium med koefficienter i brøklegemet K. Hvis $\phi(X)A(X) \in R[X]$, så vil $\phi(X) \in R[X]$.*

Bevis. Vi skriver

$$\phi(X) = \frac{a}{s}F(X),$$

hvor $a, s \in R$ er primiske, og hvor $F(X) \in R[X]$ er et primitivt polynomium (jfr. 4.6), og vi viser, at elementet s må være en enhed i R.

Sætter vi $A(X)\phi(X) = G(X) \in R[X]$, har vi i $R[X]$:

$$a\,F(X)\,A(X) = s\,G(X).$$

Hvis s ikke er en enhed, findes i R et primelement p, som er divisor i s. Dette element p er ikke divisor i a (da a og s var primiske) og det er heller ikke divisor i $F(X)$ eller $A(X)$ (da disse polynomier er primitive). Da p er divisor i produktet $aF(X)A(X)$ er dette i modstrid med at p er

et primelement i $R[X]$ (sætning 4.1) ▨
[Bemærk, at 4.5 egentlig kom ud som korollar til 4.1].

4.6. Er $A(X)$, $G(X)$ polynomier i $R[X]$ således at der i $K[X]$ gælder, at $A(X)$ er divisor i $G(X)$, kan vi i almindelighed ikke slutte, at $A(X)$ er divisor i $G(X)$ inden for $R[X]$. (Eks. $A(X) = 2X+2 \in \mathbb{Z}[X]$ er divisor i $G(X) = X^2-1 \in \mathbb{Z}[X]$ inden for $\mathbb{Q}[X]$, men ikke inden for $\mathbb{Z}[X]$).
Korollar 4.5 udsiger imidlertid for polynomier $A(X)$, $G(X)$ med koefficienter i en faktoriel ring R, at hvis $A(X)$ er divisor i $G(X)$ inden for $K[X]$, og $A(X)$ er et primitivt polynomium, så er $A(X)$ divisor i $G(X)$ inden for $R[X]$.

4.7. GAUSS' SÆTNING. <u>Lad R være en faktoriel ring med brøklegemet K. Da er også polynomiumsringen $R[X]$ faktoriel, og primelementerne i $R[X]$ er dels de konstanter, der er primelementer i R, dels de polynomier i $R[X]$, der er primitive og irreducible i $K[X]$.</u>
Vi minder om, at ringen $K[X]$ er et hovedidealområde og dermed en faktoriel ring.
Bevis. ① Polynomier $P(X)$ i $R[X]$ af den angivne form er primelementer i $R[X]$. Er nemlig $P(X)$ en konstant, følger dette af sætning 4.1 og er $\deg P \geq 1$ følger dette af korollar 4.5. Er nemlig P inden for $R[X]$ divisor i et produkt AB, kan vi, da P er et primelement i $K[X]$, slutte, at P inden for $K[X]$ er divisor i en af faktorerne, og da P ydermere er

primitivt, kan vi slutte, at enhver forskellig fra $R[X]$ er divisor i denne faktor.

② Hvert polynomium $A(X) \neq \{$enhed i $R[X]$ har en opløsning i (prim-) faktorer af den angivne form. Er nemlig A en konstant, følger dette af at R er faktoriel, og er $\deg A \geqslant 1$, betragter vi først en primopløsning af $A(X)$ i $K[X]$:

$$A(X) = \Pi_1(X) \cdots \Pi_r(X).$$

Nu kan vi skrive $\Pi_i(X) = \alpha_i P_i(X)$, hvor $\alpha_i \in K^*$ og $P_i(X) \in R[X]$ er primitivt; da $\Pi_i(X)$ er irreducibel i $K[X]$, er også $P_i(X)$ irreducibel i $K[X]$, og altså af den angivne form, $i = 1, \cdots, r$. Sætter vi $\alpha = \alpha_1 \cdots \alpha_r \in K^*$, har vi

$$A(X) = \alpha P_1(X) \cdots P_r(X).$$

Her er produktet $P_1 \cdots P_r$ igen et primitivt polynomium (Gauß' lemma), og af korollar 4.5 kan vi derfor slutte, at $\alpha \in R$. Idet vi nu primopløser α i R, får vi den søgte opløsning af $A(X)$:

$$A(X) = p_1 \cdots p_s P_1(X) \cdots P_r(X).$$

③ Det følger nu, at $R[X]$ er faktoriel. At samtlige primelementer i $R[X]$ er af den angivne form følger nu let enten af ② eller ved at bemærke, at samtlige irreducible elementer i $R[X]$ må være af den angivne form ▨

4.8. <u>Polynomiumsringen $\mathbb{Z}[X_1, \cdots, X_n]$ i n variable (specielt polynomiumsringen $\mathbb{Z}[X]$ i én variabel) er en faktoriel ring.</u>

<u>Polynomiumsringen $L[X_1, \cdots, X_n]$ i n variable med koefficienter i et legeme L er en faktoriel ring.</u>

Begge resultater bevises ved induktion ud fra Gauss' sætning, idet vi har

$$R[X_1, \ldots, X_n] \simeq R[X_1, \ldots, X_{n-1}][X_n].$$

4.9 SCHÖNEMANN - EISENSTEINS IRREDUCIBILITETSKRITERIUM. *Lad R være en faktoriel ring, og lad*

$$f = a_0 + a_1 X + \cdots + a_n X^n \in R[X]$$

være et primitivt polynomium. Hvis der findes et primelement $p \in R$, så at

$$p \mid a_0,\ p \mid a_1, \ldots, p \mid a_{n-1} \text{ og } p^2 \nmid a_0,$$

så er f et primelement i $R[X]$ (dvs. et irreducibelt polynomium).

Er K brøklegemet for R, kan vi altså slutte, at f er irreducibel i $K[X]$.

Bevis. (Indirekte). Antag, at $f(X) = g(X)\,h(X)$ i $R[X]$, hvor g og h ikke er enheder. Da f er et primitivt polynomium, må vi have $\deg g \geq 1$, $\deg h \geq 1$:

$$a_0 + \cdots + a_n X^n = (b_0 + \cdots + b_k X^k)(c_0 + \cdots + c_{n-k} X^{n-k})$$

hvor $0 < k < n$. Da f er primitivt, er $p \nmid a_n$. Ved overgang til restklasseringen $R/(p)$ får vi

$$\overline{a_n} X^n = (\overline{b_0} + \cdots + \overline{b_k} X^k)(\overline{c_0} + \cdots + \overline{c_{n-k}} X^{n-k})$$

og $\overline{a_n} \neq 0$. Nu er (p) et primideal, og $R/(p)$ et integritetsområde. Vi slutter derfor let, at vi må have $\overline{b_0} = \cdots = \overline{b_{k-1}} = 0$ og $\overline{c_0} = \cdots = \overline{c_{n-k-1}} = 0$. Specielt er altså $p \mid b_0$ og $p \mid c_0$, men så er $p^2 \mid b_0 c_0 = a_0$ i modstrid med forudsætningen. ▨

4.10 Eksempler. Polynomiet $X^n \pm p$, hvor p er et primtal, er irreducibelt i $\mathbb{Z}[X]$ (eller $\mathbb{Q}[X]$). Derimod er $X^4 + 4 = (X^2 - 2X + 2)(X^2 + 2X + 2)$ reducibelt i $\mathbb{Z}[X]$.

Polynomiet $F_p(X) = X^{p-1} + X^{p-2} + \ldots + X + 1 = \frac{X^p - 1}{X - 1}$, hvor p er et primtal, er irreducibelt i $\mathbb{Z}[X]$ (eller $\mathbb{Q}[X]$), idet kriteriet kan anvendes på

$$F_p(X+1) = \frac{(X+1)^p - 1}{X} = X^{p-1} + \sum_{1<i<p} \binom{p}{i} X^{i-1} + p.$$

Er L et legeme, således at $n1 \neq 0$ i L (d.v.s. er L's karakteristik ikke divisor i n), så er polynomiet

$$X^n + Y^n - 1$$

irreducibelt i $L[X,Y] = L[Y][X]$,
thi for primelementet $Y - 1 \in L[Y]$ har vi $(Y-1) \mid Y^n - 1$, og da $Y^n - 1 = [(Y-1)+1]^n - 1 = \sum_{1 \leq i \leq n} \binom{n}{i} (Y-1)^i$
$= (Y-1) + (Y-1)^2 q(Y)$, har vi $(Y-1)^2 \nmid Y^n - 1$.

ALGEBRAISKE ELEMENTER

I det følgende betegner L et legeme.

1. Algebraiske elementer.

1.1. Vi minder om, at en L-algebra (også kaldet en algebra over L) er en ring A, i hvilken der er givet en ringhomomorfi $\varphi: L \to A$, således at

$$\varphi(\lambda)a = a\varphi(\lambda), \quad \lambda \in L, \ a \in A.$$

Algebraen kan betegnes (A, φ) eller blot A.

Er (A, φ) en L-algebra, sætter vi

$$\lambda a = \varphi(\lambda)a, \quad \lambda \in L, \ a \in A$$

Afbildningen $(\lambda, a) \mapsto \lambda a$ er en ydre komposition $L \times A \to A$, og det er let at se, at A med denne ydre komposition som multiplikation med skalar og med den givne addition (i ringen A) er organiseret som et vektorrum over L. Det ses, at vi har

$$(\lambda a)b = a(\lambda b) = \lambda(ab), \quad \lambda \in L, \ a, b \in A,$$

og homomorfien $\varphi: L \to A$ er afbildningen $\lambda \mapsto \lambda 1$, hvor 1 er et-elementet i ringen A.

Er der omvendt givet en mængde A forsynet med kompositioner

$A \times A \to A$ betegnet $(a, b) \mapsto a + b$

$A \times A \to A$ betegnet $(a, b) \mapsto a \cdot b$

$L \times A \to A$ betegnet $(\lambda, a) \mapsto \lambda a$,

således at

1) $(A, +, \cdot)$ er en ring
2) $(A, +, L)$ er et vektorrum
3) $(\lambda a) \cdot b = a(\lambda b) = \lambda(a \cdot b)$ for $\lambda \in L$, $a, b \in A$,

så organiseres ringen A ved afbildningen $\lambda \mapsto \lambda 1$ til en algebra over L.

. DEFINITION. Lad A være en L-algebra. Dimensionen af A som vektorrum over L, kaldes da A's dimension, og betegnes $|A:L|$. En endeligdimensional algebra kaldes også en endelig algebra.

1.2 Algebraen $Mat_n(L)$ af $(n\times n)$-matricer med koefficienter i L har dimensionen n^2 over L, idet en basis udgøres af matricerne ε_{ij}, $i,j = 1,\dots,n$, hvor ε_{ij} har 1 på plads (i,j) og 0 på de øvrige pladser. Er V et n-dimensionalt vektorrum over L, har vi også

$$|End_L(V) : L| = n^2,$$

idet vi efter et valg af basis i V får en isomorfi $End_L(V) \simeq Mat_n(L)$.

Algebraen $L[X]$ af polynomier med koefficienter i L er ikke endelig. Polynomierne $1, X, X^2, \dots$ er en L-basis for $L[X]$. For en kvotient $L[X]/(f)$, hvor $f \neq 0$ er et polynomium af grad n, finder vi

$$|L[X]/(f) : L| = \deg f = n,$$

idet elementerne $\textcircled{1}, \textcircled{X}, \textcircled{X}^2, \dots, \textcircled{X}^{n-1}$ er en L-basis for kvotienten.

$\mathbb{R}$, $\mathbb{C}$ og $\mathbb{H}$ ($\mathbb{H}$ er kvaternionskerlegemet) er endelige $\mathbb{R}$-algebraer. Vi har

$$|\mathbb{R}:\mathbb{R}| = 1, \quad |\mathbb{C}:\mathbb{R}| = 2, \quad |\mathbb{H}:\mathbb{R}| = 4.$$

1.3. Vi minder om at vi svarende til et element α i L-algebraen A har en homomorfi $L[X] \to A$ givet ved $p \mapsto p(\alpha)$, hvor vi for et polynomium

$$p = \lambda_0 + \lambda_1 X + \cdots + \lambda_n X^n \in L[X]$$

har sat

$$p(a) = \lambda_0 1 + \lambda_1 a + \cdots + \lambda_n a^n \in A.$$

Billedet, der betegnes $L[a]$, er den mindste delalgebra af A, som indeholder a, og kernen $\{p \in L[X] \mid p(a)=0\}$ består af de polynomier, der har a som rod. Ifølge isomorfisætningen har vi en L-isomorfi

$$L[X] / \text{kernen} \xrightarrow{\sim} L[a].$$

Kernen $\{p \in L[X] \mid p(a) = 0\}$ er et ideal. Da L er et legeme, er $L[X]$ en hovedidealring; så dette ideal er enten (0) eller af formen (f), med en entydigt bestemt normeret frembringer f.

DEFINITION. Elementet a i L-algebraen A kaldes <u>transcendent (over L)</u>, hvis der for hvert polynomium $p \in L[X]$, $p \neq 0$, gælder $p(a) \neq 0$. Elementet a i A kaldes <u>algebraisk (over L)</u>, hvis der findes polynomier $p \neq 0$ i $L[X]$, så at $p(a) = 0$. Den normerede frembringer for idealet $\{p \in L[X] \mid p(a) = 0\} \subseteq L[X]$ kaldes da <u>a's minimale polynomium</u> og betegnes $f_{a/L}$. Har $f_{a/L}$ graden n, siger vi, at a er <u>algebraisk af grad n</u>

Det minimale polynomium $f_{a/L}$ har altså a som rod, og ethvert polynomium i $L[X]$, der har a som rod, er et multiplum af $f_{a/L}$.

1.4. Hvis $a \in A$ er transcendent, så er homomorfien $p \mapsto p(a)$ en isomorfi : $L[X] \to L[a]$. Elementerne $1, a, a^2, \ldots$ er derfor en L-basis for $L[a]$; specielt er $|L[a] : L| = \infty$.

Hvis $a \in A$ derimod er algebraisk, så inducerer homomorfien $p \mapsto p(a)$ en isomorfi : $L[X]/(f_{a/L}) \xrightarrow{\sim} L[a]$.

Er α algebraisk af grad n, altså $n = \deg f_{\alpha/L}$, så er elementerne $1, \alpha, \dots, \alpha^{n-1}$ derfor en L-basis for $L[\alpha]$. Vi har altså

$$|L[\alpha] : L| = n$$

Specielt er altså $|L[\alpha] : L| < \infty$ i dette tilfælde, så vi slutter:

SÆTNING. *Elementet α i L-algebraen A er algebraisk, hvis og kun hvis delalgebraen $L[\alpha]$ er endelig.*

KOROLLAR. *Hvis A er en endelig L-algebra, så er hvert element α i A algebraisk over L af grad $\leq |A:L|$.*
thi $L[\alpha]$ er specielt et underrum i A.

1.5. Er V et n-dimensionalt vektorrum over L, har vi $|\mathrm{End}_L(V) : L| = n^2$. Enhver endomorfi $u \in \mathrm{End}_L(V)$ er altså algebraisk over L af grad $\leq n^2$. Her gælder som bekendt, at enhver endomorfi $u \in \mathrm{End}_L(V)$ er rod i sit karakteristiske polynomium $\chi_u(X) = \det(u - X1)$. Det minimale polynomium $f_{u/L}$ er derfor divisor i det karakteristiske polynomium χ_u. Specielt er altså $\deg f_{u/L} \leq n$. Eksempel: Matricerne

$$\begin{pmatrix} 0&0&0\\0&0&0\\0&0&0 \end{pmatrix}, \begin{pmatrix} 1&0&0\\0&1&0\\0&0&1 \end{pmatrix}, \begin{pmatrix} \lambda&1&0\\0&\lambda&0\\0&0&\mu \end{pmatrix}, \begin{pmatrix} \lambda&0&0\\0&\lambda&0\\0&0&\mu \end{pmatrix}, \begin{pmatrix} \lambda&0&0\\0&\mu&0\\0&0&\nu \end{pmatrix}, \begin{pmatrix} 0&1\\-1&0 \end{pmatrix},$$

hvor $\lambda, \mu, \nu \in L$ er forskellige, har som minimale polynomier

$$X,\ X-1,\ (X-\lambda)^2(X-\mu),\ (X-\lambda)(X-\mu),\ (X-\lambda)(X-\mu)(X-\nu),\ X^2+1.$$

Elementet $i \in \mathbb{C}$ har det minimale polynomium $f_{i/\mathbb{R}} = X^2+1$. Hvert element i $\mathbb{C}$ er algebraisk over $\mathbb{R}$ af grad ≤ 2.

For en kvaternion $\xi = \lambda_0 + \lambda_1 i + \lambda_2 j + \lambda_3 k \in \mathbb{H}$, $\lambda_0, \lambda_1, \lambda_2, \lambda_3 \in \mathbb{R}$ sættes $\overline{\xi} = \lambda_0 - \lambda_1 i - \lambda_2 j - \lambda_3 k$. Ved udregning finder vi $\xi + \overline{\xi} = 2\lambda_0 \in \mathbb{R}$, $\overline{\xi}\xi = \lambda_0^2 + \lambda_1^2 + \lambda_2^2 + \lambda_3^2 \in \mathbb{R}$.

Polynomiet $\chi_\xi(X) = X^2 - (\xi + \bar{\xi})X + \bar{\xi}\xi$ har således reelle koefficienter, og da det øjensynlig har ξ som rod, slutter vi, at ξ er algebraisk over $\mathbb{R}$ af grad ≤ 2. Vi ser, at det minimale polynomium $f_{\xi/\mathbb{R}}$ er divisor i χ_ξ, og dermed af grad 1 eller 2. Hvis $\xi \notin \mathbb{R}$, er grad 1 udelukket, således at vi i dette tilfælde har $f_{\xi/\mathbb{R}} = \chi_\xi$. Er derimod $\xi \in \mathbb{R}$, finder vi $f_{\xi/\mathbb{R}} = X - \xi$, $\chi_\xi = (X-\xi)^2$.

2. Udvidelser.

2.1. DEFINITION. Ved en udvidelse af legemet L vil vi her forstå et legeme K i hvilket der er givet en homomorfi: $L \to K$. Vi siger også, at K/L er en udvidelse. Den givne homomorfi: $L \to K$ kaldes indlejringen. Den er nødvendigvis injektiv (idet dens kerne er et ideal i L, som ikke kan være hele L (!), og som derfor må være (0)). Ofte identificerer vi elementerne i L med deres billeder i K ved indlejringen, og tænker altså på L som et dellegeme af K. Vi skriver da $L \hookrightarrow K$.

2.2. DEFINITION. Er K/L en udvidelse, kan vi specielt opfatte K som L-algebra. Dimensionen $|K:L|$ kaldes udvidelsens grad. Er $|K:L| < \infty$, kaldes K/L en endelig udvidelse. Er hvert element i K algebraisk over L, siger vi, at K/L er en algebraisk udvidelse.

2.3. SÆTNING. Enhver endelig udvidelse K/L er algebraisk

Bevis. Følger umiddelbart af korollar 1.4 ▨

2.4. Eksempel. $\mathbb{C}/\mathbb{R}$ er en endelig udvidelse. $\mathbb{C}/\mathbb{Q}$ og $\mathbb{R}/\mathbb{Q}$ er uendelige udvidelser.

2.5. Det er klart, at en fællesmængde af dellegemer (resp. delringe) af et legeme K igen er et dellegeme (resp. en delring) af K.

Er der givet en udvidelse $L \hookrightarrow K$, og en

vilkårlig delmængde $S \subseteq K$, kan vi betragte det mindste dellegeme (resp. den mindste delring) af K, som indeholder L og S. Herfor bruges betegnelsen $L(S)$ (resp. $L[S]$). Vi kan opfatte $L(S)$ som en udvidelse: $L \hookrightarrow L(S)$, udvidelsen frembragt af S. Det ses let, at delringen $L[S] \subseteq K$ består af alle endelige L-linearkombinationer af elementer af formen

$$s_1 \cdots s_p, \quad \text{hvor } s_1, \ldots, s_p \in S, \ p \geq 0,$$

og at $L(S)$ er (isomorft med) brøklegemet for $L[S]$.

Er $S = \{s_1, \ldots, s_n\} \subseteq K$ en endelig delmængde, bruges også betegnelserne $L(s_1, \ldots, s_n)$ (resp. $L[s_1, \ldots, s_n]$). Det er klart, at vi i dette tilfælde har

$$L(s_1, \ldots, s_n) = L(s_1, \ldots, s_{n-1})(s_n).$$

Vi siger også, at udvidelsen $L \hookrightarrow L(S)$ fremkommer ved at adjungere elementerne i S til L.

2.6. SÆTNING. *Lad der være givet en udvidelse $L \hookrightarrow K$ og et element $\alpha \in K$. Hvis α er transcendent over L, har vi en isomorfi*

$$L[X] \xrightarrow{\sim} L[\alpha],$$

og dermed en isomorfi mellem brøklegemerne

$$L(X) \xrightarrow{\sim} L(\alpha)$$

Specielt er altså $L \hookrightarrow L(\alpha)$ en uendelig udvidelse.

Hvis α derimod er algebraisk over L, så er det minimale polynomium $f_{\alpha/L}$ et irreducibelt polynomium, ringen $L[\alpha]$ er et legeme, og vi har en isomorfi

$$L[X]/(f_{\alpha/L}) \xrightarrow{\sim} L[\alpha] = L(\alpha)$$

Specielt er $L \hookrightarrow L(\alpha)$ en endelig udvidelse med $|L(\alpha) : L| = \deg f_{\alpha/L}$.

Bevis. Til tilfældet, hvor α er transcendent, følger umiddelbart af overvejelserne i 1.4.

Er α algebraisk, har vi en isomorfi

$$L[X]/(f_{\alpha/L}) \xrightarrow{\sim} L[\alpha].$$

Kvotienten $L[X]/(f_{\alpha/L})$ er således isomorf med en delring af et legeme, og er derfor et integritetsområde. Dit følger, at idealet $(f_{\alpha/L})$ er et primideal. Polynomiet $f_{\alpha/L} \neq 0$ er derfor et primelement i $L[X]$, og specielt irreducibelt. Da $L[X]$ er en hovedidealring, kan vi slutte, at idealet $(f_{\alpha/L})$ endda er et maksimalidеal, og dermed, at kvotienten $L[X]/(f_{\alpha/L}) \xrightarrow{\sim} L[\alpha]$ er et legeme. Vi har derfor $L[\alpha] = L(\alpha)$. Den sidste påstand følger nu klart af 1.4 ▨

2.7. Lad der være givet en udvidelse $L \hookrightarrow K$, og i K et element α, der er algebraisk over L med det minimale polynomium

$$f_{\alpha/L} = X^n + p_{n-1}X^{n-1} + \cdots + p_1 X + p_0 \in L[X].$$

Elementerne ξ i $L[\alpha]$ har da en fremstilling

$$\xi = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1},$$

hvor koefficienterne $a_0, \ldots, a_{n-1} \in L$ er entydigt bestemte. For et produkt $\xi\eta$ finder vi den tilhørende fremstilling ved at bruge $\alpha^n = -p_0 - p_1\alpha - \cdots - p_{n-1}\alpha^{n-1}$. Elementerne i brøklegemet $L(\alpha)$ er af formen

$$\xi/\eta = \frac{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}}{b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}}$$

hvor $(b_0, \ldots, b_{n-1}) \neq (0, \ldots, 0)$. Ifølge sætningen har

vi $L(\alpha) = L[\alpha]$. Brøken ξ/η kan altså entydigt skrives

$$\xi/\eta = z_0 + z_1\alpha + \cdots + z_{n-1}\alpha^{n-1}, \quad z_0, \ldots, z_{n-1} \in L.$$

For at bestemme koefficienterne $z_0, \ldots, z_{n-1}$ udregner vi $\eta(z_0 + \cdots + z_{n-1}\alpha^{n-1}) = (b_0 + \cdots + b_{n-1}\alpha^{n-1})(z_0 + \cdots + z_{n-1}\alpha^{n-1})$ under brug af $\alpha^n = -p_0 - \cdots - p_{n-1}\alpha^{n-1}$, og sammenligner med $\xi = a_0 + \cdots + a_{n-1}\alpha^{n-1}$. Herved fremkommer et lineært ligningssystem til bestemmelse af $z_0, \ldots, z_{n-1}$.

2.8 Eksempel. Elementet $\alpha = \sqrt[3]{2} \in \mathbb{R}$ er algebraisk over $\mathbb{Q}$, idet det er rod i polynomiet $X^3 - 2$. Det minimale polynomium $f_{\sqrt[3]{2}/\mathbb{Q}}$ er altså divisor i $X^3 - 2$; og da $X^3 - 2 \in \mathbb{Q}[X]$ er et irreducibelt polynomium, må vi have $f_{\sqrt[3]{2}/\mathbb{Q}} = X^3 - 2$.
Udvidelsen $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ har altså grad 3: En basis er $1, \sqrt[3]{2}, (\sqrt[3]{2})^2$. F.eks. finder vi

$$\frac{1 + \sqrt[3]{2}}{1 + 2\sqrt[3]{2}} = \frac{-5}{3} - \frac{1}{3}\sqrt[3]{2} + \frac{2}{3}(\sqrt[3]{2})^2$$

2.9. SÆTNING. *Lad $L \subset K$ være en endelig udvidelse, og lad V være et endeligdimensionalt vektorrum over K. Da er V også et endeligdimensionalt vektorrum over L, og*

$$\dim_L V = (\dim_K V)\,|K : L|.$$

Bevis. Lad $v_1, \ldots, v_n \in V$ være en K-basis for V, og lad $\alpha_1, \ldots, \alpha_p \in K$ være en L-basis for K. Vi viser, at de np elementer $\alpha_i v_j \in V$, $i = 1, \ldots, p$; $j = 1, \ldots, n$ er en L-basis for V:

De er et frembringersystem, thi hver vektor $v \in V$ kan skrives som K-linearkombination af vektorerne $v_1, \ldots, v_m$, og her kan hver af koefficienterne skrives som L-linearkombination af elementerne $\alpha_1, \ldots, \alpha_p$. Indsættes får vi v skrevet som L-linearkombination af vektorerne $\alpha_i v_j$.

De er uafhængige, thi en linear relation

$$\sum a_{ij} (\alpha_i v_j) = 0, \qquad a_{ij} = 0,$$

kan skrives $\sum_j \left(\sum_i a_{ij} \alpha_i \right) v_j = 0.$

For hvert j er $\sum_i a_{ij} \alpha_i \in K$, og da v_j'erne er K-uafhængige kan vi slutte, at $\sum_i a_{ij} \alpha_i = 0$, og da α_i'erne er L-uafhængige, kan vi heraf slutte $a_{ij} = 0$ for hvert i. ∎

2.10. SÆTNING. *Lad der være givet udvidelsen $L \hookrightarrow K$ og $K \hookrightarrow M$. Udvidelsen $L \hookrightarrow M$ er da endelig, hvis og kun hvis begge udvidelserne $L \hookrightarrow K$ og $K \hookrightarrow M$ er endelige. Hvis det er tilfældet, har vi*

$$|M : L| = |M : K| \, |K : V|.$$

Bevis. "hvis" fås ved at anvende sætning 2.9 på M opfattet som vektorrum over K.

"kun hvis": Er M endelig dimensionalt som vektorrum over L, så er underrummet K ligeledes endelig dimensionalt over L. Er $v_1, \ldots, v_n \in M$ en L-basis for M, så kan hvert element i M skrives som en L-linearkombination. Her er koefficienterne elementer i $L \hookrightarrow K$, så $v_1, \ldots, v_n$ er også et K-frembringersystem for M.

Følgelig er M et endeligdimensionalt vektorrum over K ▨

2.11. SÆTNING.

Lad der være givet en udvidelse $L \hookrightarrow K$ og elementer $\beta_1, \dots, \beta_n \in K$, der er algebraiske over L. Da er $L[\beta_1, \dots, \beta_n] = L(\beta_1, \dots, \beta_n)$, og udvidelsen $L \hookrightarrow L(\beta_1, \dots, \beta_n)$ er en endelig udvidelse.

Bevis. Vi viser påstanden ved induktion efter n. Den er klart rigtig for $n = 0$. Er $n \geq 1$ og er påstanden rigtig for $n-1$, så er $L[\beta_1, \dots, \beta_{n-1}] = L(\beta_1, \dots, \beta_{n-1})$, og $L \hookrightarrow L(\beta_1, \dots, \beta_{n-1})$ er en endelig udvidelse. Elementet β_n er algebraisk over L, altså rod i et polynomium $\neq 0$ med koefficienter i L. Da disse koefficienter også tilhører det størrelegeme $L' = L(\beta_1, \dots, \beta_{n-1})$, er β_n algebraisk over L'. Af sætning 2.6 følger derfor, at $L'(\beta_n) = L'[\beta_n]$ og at udvidelsen $L' \hookrightarrow L'(\beta_n)$ er endelig. Nu er $L'(\beta_n) = L(\beta_1, \dots, \beta_{n-1})(\beta_n) = L(\beta_1, \dots, \beta_n)$, og vi finder

$$\begin{aligned} L[\beta_1, \dots, \beta_n] &= L[\beta_1, \dots, \beta_{n-1}][\beta_n] = L(\beta_1, \dots, \beta_{n-1})[\beta_n] \\ &= L'[\beta_n] = L'(\beta_n) \\ &= L(\beta_1, \dots, \beta_n), \end{aligned}$$

og da udvidelserne $L \hookrightarrow L'$ og $L' \hookrightarrow L'(\beta_n) = L(\beta_1, \dots, \beta_n)$ begge er endelige, slutter vi af sætning 2.10, at også udvidelsen $L \hookrightarrow L(\beta_1, \dots, \beta_n)$ er endelig ▨

2.12. SÆTNING. Lad der være givet en udvidelse $L \hookrightarrow K$. Delmængden $\bar{L} \subseteq K$ bestående af de elementer $\alpha \in K$, der er algebraiske over L, er da et delegeme (som indeholder L).

Bevis. Sætningen udsiger, at dersom elementer $\alpha, \beta \in K$ er algebraiske over L, så er også summen $\alpha+\beta$, differensen $\alpha-\beta$, produktet $\alpha\beta$ og (dersom $\beta \neq 0$) kvotienten $\frac{\alpha}{\beta}$ algebraiske over L. Disse elementer tilhører alle dellegemet $L(\alpha,\beta) \subseteq K$. Af sætning 2.11 følger, at $L \hookrightarrow L(\alpha,\beta)$ er en endelig udvidelse, og dette medfører (sætning 2.3), at alle elementer i $L(\alpha,\beta)$ er algebraiske over L ▨

2.13. DEFINITION. Er $L \hookrightarrow K$ en udvidelse, så kaldes dellegemet

$$\bar{L} = \{\alpha \in K \mid \alpha \text{ er algebraisk over } L\}$$

for L's <u>algebraiske afslutning i K</u>. Det er klart, at $L \hookrightarrow \bar{L}$ er en algebraisk udvidelse, og at $\bar{L}$ er det største dellegeme $L \hookrightarrow L' \subseteq K$, som er algebraisk over L.

2.14 SÆTNING. <u>Lad der være udvidelser $L \hookrightarrow K$ og $K \hookrightarrow M$. Udvidelsen $L \hookrightarrow M$ er da algebraisk, hvis og kun hvis begge udvidelserne $L \hookrightarrow K$ og $K \hookrightarrow M$ er algebraiske.</u>

Bevis. "hvis". Vi skal vise, at hvert $\beta \in M$ er algebraisk over L. Nu er β algebraisk over K, altså rod i et polynomium $X^n + \alpha_1 X^{n-1} + \ldots + \alpha_n$ med koefficienter $\alpha_1, \ldots, \alpha_n \in K$. Disse koefficienter tilhører naturligvis dellegemet $L(\alpha_1, \ldots, \alpha_n)$, så β er algebraisk over dette dellegeme, og $L(\alpha_1, \ldots, \alpha_n) \hookrightarrow L(\alpha_1, \ldots, \alpha_n)(\beta) = L(\alpha_1, \ldots, \alpha_n, \beta)$ er en endelig udvidelse. Elementerne $\alpha_1, \ldots, \alpha_n$ tilhører K, og er derfor algebraiske over L. Af sætning 2.11 følger derfor, at også $L \hookrightarrow L(\alpha_1, \ldots, \alpha_n)$ er en endelig udvidelse; Sætning 2.10 viser nu først, at $L \hookrightarrow L(\alpha_1, \ldots, \alpha_n)(\beta)$ er endelig, og dernæst, at den mindre udvidelse $L \hookrightarrow L(\beta)$

er endelig. Følgelig er β algebraisk over L.
"kun hvis" er trivielt ▨

2.15. Vi ser specielt, at dersom vi for en udvidelse $L \hookrightarrow K$ betragter den algebraiske afslutning $\overline{L}$ af L i K, så vil hvert element i K, der er algebraisk over $\overline{L}$, selv tilhøre $\overline{L}$.

2.16. DEFINITION. Legemet L kaldes <u>algebraisk afsluttet</u> der som det opfylder en af følgende (ækvivalente) betingelser

(i) Ethvert polynomium $f \in L[X]$ af grad ≥ 1 har en rod i L

(ii) Ethvert polynomium $f \in L[X]$ af grad $n \geq 1$ kan skrives på formen

$$f = a(X-\alpha_1)\cdots(X-\alpha_n), \quad a, \alpha_1, \ldots, \alpha_n \in L$$

(iii) De irreducible polynomier i $L[X]$ er netop 1ste grads polynomierne.

(At disse betingelser er ækvivalente følger af, at $f \in L[X]$ har roden α, hvis og kun hvis $X-\alpha$ er divisor i f. Således ser vi, at <u>(i) $\Rightarrow$ (ii)</u>, ved at skrive $f = (X-\alpha_1)f_2$, hvor α_1 er en rod i f, dernæst skrive $f_2 = (X-\alpha_2)f_3$, og fortsætte indtil vi efter n skridt har $f = (X-\alpha_1)\cdots(X-\alpha_n)f_{n+1}$, hvor f_{n+1} har grad 0, og således er konstant.
<u>(ii) $\Rightarrow$ (i)</u> er klart, <u>(ii) $\Rightarrow$ (iii)</u> er klart, idet de eneste irreducible polynomier af formen i (ii) øjensynlig er 1ste-grads polynomier, og <u>(iii) $\Rightarrow$ (ii)</u>, thi hvert $f \in L[X]$ af grad ≥ 1 kan skrives har en primopløsning $f = a p_1 \cdots p_n$, hvor $p_1, \ldots, p_n$ er normerede, irreducible polynomier (og $a \in L^*$).

Er $p_1, \ldots, p_n$ 1ste-grads polynomier, er dette netop en fremstilling som ønsket.)

2.17. Som bekendt udsiger algebraens fundamentalsætning, at legemet $\mathbb{C}$ af komplekse tal er algebraisk afsluttet.
Tal i $\mathbb{C}$, der er algebraiske over $\mathbb{Q}$, kaldes <u>algebraiske tal</u>. Disse tal udgør altså et legeme $\overline{\mathbb{Q}} \subseteq \mathbb{C}$, den algebraiske afslutning af $\mathbb{Q}$ i $\mathbb{C}$. Der gælder nu, at også <u>legemet $\overline{\mathbb{Q}}$ af algebraiske tal er et algebraisk afsluttet legeme</u>. Et polynomium $f \in \overline{\mathbb{Q}}[X]$ af grad ≥ 1 har nemlig en rod $\alpha \in \mathbb{C}$. Denne rod α er algebraisk over $\overline{\mathbb{Q}}$, og da $\overline{\mathbb{Q}}$ er algebraisk over $\mathbb{Q}$, slutter vi, at α er algebraisk over $\mathbb{Q}$, og dermed at $\alpha \in \overline{\mathbb{Q}}$.

Det er velkendt, at udvidelsen $\mathbb{Q} \hookrightarrow \mathbb{C}$ ikke er en algebraisk udvidelse. Vi har altså $\overline{\mathbb{Q}} \subset \mathbb{C}$.
[At der findes elementer i $\mathbb{C}$, der er transcendente over $\mathbb{Q}$ kan enten vises ved et kardinalitetsargument ($\mathbb{Q}$ og dermed $\mathbb{Q}[X]$ og dermed $\overline{\mathbb{Q}}$ er numerable mængder, $\mathbb{C}$ er ikke numerabel) eller ved at bevise, at visse analytisk definerede tal er transcendente. Således kan man vise, at e og π er transcendente tal].

2.18 Lad $c > 0$ være et reelt tal. Lad os et øjeblik sige, at en følge (r_n) af rationale tal er <u>c-konvergent</u> (mod $\xi \in \mathbb{R}$), hvis elementerne r_n er indbyrdes forskellige, og hvis de kan skrives $r_n = \frac{p_n}{q_n}$, $p_n \in \mathbb{Z}$, $q_n \in \mathbb{N}$, hvor

$$q_n^c (r_n - \xi) \text{ er begrænset.}$$

Det følger let, at vi så har $q_n \to \infty$, og at ξ er grænseværdi

for følgen (r_n). Det er klart, at en c-konvergent følge også er c'-konvergent for hvert $c' < c$. Der gælder nu følgende SÆTNING (Liouville, 1851). *Grænseværdien ξ for en c-konvergent følge (r_n) kan ikke være et algebraisk tal af grad $< c$.*

Bevis. Indirekte. Antag at ξ er rod i et polynomium $f \in \mathbb{Q}[X]$ af grad $N < c$. Vi kan antage, at f har koefficienter i $\mathbb{Z}$ (ellers kan dette opnås ved at multiplicere koefficienterne med en "fælles nævner"). Vi kan skrive

$$f(X) = (X - \xi)\, g(X),$$

hvor polynomiet g har reelle koefficienter, og vi kan skrive $r_n = \frac{p_n}{q_n}$, hvor følgen $q_n^c(r_n - \xi)$ er begrænset. Nu finder vi

$$\begin{aligned} q_n^N f(r_n) &= q_n^N (r_n - \xi)\, g(r_n) \\ &= \frac{1}{q_n^{c-N}}\, q_n^c (r_n - \xi)\, g(r_n) \end{aligned}$$

For $n \to \infty$ har vi her $\frac{1}{q_n^{c-N}} \to 0$ (da $c - N > 0$ og $q_n \to \infty$), $q_n^c(r_n - \xi)$ er begrænset, og $g(r_n) \to g(\xi)$. Følgelig har vi $q_n^N f(r_n) \to 0$. På den anden side er $q_n^N f(r_n) = q_n^N f\left(\frac{p_n}{q_n}\right)$ element i $\mathbb{Z}$, når f er et polynomium af grad N med koefficienter i $\mathbb{Z}$. Vi må derfor have $q_n^N f(r_n) = 0$, altså $f(r_n) = 0$, fra et vist trin, men dette er en modstrid, da r_n'erne er forskellige, og f kun har endelig mange rødder. ▨

Eksempel. $\xi = \sum_{i=1}^{\infty} 10^{-i!}$ er grænseværdi for følgen $r_n = \sum_{i=1}^{n} 10^{-i!}$. Det er let at vise, at (r_n) er c-konvergent for ethvert c. Grænseværdien ξ må derfor være transcendent!

Det er klart, at hvert $\xi \in \mathbb{R}$ er grænseværdi for en 1-konvergent følge (f.eks. følgen $\frac{[n\xi]+1}{n}$). Man kan vise – og det er ikke dybtliggende –, at hvert irrationalt tal er grænseværdi for en 2-konvergent følge.

Det er derimod en dybtliggende sætning (Roth, 1955), at enhver grænseværdi for en c-konvergent følge, hvor $c > 2$, er transcendent.

2.19. Lad der være givet et legeme L og et irreducibelt polynomium $p \in L[X]$. Hvis p har en rod α i en udvidelse $L \hookrightarrow K$, så er p bortset fra en konstant faktor det minimale polynomium for α over L. Polynomiet $f_{\alpha/L}$ er nemlig divisor i p, og da p er irreducibel og dermed kun har trivielle divisorer, følger påstanden. Specielt har vi altså $(p) = (f_{\alpha/L})$, og vi får en isomorfi

$$L[X]/(p) = L[X]/(f_{\alpha/L}) \xrightarrow{\sim} L[\alpha] = L(\alpha)$$

ved hvilken $\overline{X} \longmapsto \alpha$.

Udvidelsen $L \hookrightarrow L(\alpha)$ afhænger altså kun af det givne irreducible polynomium p, og vi slutter let:

SÆTNING. <u>Lad der være et legeme L. Hvis et irreducibelt polynomium $p \in L[X]$ har en rod α i en udvidelse $L \hookrightarrow K$ og en rod α' i en udvidelse $L \hookrightarrow K'$, så findes netop en L-isomorfi $: L(\alpha) \xrightarrow{\sim} L(\alpha')$, således at $\alpha \mapsto \alpha'$.</u>

Bevis.

$$\begin{array}{ccccc} & & L & & \\ & \swarrow & \downarrow & \searrow & \\ (K \supseteq) & L(\alpha) \xleftarrow{\sim} L[X]/(p) & \xrightarrow{\sim} & L(\alpha') & (\subseteq K') \\ & \alpha \longleftarrow \overline{X} & \longmapsto & \alpha' & \end{array}$$

□

2.20. Eksempel. Polynomiet $X^2+1 \in \mathbb{R}[X]$ er irreducibelt, og har i $\mathbb{C}$ rødderne i og $-i$. Vi har $\mathbb{R}(i) = \mathbb{C} = \mathbb{R}(-i)$, og $\mathbb{R}$-isomorfien $: \mathbb{C} \to \mathbb{C}$, som sender $i \mapsto -i$ er

komplekse konjugering.

2.21. SÆTNING. *Lad der være givet et irreducibelt polynomium $p \in L[X]$. Der findes da en udvidelse $L \hookrightarrow K$ således at p har en rod i K.*

Bevis. Da p er irreducibelt, er hovedidealet (p) et maksimalideal i $L[X]$, og kvotienten $K = L[X]/(p)$ er altså et legeme. Den sammensatte afbildning $a \mapsto \textcircled{a}$ af:

$$L \to L[X] \to L[X]/(p) = K$$

er altså en udvidelse, og i denne udvidelse har p roden $\textcircled{X}$. Er nemlig

$$p = a_0 + a_1 X + \cdots + a_n X^n,$$

finder vi i $L[X]/(p)$:

$$0 = \textcircled{p} = \textcircled{a_0 + a_1 X + \cdots + a_n X^n}$$
$$= \textcircled{a_0} + \textcircled{a_1}\textcircled{X} + \cdots + \textcircled{a_n}\textcircled{X}^n$$
$$= p(\textcircled{X}). \quad \blacksquare$$

2.22. Til et givet irreducibelt polynomium $p \in L[X]$ kan vi altså finde en udvidelse $L \hookrightarrow K$ og et element $\alpha \in K$ som er rod i p. I K kan vi betragte delegemet $L(\alpha)$. Dette legeme er isomorft med $L[X]/(p)$, og afhænger altså kun af det givne polynomium p. Vi siger at det fremkommer ved <u>til L at adjungere en rod i p</u>.

F. eks. kan legemet $\mathbb{C}$ af komplekse tal <u>defineres</u> som det legeme der fremkommer ved til $\mathbb{R}$ at adjungere en rod i $X^2 + 1$.

2.23. Har vi givet en udvidelse $L \hookrightarrow K$, får vi en injektiv homomorfi $L[X] \hookrightarrow K[X]$, og kan altså opfatte $L[X]$ som en delring af $K[X]$.

SÆTNING. *Til hvert polynomium*

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0 \in L[X],$$

af grad $n \geq 1$, findes en udvidelse $L \hookrightarrow K$ og elementer $\alpha_1, \ldots, \alpha_n \in K$, så at vi i $K[X]$ har

$$f = a_n (X - \alpha_1) \cdots (X - \alpha_n).$$

Bevis. Der findes et irreducibelt polynomium $p_1 \in L[X]$, som er divisor i f. Adjungeres til L en rod i dette irreducible polynomium, får vi en udvidelse $L \hookrightarrow L_1$ og et element $\alpha_1 \in L_1$, som er rod i p. Elementet α_1 er derfor også rod i f, så i $L_1[X]$ kan vi skrive

$$f = (X - \alpha_1) f_1 \quad , \quad f_1 \in L_1[X].$$

I $L_1[X]$ kan vi finde et irreducibelt polynomium, som er divisor i f_1, og adjungeres til L_1 en rod heri, får vi en udvidelse $L_1 \hookrightarrow L_2$ og et element $\alpha_2 \in L_2$ som er rod i f_2. I $L_2[X]$ har vi derfor $f_1 = (X - \alpha_2) f_2$, $f_2 \in L_2[X]$, altså

$$f = (X_1 - \alpha_1)(X_2 - \alpha_2) f_2 \,, \quad f_2 \in L_2[X].$$

I det vi fortsætter således får vi udvidelser

$$L \hookrightarrow L_1 \hookrightarrow L_2 \hookrightarrow \cdots \hookrightarrow L_n,$$ og elementer $\alpha_i \in L_i \subseteq L_n$, så at vi i $L_n[X]$ har

$$f = (X - \alpha_1) \cdots (X - \alpha_n) f_n \,, \quad f_n \in L_n[X];$$

her må imidlertid f_n have grad 0, og vi slutter, at $f_n = a_n$ ▨

3. Indskud om symmetriske polynomier

3.1. Elementerne i polynomiumsringen $R[X_1, \cdots, X_n]$ i n variable med koefficienter i en kommutativ ring R er endelige summer

$$p = \sum p_{i_1, \ldots, i_n} X_1^{i_1} \cdots X_n^{i_n}$$

Der summeres over alle multiindices $i = (i_1, \cdots, i_n) \in \mathbb{N}_0^n$. At summen er endelig betyder, at der kun for endelig mange $i = (i_1, \cdots, i_n)$ gælder, at koefficienten $p_{i_1, \ldots, i_n}$ er $\neq 0$ i R. Hvis $p_{i_1, \ldots, i_n} \neq 0$, siger vi, at $X_1^{i_1} \cdots X_n^{i_n}$ forekommer i polynomiet p, og $p_{i_1, \ldots, i_n} X_1^{i_1} \cdots X_n^{i_n}$ kaldes et led i p.

Idet vi for et multiindex $i = (i_1, \ldots, i_n)$ sætter

$$X^i = X_1^{i_1} \cdots X_n^{i_n},$$

kan vi skrive

$$p = \sum p_i X^i$$

3.2. Ringen $R[X_1, \cdots, X_n]$ kan opfattes som en R-algebra, idet homomorfien $R \hookrightarrow R[X_1, \cdots, X_n]$ er givet ved

$$r \longmapsto \text{konstante polynomium } r$$

Er der givet en kommutativ R-algebra A, og et sæt $(\alpha_1, \ldots, \alpha_n)$ af elementer i A, kan vi indsætte $(\alpha_1, \ldots, \alpha_n)$ i et polynomium $p \in R[X_1, \cdots, X_n]$, idet vi sætter

$$p(\alpha_1, \ldots, \alpha_n) = \sum p_{i_1 \ldots i_n} \alpha_1^{i_1} \cdots \alpha_n^{i_n} \in A$$

Ved $p \longmapsto p(\alpha_1, \ldots, \alpha_n)$ definerus åbenbart en R-algebrahomomorfi

$$R[X_1, \ldots, X_n] \longrightarrow A;$$

Billedet ved denne afbildning er den mindste delalgebra af A, som indeholder $\alpha_1, \dots, \alpha_n$. Den betegnes $R[\alpha_1, \dots, \alpha_n]$. Hvis afbildningen $p \mapsto p(\alpha_1, \dots, \alpha_n)$ er injektiv, siger vi, at $(\alpha_1, \dots, \alpha_n)$ er <u>algebraisk uafhængige</u> over R. I dette tilfælde har vi altså en isomorfi

$$R[X_1, \dots, X_n] \xrightarrow{\sim} R[\alpha_1, \dots, \alpha_n] \quad (\subseteq A).$$

Indsættes $(X_1, \dots, X_n)$ i et polynomium p, får vi åbenbart $p(X_1, \dots, X_n) = p$.

3.3. For et <u>monomium</u> $X_1^{i_1} \dots X_n^{i_n}$ defineres <u>graden</u>, betegnet $\deg(X_1^{i_1} \dots X_n^{i_n})$ ved $i_1 + \dots + i_n \in \mathbb{N}_0$. Idet vi for et multiindex $i = (i_1, \dots, i_n)$ sætter

$$|i| = i_1 + \dots + i_n,$$

har vi altså

$$\deg(X^i) = |i|.$$

For et polynomium $p = \sum p_i X^i \neq 0$ i $R[X_1, \dots, X_n]$ defineres <u>graden</u>, betegnet $\deg(p)$, som den største grad af de monomier X^i, der forekommer i p, altså

$$\deg(p) = \max\{|i| \mid p_i \neq 0\}.$$

3.4 Multiindices kan <u>adderes</u> (komponentvis addition), idet vi for multiindices $i = (i_1, \dots, i_n)$, $j = (j_1, \dots, j_n)$ sætter

$$i + j = (i_1 + j_1, \dots, i_n + j_n)$$

For produktet af monomier X^i og X^j i $R[X_1, \dots, X_n]$ har vi

$$X^i X^j = X^{i+j}$$

Bemærk, at $|i+j| = |i| + |j|$.

Videre kan disse multiindices <u>ordnes</u>, idet

vi for multiindices $i = (i_1, \cdots, i_n)$ og $j = (j_1, \cdots, j_n)$ skriver

$$i < j,$$

hvis

$$|i| < |j|$$

eller $|i| = |j|$ og der findes $\nu \in \{1, \cdots, n\}$, så at $i_1 = j_1, \cdots, i_{\nu-1} = j_{\nu-1}$, $i_\nu < j_\nu$.

Det er let at se, at mængden af multiindices $\mathbb{N}_0^n$ herved bliver totalt ordnet, og at der til et givet multiindex $j = (j_1, \cdots, j_n)$ kun findes endelig mange multiindices $< j$. Dette sikrer let, at $(\mathbb{N}_0^n, <)$ er velordnet, således at (visse) sætninger om multiindices kan vises ved induktion. (Det er for øvrigt let at se, at $(\mathbb{N}_0^n, <)$ er isomorf med $(\mathbb{N}, <)$.). Det mindste multiindex er $(0, \cdots, 0)$; vi har

$$(0,\cdots,0) < (0,\cdots,0,1) < (0,\cdots,1,0) < \cdots < (1,0,\cdots,0) < (0,\cdots,0,2) < (0,\cdots,1,1) < \cdots$$

Bemærk, at vi for multiindices i, j, k har

$$i < j \Rightarrow i + k < j + k.$$

3.5. For et polynomium $p = \sum p_i X^i \neq 0$ i $R[X_1, \cdots, X_n]$ defineres <u>signaturen</u>, betegnet $\operatorname{sgt}(p)$, som det største multiindex i, for hvilket X^i forekommer i p, altså

$$\operatorname{sgt}(p) = \max \{ i \in \mathbb{N}_0^n \mid p_i \neq 0 \}.$$

Har p altså signaturen k, så kan vi skrive

$$p = p_k X + \sum_{i<k} p_i X^i, \quad p_k \neq 0.$$

Koefficienten p_k vil vi kalde <u>højestekoefficienten</u>.

Det er klart, at

$$|\operatorname{sgt}(p)| = \deg(p).$$

3.6. Har vi givet polynomier p, q med signaturer k, ℓ, så kan vi skrive

$$p = p_k X^k + \dots \quad , \quad p_k \neq 0$$

$$q = q_\ell X^\ell + \dots \quad , \quad q_\ell \neq 0$$

(hvor ... de to steder står for en sum af led af mindre signatur).
For produktet finder vi

$$pq = p_k q_\ell X^{k+\ell} + \dots .$$

Det følger, at vi i almindelighed har

$$sgt(pq) \leqslant sgt(p) + sgt(q),$$

og at vi endda har

$$sgt(pq) = sgt(p) + sgt(q), \text{ hvis } p_k q_\ell \neq 0.$$

Det sidste er f.eks. opfyldt, hvis R er et integritetsområde (eller hvis $p_k = 1$ eller $q_\ell = 1$).

Tilsvarende finder vi for summen

$$sgt(p+q) \leqslant \max\{sgt(p), sgt(q)\}$$

samt

$$sgt(p+q) = \max\{sgt(p), sgt(q)\}, \text{ hvis } sgt(p) \neq sgt(q).$$

Har p og q derimod samme signatur k, og samme højeste koefficient, så er $sgt(p-q) < k$.

[I ovenstående uligheder tilføjes nulpolynomiet 0 en signatur, der er $<$ ethvert multiindex].

Vi får tilsvarende uligheder (og ligheder) for graden af polynomier.

3.7. Eksempel. Ordner vi i polynomiet

$$p = 3 + 5X_1X_3^2 + X_2 + 8X_3^3 - X_1X_2X_3 \in \mathbb{Z}[X_1, X_2, X_3]$$

leddene efter (aftagende) signatur, får det udseendet

$$p = -X_1X_2X_3 + 5X_1X_3^2 + 8X_3^3 + X_2 + 3.$$

Signaturen er $(1,1,1)$, højestekoefficienten er -1 og graden er $1+1+1=3$.

3.8. For $\nu = 1, \cdots, n$ defineres polynomierne $s_\nu \in R[X_1, \cdots, X_n]$ ved

$$s_1 = \sum_{1 \le i \le n} X_i = X_1 + X_2 + \cdots + X_n$$

$$s_2 = \sum_{1 \le i_1 < i_2 \le n} X_{i_1} X_{i_2} = X_1 X_2 + X_1 X_3 + \cdots \cdots + X_{n-1} X_n$$

$$\vdots$$

$$s_\nu = \sum_{1 \le i_1 < i_2 < \cdots < i_\nu \le n} X_{i_1} X_{i_2} \cdots X_{i_\nu} = X_1 X_2 \cdots X_\nu + \cdots + X_{n-\nu+1} \cdots X_{n-1} X_n$$

$$\vdots$$

$$s_n = \sum_{1 \le i_1 < i_2 < \cdots < i_n \le n} X_{i_1} \cdots X_{i_n} = X_1 X_2 \cdots X_n$$

For et monomium $X_{i_1} \cdots X_{i_\nu}$, med $i_1 < \cdots < i_\nu$, har vi

$$\operatorname{sgt}(X_{i_1} \cdots X_{i_\nu}) = (0, \cdots, \underset{\uparrow}{1}, \cdots \underset{\uparrow}{0}, \underset{\uparrow}{1}, \cdots, 1, \cdots, 0)$$
$$i_1 \qquad i_2 \qquad i_\nu$$

så vi finder $\operatorname{sgt}(s_\nu) = (\underbrace{1, \cdots, 1}_{\nu \text{ et-taller}}, 0, \cdots, 0)$

For et potensprodukt $s_1^{l_1} \cdots s_n^{l_n}$ finder vi derfor

$$\operatorname{sgt}(s_1^{l_1} \cdots s_n^{l_n}) = (l_1 + \cdots + l_n, l_2 + \cdots + l_n, \cdots, l_{n-1} + l_n, l_n),$$

og højestekoefficienten er 1.

Polynomierne $s_1, \cdots, s_n$ kaldes de <u>elementarsymmetriske</u> polynomier (i n variable). Ofte betragtes også polynomierne

$$a_\nu = (-1)^\nu s_\nu = s_\nu(-X_1, \cdots, -X_n).$$

3.9. For polynomiet

$$\Delta = \prod_{i_1 < i_2} (X_{i_1} - X_{i_2})$$

finder vi signaturen

$$sgt(\Delta) = (n-1, n-2, \ldots, 1, 0)$$

og graden $\deg(\Delta) = \binom{n}{2}$.

3.10. Lad der være givet en permutation $\sigma \in \mathcal{S}_n$. For et givet polynomium $p \in R[X_1, \ldots, X_n]$,

$$p = \sum p_{i_1, \ldots, i_n} X_1^{i_1} \ldots X_n^{i_n}$$

definerer polynomiet $\sigma(p) \in R[X_1, \ldots, X_n]$ ved

$$\sigma(p) = \sum p_{i_1, \ldots, i_n} X_{\sigma(1)}^{i_1} \ldots X_{\sigma(n)}^{i_n}.$$

Vi finder let for polynomier p, q, at

$$(A) \begin{cases} \sigma(p+q) = \sigma(p) + \sigma(q) \\ \sigma(pq) = \sigma(p)\sigma(q), \end{cases}$$

samt for permutationer σ, τ, at

$$(B) \quad \sigma(\tau(p)) = (\sigma\tau)(p)$$

DEFINITION. Et polynomium $p \in R[X_1, \ldots, X_n]$ kaldes <u>symmetrisk</u>, hvis $\sigma(p) = p$ for alle permutationer $\sigma \in \mathcal{S}_n$.

3.11. Polynomiet $X_1^4X_2^2 + X_1^4X_3^2 + X_1^2X_2^4 + X_1^2X_3^4 + X_2^4X_3^2 + X_2^2X_3^4$ er symmetrisk ($n=3$). De elementarsymmetriske polynomier $s_1, \ldots, s_n$ (jfr. 3.8) er symmetriske polynomier.

For polynomiet $\Delta = \prod_{i_1 < i_2} (X_{i_1} - X_{i_2})$ finder vi

$$\sigma(\Delta) = (\operatorname{sign}\sigma)\,\Delta .$$

[vi finder faktisk $\sigma(\Delta) = (-1)^{I(\sigma)}\Delta$, hvor $I(\sigma)$ er antallet af inversioner i permutationen σ = antallet af par (i_1, i_2), hvor $i_1 < i_2$ og $\sigma(i_1) > \sigma(i_2)$. Definerer fortegnet $\operatorname{sign}\sigma$ ved $\operatorname{sign}\sigma = (-1)^{I(\sigma)}$, følger det let af ligningen 3.10 (B), at vi har $\operatorname{sign}(\sigma\tau) = (\operatorname{sign}\sigma)(\operatorname{sign}\tau)$].

Vi slutter, at kvadratet $D = \Delta^2$ er et symmetrisk polynomium. Polynomiet

$$D = \Delta^2 = \prod_{i_1 < i_2} (X_{i_1} - X_{i_2})^2 = (-1)^{\binom{n}{2}} \prod_{i_1 \neq i_2} (X_{i_1} - X_{i_2})$$

kaldes <u>diskriminanten</u>.

3.12 HOVEDSÆTNING OM SYMMETRISKE POLYNOMIER.

<u>Til hvert symmetrisk polynomium $p \in R[X_1, \dots, X_n]$ findes netop et polynomium $q \in R[X_1, \dots, X_n]$, således at vi ved indsættelse af de elementarsymmetriske polynomier $s_1, \dots, s_n$ i q får polynomiet p:</u>

$$\underline{p = q(s_1, \dots, s_n).}$$

Bevis. Vi bemærker først, at der for signaturen $\operatorname{sgt}(p) = k = (k_1, \dots, k_m)$ af et symmetrisk polynomium

$$p = \sum p_i X^i = p_k X^k + \cdots$$

gælder

$$k_1 \geqslant k_2 \geqslant \cdots \geqslant k_n .$$

Fandtes nemlig et $\nu < n$, således at $k_\nu < k_{\nu+1}$, så kunne vi sætte $l = (k_1, k_2, \dots, k_{\nu+1}, k_\nu, \dots, k_{n-1}, k_n)$ og betragte transpositionen $\tau = (\nu, \nu+1)$. Vi ser, at X^l ville forekomme i polynomiet $\tau(p)$, således at vi ville have $\operatorname{sgt}(\tau(p)) \geqslant l$. Da $l > k = \operatorname{sgt}(p)$ er dette i modstrid med at $\tau(p) = p$.

Vi viser nu for et symmetrisk polynomium p eksistensen af det søgte polynomium q ved fuldstændig induktion efter signaturen af p: Er $p = 0$ kan vi bruge $q = 0$. Har $p \neq 0$ signaturen $k = (k_1, \cdots, k_n)$, og antager vi, at eksistensen er vist for alle symmetriske polynomier af signatur $< k$, så kan vi skrive

$$p = p_k X^k + \cdots \quad , \quad p_k \neq 0.$$

I følge bemærkningen har vi $k_1 \geqslant k_2 \geqslant \cdots \geqslant k_n$, og vi kan derfor skrive

$$(k_1, k_2, \cdots, k_n) = (l_1 + \cdots + l_n, l_2 + \cdots + l_n, \cdots, l_n)$$

med tal $l_\nu \geqslant 0$. Udregningen i 3.8. viser nu, at polynomiet $p_k s_1^{l_1} \cdots s_n^{l_n}$ har signatur $k = (k_1, \cdots, k_n)$ og samme højeste koefficient som p (nemlig p_k), så differensen $p - p_k s_1^{l_1} \cdots s_n^{l_n}$ har signatur $< k$. Da denne differens øjensynlig er et symmetrisk polynomium, findes et polynomium $\tilde{q}$, så at

$$p - p_k s_1^{l_1} \cdots s_n^{l_n} = \tilde{q}(s_1, \cdots, s_n),$$

men så er

$$p = q(s_1, \cdots, s_n), \text{ med } q = p_k X_1^{l_1} \cdots X_n^{l_n} + \tilde{q}(X_1, \cdots, X_n).$$

For at vise entydigheden er det nok at vise, at vi for et polynomium $q \neq 0$ har

$$q(s_1, \cdots, s_n) \neq 0.$$

Et sådant polynomium er imidlertid sum af sine led

$$q_i X^i = q_i X_1^{i_1} \cdots X_n^{i_n} \qquad q_i \neq 0$$

som har indbyrdes forskellig signatur. Ved indsættelse af $s_1, \cdots, s_n$ ser vi, at $q(s_1, \cdots, s_n)$ er sum af de tilsvarende polynomier

$$q_i s_1^{i_1} \cdots s_n^{i_n},$$

og udregningen i 3.8. viser, at disse polynomier

også har indbyrdes forskellig signatur. Deres sum må derfor være $\neq 0$ ▨

3.13. Bemærk, at entydighedsudsagnet i hovedsætningen udsiger, at polynomierne $s_1, \cdots, s_n \in R[X_1, \cdots, X_n]$ er algebraisk uafhængige, og at eksistensudsagnet udsiger, at delringen

$$R[s_1, \cdots, s_n] \subseteq R[X_1, \cdots, X_n]$$

netop består af de symmetriske polynomier.

3.14. For $n = 2$ er polynomierne $X_1^2 + X_2^2$, $X_1^3 + X_2^3$, $D = \Delta^2 = (X_1 - X_2)^2 = X_1^2 + X_2^2 - 2X_1X_2$ symmetriske. Man finder let

$$\begin{aligned} X_1^2 + X_2^2 &= s_1^2 - 2s_2 \\ X_1^3 + X_2^3 &= s_1^3 - 3s_1s_2 \\ D &= s_1^2 - 4s_2. \end{aligned}$$

For $n = 3$ er polynomierne $X_1^4X_2^2 + X_1^4X_3^2 + X_1^2X_2^4 + X_1^2X_3^4 + X_2^4X_3^2 + X_2^2X_3^4$, $D = \Delta^2 = (X_1 - X_2)^2(X_1 - X_3)^2(X_2 - X_3)^2$ symmetriske. Det er noget omstændeligt at finde

$$X_1^4X_2^2 + X_1^4X_3^2 + X_1^2X_2^4 + X_1^2X_3^4 + X_2^4X_3^2 + X_2^2X_3^4 = -2s_1^3s_3 + s_1^2s_2^2 + 4s_1s_2s_3 - 2s_2^3 - 3s_3^2$$

og

$$D = -4s_1^3s_3 + s_1^2s_2^2 + 18s_1s_2s_3 - 4s_2^3 - 27s_3^2$$

Vi bemærker, at da $a_\nu = (-1)^\nu s_\nu$, $\nu = 1, \cdots, n$, kan vi på oplagt måde udtrykke et hvert symmetrisk polynomium $p \in R[X_1, \cdots, X_n]$ som et polynomium i $a_1, \cdots, a_n$.

3.15 Hovedsætningen anvendes ofte i følgende situation: Der er givet en kommutativ R-algebra A, og et normeret n-te grads polynomium (i én variabel)

$$(1)\quad f = X^n + \tilde{a}_1 X^{n-1} + \cdots + \tilde{a}_{n-1} X + \tilde{a}_n \in A[X],$$

som har en fremstilling

$$(2)\quad f = (X-\alpha_1)\cdots(X-\alpha_n),$$

hvor $\alpha_1, \ldots, \alpha_n \in A$. Udregnes produktet i (2) og sammenlignes med koefficienterne i (1), ser vi, at

$$\tilde{a}_\nu = (-1)^\nu \sum_{1 \le i_1 < \cdots < i_\nu \le n} \alpha_{i_1} \cdots \alpha_{i_\nu}.$$

Vi har altså

$$\tilde{a}_\nu = a_\nu(\alpha_1, \ldots, \alpha_n), \quad \nu = 1, \ldots, n,$$

hvor $a_\nu \in R[X_1, \ldots, X_n]$ er de elementarsymmetriske polynomier.

Er $p \in R[X_1, \ldots, X_n]$ et polynomium, så kan vi indsætte $\alpha_1, \ldots, \alpha_n$ i p, og får elementet $p(\alpha_1, \ldots, \alpha_n) \in A$. Hvis p er symmetrisk, ser vi, at $p(\alpha_1, \ldots, \alpha_n)$ ikke afhænger af rækkefølgen af faktorerne i (2).

Ifølge hovedsætningen kan det symmetriske polynomium p skrives

$$p = q(a_1, \ldots, a_n)$$

med et passende polynomium q. Ved indsættelse får vi derfor

$$p(\alpha_1, \ldots, \alpha_n) = q(a_1(\alpha_1, \ldots, \alpha_n), \ldots, a_n(\alpha_1, \ldots, \alpha_n))$$

altså

$$p(\alpha_1, \ldots, \alpha_n) = q(\tilde{a}_1, \ldots, \tilde{a}_n)$$

For et symmetrisk polynomium $p \in R[X_1, \ldots, X_n]$, kan $p(\alpha_1, \ldots, \alpha_n)$ altså udtrykkes som et polynomium i koefficienterne $\tilde{a}_1, \ldots, \tilde{a}_n$. Specielt ser vi, at

$$p(\alpha_1, \ldots, \alpha_n) \in R[\tilde{a}_1, \ldots, \tilde{a}_n]$$

3.16. Eksempel. Polynomiet $f = X^3 + 2X + 5 \in \mathbb{Z}[X]$ har i $\mathbb{C}$ tre rødder $\alpha_1, \alpha_2, \alpha_3$ og altså en fremstilling

$$f = (X-\alpha_1)(X-\alpha_2)(X-\alpha_3).$$

Uden at kende disse rødder finder vi (jfr. 3.14)

$$\alpha_1^4\alpha_2^2 + \alpha_1^4\alpha_3^2 + \alpha_1^2\alpha_2^4 + \alpha_1^2\alpha_3^4 + \alpha_2^4\alpha_3^2 + \alpha_2^2\alpha_3^4 = -2\cdot 2^3 - 3(-5)^2$$
$$= -91$$

$$(\alpha_1-\alpha_2)^2(\alpha_1-\alpha_3)^2(\alpha_2-\alpha_3)^2 = -4\cdot 2^3 - 27(-5)^2 = -707.$$

4. Algebraens fundamentalsætning.

4.1. ALGEBRAENS FUNDAMENTALSÆTNING. Ethvert polynomium

$$f = X^n + a_1 X^{n-1} + \cdots + a_{n-1} X + a_n \in \mathbb{C}[X],$$

af grad $n \geq 1$, har en rod i $\mathbb{C}$.

Beviset er i en række skridt:

① Sætningen er rigtig for $n = 2$. Skriver vi

$$f = X^2 + a_1 X + a_2 = \left(X + \tfrac{1}{2}a_1\right)^2 - \frac{a_1^2 - 4a_2}{4} = \left(X + \tfrac{1}{2}a_1\right)^2 - \frac{D}{4}$$

ser vi, at det er nok at vise, at hvert komplekst tal har en kvadratrod, altså at der til hvert tal $a \in \mathbb{C}$ findes et element $\alpha \in \mathbb{C}$, så at $a = \alpha^2$. Hertil bemærker vi, at hvert reelt tal ≥ 0 som bekendt har en reel kvadratrod, der er ≥ 0. Skriver vi

$$a = a' + i\,a'', \quad a', a'' \in \mathbb{R}$$

ser vi nu lit ved udregning, at af tallene

$$\sqrt{\frac{\sqrt{a'^2 + a''^2} + a'}{2}} \quad \pm i\sqrt{\frac{\sqrt{a'^2 + a''^2} - a'}{2}}$$

kan et bruges som α.

② Det er nok at vise, at hvert polynomium med reelle koefficienter af grad ≥ 1 har en rod i $\mathbb{C}$.

Er nemlig dette vist, og er

$$f = X^n + a_1 X^{n-1} + \cdots + a_n \in \mathbb{C}[X], \quad n \geq 1$$

et vilkårligt polynomium, så kan vi betragte det konjugerede polynomium

$$\bar{f} = X^n + \bar{a}_1 X^{n-1} + \cdots + \bar{a}_n.$$

Produktet $f\bar{f}$ har da reelle koefficienter og grad ≥ 2, og det har derfor en rod $\alpha \in \mathbb{C}$. Vi har nu $f(\alpha)\bar{f}(\alpha) = 0$, og altså $f(\alpha) = 0$ eller $\bar{f}(\alpha) = 0$. Hvis $f(\alpha) = 0$, så er α rod i f, og hvis $\bar{f}(\alpha) = 0$,

så er også $f(\bar{\alpha}) = \overline{f(\alpha)} = 0$, og altså $\bar{\alpha}$ rod i f.

③ Et tal $n \geq 1$ kan entydigt skrives

$$n = 2^k u, \quad k \geq 0, \quad u \text{ ulige}.$$

Vi viser nu udsagnet i ② for polynomier af grad $n = 2^k u$, $k \geq 0$, u ulige, ved <u>induktion efter k</u>.

For $k = 0$ er påstanden, at ethvert reelt polynomium af ulige grad har en rod i $\mathbb{C}$. Dette følger af et velkendt sammenhængsargument: Et sådant polynomium definerer en kontinuert funktion

$$f : \mathbb{R} \to \mathbb{R},$$

og billedmængden $f(\mathbb{R})$ er derfor et interval. Da graden er ulige, ser vi, at dette interval hverken kan være opad eller nedad begrænset, så vi må have $f(\mathbb{R}) = \mathbb{R}$. Specielt er altså

$$0 \in f(\mathbb{R}),$$

så f har endda en rod i $\mathbb{R}$.

④ Induktionsskridtet: Vi betragter et polynomium

$$f = X^n + a_1 X^{n-1} + \cdots + a_n$$

med reelle koefficienter $a_1, \ldots, a_n$ af grad $n = 2^k u$, $k > 0$, u ulige, og antager, at påstanden i ② er vist for alle polynomier af grad $2^{k-1} u'$, u' ulige.

Betragter vi f som et polynomium i $\mathbb{C}[X]$ følger det af sætning 2.23, at vi kan finde en udvidelse $\mathbb{C} \subset K$ og elementer $\alpha_1, \ldots, \alpha_n \in K$, så at vi i $K[X]$ har en fremstilling

$$f = (X - \alpha_1) \cdots (X - \alpha_n).$$

Vi har nu

$$\mathbb{R} \subseteq \mathbb{C} \subseteq K,$$

og vi ønsker at vise, at et af α_i'erne tilhører $\mathbb{C}$.

For et tal $t \in \mathbb{R}$ betragter vi nu polynomiet

$$g_t = \prod_{1 \le i < j \le n} \left(X - (\alpha_i + \alpha_j + t\alpha_i\alpha_j)\right)$$

Dette er et polynomium i $K[X]$, det har grad $\binom{n}{2}$ og i K rødderne $\alpha_i + \alpha_j + t\alpha_i\alpha_j$, $i < j$. Ved udregning af produktet, ser vi, at hver koefficient i g_t kan udtrykkes som et symmetrisk polynomium i $\alpha_1, \dots, \alpha_n$ med koefficienter (der afhænger af t) i $\mathbb{R}$. I følge hovedsætningen om symmetriske polynomier kan vi derfor slutte, at g_t's koefficienter tilhører $\mathbb{R}[a_1, \dots, a_n] = \mathbb{R}$. Da endvidere g_t's grad $\binom{n}{2} = \frac{n}{2}(n-1) = 2^{k-1}u(2^k u - 1)$ er af formen $2^{k-1}u'$, u' ulige, kan vi af induktionsforudsætningen slutte, at g_t har en rod i $\mathbb{C}$. Denne rod må være af formen $\alpha_i + \alpha_j + t\alpha_i\alpha_j$, så til det givne $t \in \mathbb{R}$ findes altså (i,j) med $1 \le i < j \le n$, således at

$$\alpha_i + \alpha_j + t\alpha_i\alpha_j \in \mathbb{C}.$$

For hvert $t \in \mathbb{R}$ findes altså et par (i,j), $1 \le i < j \le n$ således at $\alpha_i + \alpha_j + t\alpha_i\alpha_j \in \mathbb{C}$. Der er uendelig mange t'er, men kun endelig mange par (i,j). Det følger, at der må findes elementer $s \neq t$ i $\mathbb{R}$ og et par (i,j) så at

$$\alpha_i + \alpha_j + t\alpha_i\alpha_j \in \mathbb{C}$$
$$\alpha_i + \alpha_j + s\alpha_i\alpha_j \in \mathbb{C}.$$

Ved "subtraktion" slutter vi, at $(t-s)\alpha_i\alpha_j \in \mathbb{C}$, og dermed, at $\alpha_i\alpha_j = (t-s)^{-1}(t-s)\alpha_i\alpha_j \in \mathbb{C}$, og heraf følger videre, at også $\alpha_i + \alpha_j \in \mathbb{C}$. Polynomiet

$$(X - \alpha_i)(X - \alpha_j) = X^2 - (\alpha_i + \alpha_j)X + \alpha_i\alpha_j$$

har således koefficienter i $\mathbb{C}$, det har grad 2 og det har rødderne α_i og α_j i K. Af ① følger, at dette polynomium har en rod i $\mathbb{C}$. Vi har derfor $\alpha_i \in \mathbb{C}$ eller $\alpha_j \in \mathbb{C}$. ▨

4.2. Algebraens fundamentalsætning medfører, at de irreducible polynomier i $\mathbb{C}[X]$ er 1ste grads polynomierne. De normerede irreducible polynomier i $\mathbb{C}[X]$ er altså polynomierne af formen

$$X - a, \quad a \in \mathbb{C}.$$

Algebraens fundamentalsætning medfører videre, at de normerede irreducible polynomier i $\mathbb{R}[X]$ er polynomierne af formen

(1) $X - a$, $a \in \mathbb{R}$

(2) $(X-a)^2 + b^2$, $a, b \in \mathbb{R}$, $b \neq 0$.

Er nemlig p et sådant polynomium, så har p en rod $\alpha = a + ib$ i $\mathbb{C}$, og vi har $p = f_{\alpha/\mathbb{R}}$, jfr. 2.19. Det minimale polynomium for $\alpha = a+ib$ er øjensynlig $X-a$, hvis $b=0$, og $(X-a)^2+b^2$, hvis $b \neq 0$.

5. Endelige, reelle divisionsalgebraer.

5.1. DEFINITION. En algebra A over legemet L kaldes en <u>divisionsalgebra</u> (resp. <u>integritetsalgebra</u>), hvis ringen A er et skevlegeme (resp. integritetsområde).

5.2. SÆTNING. <u>Enhver endelig integritetsalgebra A er en divisionsalgebra.</u>

Bevis. For et givet $\alpha \neq 0$ i A betragtes afbildningen $r_\alpha : A \to A$ givet ved

$$r_\alpha : \xi \longmapsto \xi\alpha.$$

Denne afbildning er lineær, altså en endomorfi i det endeligdimensionale vektorrum A. Da nulreglen gælder i A, ser vi, at den er injektiv. Vi slutter, at den er bijektiv. Specielt findes et element $\alpha' \in A$, så at $\alpha'\alpha = 1$. Her er nødvendigvis $\alpha' \neq 0$, så tilsvarende findes $\alpha'' \in A$, så at $\alpha''\alpha' = 1$. Men så er $\alpha'' = \alpha''(\alpha'\alpha) = (\alpha''\alpha)\alpha = \alpha$, og vi har $\alpha'\alpha = 1$ og $\alpha\alpha' = 1$. Elementet α er altså invertibelt ▨

5.3. KOROLLAR. <u>Enhver delalgebra B af en endelig divisionsalgebra A er selv en endelig divisionsalgebra.</u>

Bevis. Delalgebraen B er specielt et underrum i A, og dermed endeligdimensional. Da nulreglen gælder i delmængden, følger påstanden af sætning 5.2 ▨

5.4. Vi kan opfatte legemet L som en 1-dimensio-

nal divisionsalgebra. For enhver endelig udvidelse $L \subset K$ er K en kommutativ endelig divisionsalgebra.
Over $\mathbb{R}$ er $\mathbb{R}$, $\mathbb{C}$ og $\mathbb{H}$ endelige divisionsalgebraer. Som vi om lidt skal se findes der ikke andre.

5.5. Er A en L-algebra $\neq 0$, så er homomorfien $L \to A$ injektiv. Vi vil sædvanligvis identificere elementerne i L med deres billeder i A, altså opfatte L som en delring $L \subseteq A$. Vi har endda

$$L \subseteq \mathrm{Cent}(A).$$

Hvis A er en endelig divisionsalgebra, så er hvert element $\alpha \in A$ algebraisk over L (Korollar 1.4), og delalgebraen $L[\alpha]$ er selv en endelig divisionsalgebra. Vi har således en endelig udvidelse $L \subset L[\alpha]$ af legemer, og det minimale polynomium $f_{\alpha/L} \in L[X]$ er et irreducibelt polynomium. Vi bemærker her, at det irreducible polynomium $f_{\alpha/L}$ har grad 1, hvis og kun hvis $\alpha \in L$.

SÆTNING. Hvis legemet L er algebraisk afsluttet, så findes netop én endelig divisionsalgebra over L, nemlig L selv.

Bevis. Lad A være en sådan algebra. For et element $\alpha \in A$ er det minimale polynomium $f_{\alpha/L} \in L[X]$ irreducibelt. Da L er algebraisk afsluttet, må $f_{\alpha/L}$ være et 1ste gradspolynomium (jfr. 2.16), så vi har $\alpha \in L$ ▨

5.6. Sætning 5.5. kan anvendes på legemet $\mathbb{C}$ ifølge algebraens fundamentalsætning. For $L = \mathbb{R}$ gælder nu

FROBENIUS' SÆTNING. Over legemet $\mathbb{R}$ findes på isomorfi nær kun tre endelige divisionsalgebraer, nemlig $\mathbb{R}$, $\mathbb{C}$ og $\mathbb{H}$.

Bevis. Lad A være en sådan algebra. Vi kan antage, at $\mathbb{R} \subset A$. For et element $\alpha \in A \setminus \mathbb{R}$ er (jfr. 4.2) det minimale polynomium $f_{\alpha/\mathbb{R}}$ af formen

$$(*) \quad (X-a)^2 + b^2, \quad a, b \in \mathbb{R}, \ b \neq 0,$$

og delalgebraen $\mathbb{R}[\alpha]$ er isomorf med $\mathbb{C}$.
Da $\mathbb{R} \subset A$ findes der sådanne elementer α, og der findes følgelig i A en delalgebra $B \simeq \mathbb{C}$. I B findes et element I, så at

$$\boxed{I^2 = -1}$$

og vi har $B = \mathbb{R}[I]$.

Vi betragter nu afbildningen $p: A \to A$ givet ved

$$p: \xi \longmapsto I\xi I^{-1}!$$

Vi ser lit, at

1) p er $\mathbb{R}$-lineær
2) p er involutorisk (d: $p^2 = Id_A$)
3) p er multiplikativ.

Af 1) og 2) følger som bekendt, at vi har en direkte sum opspaltning

$$A = A_1 \oplus A_{-1}$$

i egenrummene

$$A_1 = \{\xi \in A \mid I\xi I^{-1} = \xi\}$$

$$A_{-1} = \{\xi \in A \mid I\xi I^{-1} = -\xi\}.$$

Af 3) følger, at A_1 er en delring, og det er klart, at $B \subseteq A_1$. For $\xi \in A_1$ har vi $I\xi = \xi I$, så ξ kommuterer med I. Heraf følger lit, at ξ kommuterer med alle elementer af formen $a + bI$,

altså med alle elementer i B. Dette betyder, at $B \subseteq \mathrm{Cent}(A_1)$, så vi kan betragte A_1 som en algebra over B. Det er klart en endelig divisionsalgebra, og da $B \simeq \mathbb{C}$ er algebraisk afsluttet, må vi have $B = A_1$ (sætning 5.5).
Hvis $A_1 = (0)$, har vi altså $A = A_1 = B \simeq \mathbb{C}$.
Er derimod $A_{-1} \neq (0)$, kan vi betragte et element $J \neq 0$ i A_{-1}. At $J \in A_{-1}$ betyder, at $IJI^{-1} = -J$, altså at

$$\boxed{IJ = -JI}$$

Det er klart, at $J \notin \mathbb{R}$, så dit minimale polynomium for J er af formen (*). Der findes altså en ligning

$$J^2 + a^2 + b^2 = 2aJ, \quad a, b \in \mathbb{R}, \quad b \neq 0.$$

Da $J \in A_{-1}$, slutter vi let af 3), at $J^2 \in A_1$. Da også $a^2 + b^2 \in \mathbb{R} \subseteq A_1$ har vi $J^2 + a^2 + b^2 \in A_1$. Nu er $2aJ \in A_{-1}$, og da $A_1 \cap A_{-1} = (0)$, må begge sider i ligningen være 0. Vi får først $a = 0$, og dernæst $J^2 = -b^2$. I stedet for at erstatte J med $b^{-1}J$, kan vi antage, at

$$\boxed{J^2 = -1}$$

Af 3) følger nu let, at der ved $\alpha \mapsto \alpha J$ defineres en afbildning $: A_1 \to A_{-1}$. Den er øjensynlig $\mathbb{R}$-lineær, og den er en isomorfi, idet afbildningen $\beta \mapsto \beta J^{-1} = -\beta J$ ses at være dens inverse. Vi slutter, at basen $1, I$ for A_1 afbildes på en basis for A_{-1}, altså at J, IJ er en basis for A_{-1}. Sættes altså

$$\boxed{IJ = K,}$$

ser vi, at $1, I, J, K$ er en $\mathbb{R}$-basis for A.

De øvrige ligninger for multiplikation med kvaternionenheden følger let af de indrammede. ▨

KATEGORIER

1. Kategoribegrebet.

1.1. BESKRIVELSE. I en kategori $\mathcal{C}$ indgår følgende tre bestanddele:

i) Objekterne i $\mathcal{C}$. At A er objekt i $\mathcal{C}$ skrives ofte $A \in \mathcal{C}$. I en given kategori $\mathcal{C}$ ligger en afgrænsning af hvilke objekter den beskæftiger sig med. Vi vil ikke nærmere komme ind på hvad der forstås ved en sådan afgrænsning, men det fremhæves, at vi ikke forudsætter, at kategoriens objekter udgør en mængde.

ii) Morfierne i $\mathcal{C}$. Til hvert par A, B af objekter i $\mathcal{C}$ er der knyttet en mængde, $\mathrm{Hom}_{\mathcal{C}}(A,B)$, hvis elementer kaldes morfier (eller homomorfier eller pile) fra A til B. At $f \in \mathrm{Hom}_{\mathcal{C}}(A,B)$ skrives ofte $f: A \to B$ eller $A \xrightarrow{f} B$. Det er ofte bekvemt at antage, at mængderne $\mathrm{Hom}_{\mathcal{C}}(A,B)$ og $\mathrm{Hom}_{\mathcal{C}}(A',B')$, svarende til to forskellige par (A,B) og (A',B') af objekter i $\mathcal{C}$, er disjunkte.

iii) Sammensætningen i $\mathcal{C}$. Til hvert tripel A, B, C af objekter i $\mathcal{C}$ er der knyttet en afbildning:

$$\mathrm{Hom}_{\mathcal{C}}(A,B) \times \mathrm{Hom}_{\mathcal{C}}(B,C) \longrightarrow \mathrm{Hom}_{\mathcal{C}}(A,C)$$

kaldet sammensætning og betegnet

$$(f,g) \longmapsto g \circ_{\mathcal{C}} f.$$

Sammensætningen knytter altså til en morfi $f: A \to B$ og en morfi $g: B \to C$ en morfi $g \circ_{\mathcal{C}} f: A \to C$. Hvis misforståelser er udelukket, skrives

$$g \circ_{\mathcal{C}} f = gf.$$

Det forudsættes, at følgende axiomer er opfyldt:

Axiom I (associativitet): For morfier

$$A \xrightarrow{f} B, \quad B \xrightarrow{g} C, \quad C \xrightarrow{h} D$$

gælder $h(gf) = (hg)f$.

Axiom II (identiteter): Til hvert objekt A findes en morfi $1_A : A \to A$, således at vi for alle morfier

$$X \xrightarrow{f} A \quad \text{har} \quad 1_A f = f$$

og alle morfier

$$A \xrightarrow{g} Y \quad \text{har} \quad g 1_A = g.$$

Det er let at se, at en morfi i $\mathrm{Hom}_{\mathcal{C}}(A,A)$ med den i axiom II nævnte egenskab er entydigt bestemt. Morfien 1_A kaldes identiteten på A.

1.2. DEFINITION. En morfi $A \xrightarrow{f} B$ i kategorien $\mathcal{C}$ kaldes en isomorfi, hvis der findes en morfi $B \xrightarrow{g} A$, således at

$$gf = 1_A \text{ og } fg = 1_B.$$

En sådan morfi g er da entydigt bestemt, thi er $g' : B \to A$ endnu en morfi, som opfylder $g'f = 1_A$ og $fg' = 1_B$, så finder vi $g' = 1_A g' = (gf)g' = g(fg') = g 1_B = g$.
Morfien g kaldes den inverse til f, og den betegnes f^{-1}.

1.3. DEFINITION. En morfi $A \xrightarrow{f} A$ i kategorien $\mathcal{C}$ fra et objekt A til sig selv kaldes også en endomorfi i A. Vi sætter

$$\mathrm{End}_{\mathcal{C}}(A) = \mathrm{Hom}_{\mathcal{C}}(A,A).$$

En endomorfi $A \xrightarrow{f} A$, der er en isomorfi, kaldes en automorfi i A. Mængden af automorfier i A betegnes $\mathrm{Aut}_{\mathcal{C}}(A)$. Sammensætningen i $\mathcal{C}$ giver for hvert objekt A en afbildning

$$\mathrm{End}_{\mathcal{C}}(A) \times \mathrm{End}_{\mathcal{C}}(A) \to \mathrm{End}_{\mathcal{C}}(A),$$

altså en komposition i $\mathrm{End}_{\mathcal{C}}(A)$, og axiomerne I og II

medfører specielt, at denne komposition er associativ med neutralt element. $End_{\mathcal{C}}(A)$ er altså et monoid (= semigruppe med neutralt element), og det ses, at $Aut_{\mathcal{C}}(A)$ netop er gruppen af invertible elementer heri.

1.4. Eksempel. I kategorien (Sets) er objekterne vilkårlige mængder, morfierne er vilkårlige afbildninger, og sammensætningen er sædvanlig sammensætning. Bemærk, at den tomme mængde $\emptyset$ er et objekt i (Sets). Hvad er $Hom_{Sets}(\emptyset, Y)$ og $Hom_{Sets}(X, \emptyset)$?

1.5. Eksempel. I kategorien (Gr) er objekterne grupper, morfierne er homomorfier af grupper, og sammensætningen er den sædvanlige.

1.6. Beskriv tilsvarende kategorierne

(Ab) af kommutative grupper

(L-vect) af vektorrum over et givet legeme L

(Rings) af ringe

(R-alg) af algebraer over en given kommutativ ring R.

1.7. I kategorien (Top) er objekterne topologiske rum

og morfierne er kontinuerte afbildninger. For mange formål er det tilstrækkeligt at betragte kategorien (Metr, cont) af metriske rum med kontinuerte afbildninger som morfier. Også kategorien $(Metr, dist_{\leqslant})$ af metriske rum, med (svagt) afstandsformindskende afbildninger som morfier, har interesse.

1.8. I kategorien (Trip) er objekterne tripler (Q, q_1, φ) bestående af en mængde Q, et udvalgt element $q_1 \in Q$, og en afbildning $\varphi: Q \to Q$. Morfierne defineres på oplagt måde.

1.9. Eksempel. I kategorien (Top_0) er objekterne par (X, x_0) bestående af et topologisk rum X samt et udvalgt element $x_0 \in X$. Oplagte morfier. Tilsvarende kategorien $(Metr_0, cont)$.

1.10. Er M et givet monoid, kan vi definere en kategori $\mathcal{C} = Cat(M)$, således at $\mathcal{C}$ har ét objekt $*$, og således at $End_{\mathcal{C}}(*) = M$.

1.11. Er $T, \leqslant$ en mængde med en refleksiv, transitiv relation $\leqslant$, kan vi definere en kategori $\mathcal{C} = Cat(T)$, således at objekterne i $\mathcal{C}$ er elementerne i T, og således at

$$Hom_{\mathcal{C}}(s,t) \begin{cases} \text{har ét element, hvis } s \leqslant t. \\ \text{er tom ellers.} \end{cases}$$

Hvis relationen er $=$, får vi en <u>diskret kategori</u>, d.v.s. en kategori, hvori de eneste morfier er identiteterne.

1.12. I visse forbindelser er det hensigtsmæssigt at betragte kategorier, hvis objekter er visse afbildninger (eller, mere generelt; visse morfier i andre kategorier).

F.eks. kan vi for en given kategori $\mathcal{C}$ betragte kategorien $\mathcal{C}^{\bullet\to\bullet}$, hvori <u>objekterne</u> er morfier $A \xrightarrow{f} B$ i $\mathcal{C}$, hvori <u>morfierne</u> fra et objekt $A \xrightarrow{f} B$ til et objekt $A' \xrightarrow{f'} B'$ er par (α, β) bestående af morfier $\alpha : A \to A'$, $\beta : B \to B'$, således at vi har $f'\alpha = \beta f$.

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & A' \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f'} \\ B & \xrightarrow{\beta} & B', \end{array}$$

og hvori <u>sammensætning</u> defineres på oplagt måde.

Er H en kommutativ semigruppe, og $S \subseteq H$ en ikke tom stabil delmængde, kan vi betragte kategorien $\mathcal{M}_{H,S}$, hvori <u>objekterne</u> er afbildninger $H \xrightarrow{\varphi} M$, hvor M er et monoid og $\varphi : H \to M$ er en homomorfi, således at elementerne $\varphi(s)$, $s \in S$, er invertible i M, hvori <u>morfierne</u> fra et objekt $H \xrightarrow{\varphi} M$ til et objekt $H \xrightarrow{\varphi'} M'$ er en homomorfi $f : M \to M'$ således at $f \circ \varphi = \varphi'$

$$\begin{array}{ccc} & H & \\ {\scriptstyle\varphi}\swarrow & & \searrow{\scriptstyle\varphi'} \\ M & \xrightarrow[f]{} & M' \end{array}$$

og hvori <u>sammensætning</u> defineres på oplagt måde.

1.13. Er $\mathcal{C}$ en given kategori, kan vi definere en ny kategori $\mathcal{C}^{op}$, kaldet den modsatte kategori, på følgende måde: i) Objekterne i $\mathcal{C}^{op}$ er de samme som objekterne i $\mathcal{C}$. ii) Morfierne i $\mathcal{C}^{op}$ fra A til B defineres ved

$$Hom_{\mathcal{C}^{op}}(A,B) = Hom_{\mathcal{C}}(B,A)$$

iii) Sammensætningen i $\mathcal{C}^{op}$ defineres ved at vi for $f \in Hom_{\mathcal{C}^{op}}(A,B)$, $g \in Hom_{\mathcal{C}^{op}}(B,C)$ sætter

$$g \circ_{\mathcal{C}^{op}} f = fg \in Hom_{\mathcal{C}^{op}}(A,C).$$

Axiomerne ses let at være opfyldte.

1.14. Ofte betragtes i en kategori $\mathcal{C}$ systemer bestående af visse objekter $\mathcal{O}$ fra $\mathcal{C}$, og visse morfier $\mathcal{M}$ mellem objekterne i $\mathcal{O}$. Et sådant system kaldes et diagram i $\mathcal{C}$. Eksempler på diagrammer er

① $A \xrightarrow{f} B$

②
$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ & {\scriptstyle h}\searrow & \downarrow{\scriptstyle g} \\ & & C \end{array}$$

③
$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle a}\downarrow & & \downarrow{\scriptstyle b} \\ A' & \xrightarrow{f'} & B' \end{array}$$

④ $1_A \; (A \underset{g}{\overset{f}{\rightrightarrows}} B) \; 1_B$

⑤
$$\begin{array}{ccccc} B & \xrightarrow{b} & C & \xrightarrow{c} & D \\ {\scriptstyle a}\uparrow & \searrow^{g} & \textcircled{5} & & \downarrow{\scriptstyle d} \\ A & & & & E \\ & {\scriptstyle f}\searrow & & \nearrow{\scriptstyle e} & \\ & & F & & \end{array}$$

⑥
$$\begin{array}{ccccccccc} \cdots \to & A_{-2} & \xrightarrow{d_{-2}} & A_{-1} & \xrightarrow{d_{-1}} & A_0 & \xrightarrow{d_0} & A_1 & \xrightarrow{d_1} \cdots \\ & {\scriptstyle a_{-2}}\downarrow & & {\scriptstyle a_{-1}}\downarrow & & {\scriptstyle a_0}\downarrow & & {\scriptstyle a_1}\downarrow & \\ \to & A'_{-2} & \xrightarrow{d'_{-2}} & A'_{-1} & \xrightarrow{d'_{-1}} & A'_0 & \xrightarrow{d'_0} & A'_1 & \to \cdots \end{array}$$

Et sådant diagram $(\Theta, \mathcal{M})$ i $\mathcal{C}$ kaldes kommutativt, hvis man for alle $A, B \in \Theta$ højst kan få en morfi fra A til B ved at sammensætte morfier fra $\mathcal{M}$. Diagrammerne ovenfor er således kommutative, når ① altid! ② $gf = h$ ③ $bf = f'a$ ④ f er isomorfi med g som invers ⑤ $ga = f$, $eg = dcb$ (som medfører, at $ef = ega = dcba$) ⑥ $a_{i+1} d_i = d_i' a_i$, $i \in \mathbb{Z}$.

2. Funktorer

2.1. BESKRIVELSE. En <u>funktor</u> $F: \mathcal{C} \to \mathcal{D}$ fra en kategori $\mathcal{C}$ til en kategori $\mathcal{D}$ knytter til hvert

objekt $A \in \mathcal{C}$ et objekt $F(A) \in \mathcal{D}$

og til hver

morfi $A \xrightarrow{f} B$ i $\mathcal{C}$ en morfi $F(A) \xrightarrow{F(f)} F(B)$ i $\mathcal{D}$,

således at der for morfier $A \xrightarrow{f} B$, $B \xrightarrow{g} C$ i $\mathcal{C}$ gælder

$$F(gf) = F(g)F(f) : F(A) \to F(C),$$

og for objekter A i $\mathcal{C}$ gælder

$$F(1_A) = 1_{F(A)} : F(A) \to F(A).$$

2.2. Det følger let, at <u>en funktor $F: \mathcal{C} \to \mathcal{D}$ afbilder isomorfi på isomorfi og kommutativt diagram på kommutativt diagram</u>.

2.3. DEFINITION. En funktor $F: \mathcal{C}^{op} \to \mathcal{D}$ fra den modsatte kategori af $\mathcal{C}$ til en kategori $\mathcal{D}$ kaldes også en <u>kontravariant funktor</u> $F: \mathcal{C} \to \mathcal{D}$. Den knytter altså til hvert objekt $A \in \mathcal{C}^{op}$, d.v.s. til hvert

objekt $A \in \mathcal{C}$ et objekt $F(A) \in \mathcal{D}$,

og til hver morfi $f \in \mathrm{Hom}_{\mathcal{C}^{op}}(A, B)$, d.v.s. til hver

morfi $B \xrightarrow{f} A$ i $\mathcal{C}$ en morfi $F(B) \xleftarrow{F(f)} F(A)$ i $\mathcal{D}$,

således at vi for morfier $B \xrightarrow{f} A$, $C \xrightarrow{g} B$ i $\mathcal{C}$ har

$$F(fg) = F(g)F(f) : F(A) \to F(C)$$

og for objekter A i $\mathcal{C}$ har

$$F(1_A) = 1_{F(A)} : F(A) \to F(A).$$

En kontravariant funktor $F: \mathcal{C} \to \mathcal{D}$ "vender" altså pilene. En funktor $F: \mathcal{C} \to \mathcal{D}$ som beskrevet i 2.1 kaldes også en <u>kovariant funktor</u>

2.4. Funktorer spiller en viglig rolle. Dels viser det sig, at en lang række fænomener mest naturligt beskrives ved hjælp af funktorer, dels kan man ved studiet af en given kategori $\mathcal{C}$ forsøge at finde funktorer $F: \mathcal{C} \to \mathcal{D}$ ind i simplere (eller mere velkendte) kategorier $\mathcal{D}$, og herved løse problemer i $\mathcal{C}$.

2.5. Eksempel. Funktoren $(\,)^*: (L\text{-vect})^{op} \to (L\text{-vect})$ knytter til hvert vektorrum V over L det duale vektorrum V^*, og til hver lineær afbildning $f: V \to W$ den duale afbildning $f^*: W^* \to V^*$.

2.6. Eksempel. Lad os et øjeblik med (Diff_0) betegne følgende kategori: <u>Objekterne</u> er par (U,a), hvor U er en åben mængde i et talrum $\mathbb{R}^k$, og hvor $a \in U$ er et udvalgt element. <u>Morfierne</u> fra (U,a) til (V,b) er C^∞-afbildninger $f: U \to V$, således at $f(a) = b$. <u>Sammensætningen</u> er den sædvanlige.

En funktor

$$T: (\mathrm{Diff}_0) \longrightarrow (\mathbb{R}\text{-vekt})$$

defineres ved at vi for $(U,a) \in (\mathrm{Diff}_0)$, hvor $U \subseteq \mathbb{R}^k$ sætter $T(U,a) = \mathbb{R}^k$

og for en morfi $f: (U,a) \to (V,b)$, hvor $V \subseteq \mathbb{R}^p$ sætter $T(f) = df_a : \mathbb{R}^k \to \mathbb{R}^p$.

2.7. Eksempler. En lang række tidligere omtalte konstruktioner kan med fordel opfattes som funktorer. Således har vi funktorer

① $H \mapsto \tilde{H}$, : (comm. semigr) → (Ab), der til hver kommutativ semigruppe H knytter brøkgruppen $\tilde{H}$.

② $R \mapsto \tilde{R}$: (Int. dom) → (fields), der til hvert kommutativt integritetsområde R knytter brøklegemet $\tilde{R}$ (Hvad er morfisme i kategorien (Int. dom)?).

③ $G \mapsto \hat{G}$: (ord. gr) → (compl. ord. gr), der til hver kommutativ ordnet gruppe G knytter kompletionen $\hat{G}$ (Hvad er morfisme i kategorien (Ord. gr)?).

④ $\Lambda \mapsto \Lambda[X]$: (Rings) → (Rings), der til hver ring Λ knytter polynomiumsringen $\Lambda[X]$.

⑤ $\Lambda \mapsto \Lambda^*$: (Rings) → (Gr), der til hver ring Λ knytter gruppen Λ^* af invertible elementer i Λ.

⑥ $M \mapsto \mathbb{Z}^{(M)}$: (Sets) → (Ab), der til hver mængde M knytter den fri kommutative gruppe frembragt af M.

⑦ $(M, \sim) \mapsto M/\sim$: (Equiv) → (Sets), der til hver mængde M med en ækvivalensrelation $\sim$ knytter kvotienten $M/\sim$.

2.8. Eksempel. Er M et monoid, kan vi betragte kategorien $\mathrm{Cat}(M)$, jfr. 1.10. Det ses, at en funktor $F: \mathrm{Cat}(M) \to \mathcal{D}$ er det samme som et objekt $D \in \mathcal{D}$ forsynet med en monoidhomomorfi $F: M \to \mathrm{End}_{\mathcal{D}}(D)$. Er M' endnu et monoid, ser vi, at en funktor $F: \mathrm{Cat}(M) \to \mathrm{Cat}(M')$ er det samme som en monoidhomomorfi : $F: M \to M'$.

2.9. Er T en mængde med en refleksiv, transitiv relation $\leqslant$, kan vi betragte kategorien $Cat(T)$, jfr. 1.11. Vi ser, at en funktor $F: Cat(T) \to \mathcal{D}$ er det samme som en tilordning, der til hvert $t \in T$ knytter

$$F_t \in \mathcal{D}$$

og for hvert $s \leqslant t$ knytter en morfi

$$F_s \xrightarrow{f_{st}} F_t \quad \text{i } \mathcal{D}$$

således at $f_{ss} = 1_{F_s}$, og således at vi for $s \leqslant t \leqslant u$ har $f_{su} = f_{tu} f_{st}$. Vi har altså et kommutativt diagram

$$\begin{array}{ccc} F_s & \xrightarrow{f_{st}} & F_t \\ & \searrow^{f_{su}} & \downarrow f_{tu} \\ & & F_u \end{array} .$$

Er T' endnu en mængde med en refleksiv, transitiv relation $\leqslant'$, ser vi, at en funktor $F: Cat(T) \to Cat(T')$ er det samme som en ordenstro afbildning $F: T \to T'$!

Hvis relationen i T er $=$ (således at $Cat(T)$ er en diskret kategori, jfr. 1.11), ser vi, at en funktor $F: Cat(T) \to \mathcal{D}$ blot er en afbildning, der til hvert element $t \in T$ knytter et objekt $F_t \in \mathcal{D}$.

Er derimod $\mathcal{D}$ en diskret kategori og $\mathcal{C}$ en vilkårlig kategori, ser vi, at en funktor $F: \mathcal{C} \to \mathcal{D}$, er en "afbildning", der til hvert objekt $A \in \mathcal{C}$ knytter et objekt $F(A) \in \mathcal{D}$ på en sådan måde, at vi har $F(A) = F(B)$, hvis der findes en morfi $: A \xrightarrow{f} B$ i $\mathcal{C}$.

2.10. Eksempel. Lad X være et topologisk (eller et metrisk) rum. Med $Open(X)$ betegner vi kate-

gorien hørende til mængden af åbne delmængder af X, med inklusionen $\subseteq$ som relation (jfr. 1.11 og 2.9). En kontravariant funktor $F : \mathrm{Open}(X) \to (\mathrm{Sets})$ kaldes et <u>præ-knippe af mængder på X</u>. Et sådant er altså givet ved, at der til hver åben delmængde $U \subseteq X$ er knyttet en mængde $F(U)$, og til åbne delmængder $V \subseteq U$ er knyttet en afbildning

$$f_{VU} : F(U) \longrightarrow F(V)$$

[kaldet <u>restriktionen</u>], således at $f_{VW} f_{UV} = f_{UW}$ når $W \subseteq V \subseteq U$, og $f_{U,U} = 1_{F(U)}$.

Tilsvarende definerer præknipper af grupper (resp. abelske grupper, resp. ringe) som kontravariante funktorer : $\mathrm{Open}(X) \to (\mathrm{Gr})$ (resp.: $\mathrm{Open}(X) \to (\mathrm{Ab})$, resp.: $\mathrm{Open}(X) \to (\mathrm{Rings})$) [Eks. præ-knippet $\mathcal{C}^\infty_{\mathbb{R}^k}$ af C^∞-funktioner på $\mathbb{R}^k$].

2.11. Enhver kategori $\mathcal{C}$ er "født" med en række vigtige funktorer: Til hvert objekt $A \in \mathcal{C}$ svarer en funktor : $\mathcal{C} \to (\mathrm{Sets})$, som til et

objekt $X \in \mathcal{C}$ knytter mængden $\mathrm{Hom}_{\mathcal{C}}(A,X)$

og til en

morfi $X \xrightarrow{f} Y$ i $\mathcal{C}$ knytter afbildningen

$$f_* : \mathrm{Hom}_{\mathcal{C}}(A,X) \longrightarrow \mathrm{Hom}_{\mathcal{C}}(A,Y), \quad \varphi \mapsto f_*(\varphi) = f\varphi$$

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & X \\ & \searrow^{f_*(\varphi)=f\varphi} & \downarrow f \\ & & Y \end{array}$$

Det er let at se, at der herved er defineret en funktor. Den betegnes $\mathrm{Hom}_{\mathcal{C}}(A,-)$.

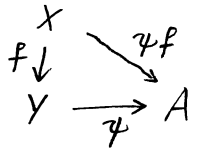
Tilsvarende kan vi definere en kontravariant funktor: $\mathcal{C} \to (Sets)$ ved til et

objekt $X \in \mathcal{C}$ at knytte mængden $Hom_{\mathcal{C}}(X, A)$,

og til en

morfi $X \xrightarrow{f} Y$ i $\mathcal{C}$ at knytte afbildningen

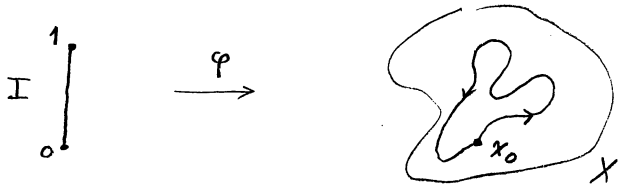
$$f^* : Hom_{\mathcal{C}}(Y, A) \longrightarrow Hom_{\mathcal{C}}(X, A)$$
$$\psi \qquad\qquad \psi$$
$$\psi \longmapsto \psi f$$



Denne funktor betegnes $Hom_{\mathcal{C}}(-, A)$. Vi siger også, at $Hom_{\mathcal{C}}(-,-)$ er en funktor $\mathcal{C} \times \mathcal{C} \to (Sets)$, kontravariant i første variabel, kovariant i anden variabel.

2.12. Som eksempel på hvorledes funktoren kan anvendes til at studere en given kategori, kan vi betragte kategorien (Top_0) af topologiske rum med udvalgt element. (Eller kategorien af metriske rum med udvalgt element (og kontinuerte afbildninger som morfier)). Idet $I = [0,1]$ betegner enhedsintervallet, defineres en <u>løkke</u> i (X, x_0) som en kontinuert afbildning

$$\varphi : I \to X, \text{ således at } \varphi(0) = \varphi(1) = x_0.$$



Mængden af løkker i (X, x_0) betegnes $\Omega(X, x_0)$. Det er let at se, at Ω kan betragtes som en funktor

$$\Omega : (Top_0) \to (Sets).$$

To løkker φ', φ'' i $\Omega(X, x_0)$ kaldes <u>homotope</u>,

og vi skriver $\varphi' \simeq \varphi''$, hvis der findes en kontinuert familie af løkker $\varphi_t \in \Omega(X, x_0)$, $0 \leq t \leq 1$, således at $\varphi_0 = \varphi'$, $\varphi_1 = \varphi''$. [En familie φ_t, $0 \leq t \leq 1$ af løkker i (X, x_0) kaldes kontinuert, hvis den ved $(s,t) \mapsto \varphi_t(s)$ definerede afbildning $: I \times I \to X$ er kontinuert]. Videre kan vi definere en komposition $*$ i $\Omega(X, x_0)$, idet vi for løkker φ, ψ definerer $\varphi * \psi$ ved

$$\varphi * \psi (t) = \begin{cases} \varphi(2t) & 0 \leq t \leq \frac{1}{2} \\ \psi(2t-1) & \frac{1}{2} \leq t \leq 1. \end{cases}$$

Det er ikke svært at vise, at $\simeq$ er en ækvivalensrelation i $\Omega(X, x_0)$, som harmonerer med $*$, og at kvotienten med den inducerede komposition er en gruppe. Denne gruppe kaldes <u>fundamentalgruppen</u> for (X, x_0), og den betegnes $\pi(X, x_0)$. Vi kan opfatte π som en funktor

$$\pi : (Top_0) \to (Gr).$$

Lad D være cirkelskiven $D = \{z \in \mathbb{C} \mid |z| \leq 1\}$, og lad S være periferien $S = \{z \in \mathbb{C} \mid |z| = 1\}$. For D finder vi let

$$\pi(D, 1) = (0) \quad (= \text{gruppen med ét element})$$

idet vi for en løkke φ i $(D, 1)$ kan definere en homotopi med den konstante løkke ved

$$(s,t) \longmapsto 1 + t(\varphi(s) - 1).$$

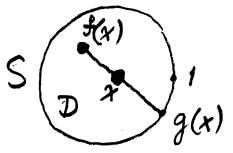
For S kan man vise, at

$$\pi(S, 1) \cong \mathbb{Z} \quad (= \text{cyklisk gruppe frembragt af homotopiklassen der indeholder løkken } t \mapsto e^{2\pi i t}). \text{ [Omløbstal]}.$$

Som anvendelse vises Brouwers fixpunktssætning. <u>Enhver kontinuert afbildning $f : D \to D$ har et fixpunkt.</u> Bevis. Antag, at der findes en kontinuert afbildning $f : D \to D$ uden fixpunkter. Vi kunne da definere en kontinuert af-

bildning $g: D \to S$ ved at

$g(x)$ = skæringspunktet mellem S og halvlinien fra $f(x)$ gennem x.



Vi har $g(x) = x$ for $x \in S$, altså et kommutativt diagram i (Top_o):

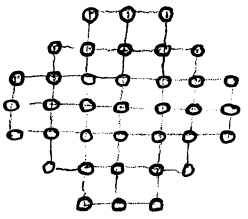
$$\begin{array}{ccc} (S,1) & \xrightarrow{i} & (D,1) \\ & \searrow^{1_S} & \downarrow g \\ & & (S,1) \end{array}$$

hvor i er inklusionsafbildningen, og hvor 1_S er identiteten. Anvender vi funktoren $\pi : (Top_o) \to (Gr)$ får vi et kommutativt diagram i (Gr):

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & (0) \\ & \searrow^{1_{\mathbb{Z}}} & \downarrow \\ & & \mathbb{Z} \end{array}$$

men dette er en modstrid ▨

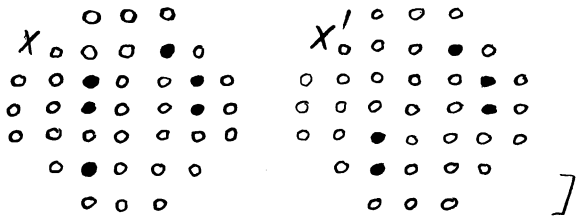
2.13. Lad der være givet en endelig delmængde $B \subseteq \mathbb{Z} \times \mathbb{Z}$.
[Vi tænker på B som et brædt, hvori der er boret huller svarende til elementerne i B. Eksempel



]

Hertil definerer vi en kategori (Sol_B), kaldet solitairespillet på B, på følgende måde.

Objekterne i (Sol_B), kaldet stillinger, er de endelige delmængder af B [Vi tænker på stillingen X ved at sætte pinde i de huller på brædtet, der svarer til elementer i X. Eksempler



]

Ved et solitairetræk fra en stilling X til en stilling X' forstås et sæt $t=(b_1,b_2,b_3)$ af tre på hinanden følgende elementer i B, således at

$$X \setminus X' = \{b_1, b_2\} \qquad X' \setminus X = \{b_3\}.$$

(Elementer $b_1, b_2, b_3 \in \mathbb{Z}\times\mathbb{Z}$ kaldes på hinanden følgende, hvis der for den ene af de to projektioner $\mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}$ gælder, at b_1, b_2, b_3 har samme koordinat, og for den anden, at koordinaterne er tre på hinanden følgende (aftagende eller voksende) hele tal.) For givne stillinger X og X' er der højst et solitairetræk t fra X til X'. Er dette tilfældet skriver vi $X \xrightarrow{t} X'$. [Solitairetrækket fra X til X' tænkes udført ved at vi lader pinden i hul b_1 springe over pinden i hul b_2 ned i det tomme hul b_3, og dernæst fjerner pinden i hul b_2. I eksemplet er vist et solitairetræk fra X til X'].

Morfismerne i (Sol_B) fra X til Y defineres som endelige følger $(t_1,\dots,t_r)$, $r\geqslant 0$ af solitairetræk $X \xrightarrow{t_1} Y_1$, $Y_1 \xrightarrow{t_2} Y_2$, $\dots$, $Y_{r-1} \xrightarrow{t_r} Y_r$.

Og sammensætningen af $(t_1,\dots,t_r): X \to Y$ og $(s_1,\dots,s_p): Y \to Z$ defineres ved

$$(t_1,\dots,t_r)(s_1,\dots,s_p) = (t_1,\dots,t_r,s_1,\dots,s_p).$$

Idet vi med $(\mathbb{Z}/2)^3$ betegner den diskrete kategori, hvis objekter er de 8 elementer i $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$ defineres en funktor

$$F : (Sol_8) \to (\mathbb{Z}/2)^3$$

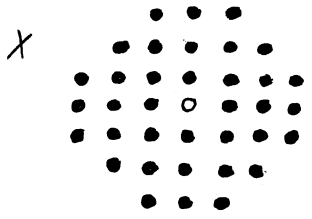
på følgende måde: For $i = 1,2,3$ betegner vi for en stilling X med X_i antallet af elementer $x \in X$, hvis koordinater (x', x'') opfylder $x' + x'' \equiv i$ (modulo 3). Vi sætter

$$F(X) = \left(\overline{X_2 - X_3}\,,\ \overline{X_3 - X_1}\,,\ \overline{X_1 - X_2}\right) \in (\mathbb{Z}/2)^3.$$

hvor $\overline{}$ er den kanoniske homomorfi: $\mathbb{Z} \to \mathbb{Z}/2$.

At der herved defineres en funktor: $(Sol_8) \to (\mathbb{Z}/2)^3$, altså at der gælder $F(X) = F(Y)$, hvis der findes en morfi $X \to Y$, indses lit ved at betragte et solitairetræk: $X \to X'$.

[Eksempel. For en stilling med kun ét element finder vi $F(Y) = (0,1,1)$ eller $(1,0,1)$ eller $(1,1,0)$. For stillingen X angivet ved



har vi $F(X) = (0,0,0)$. Der findes altså ingen morfier fra denne stilling til en stilling med kun ét element!].

2.14. I en lang række af de nævnte eksempler på kategorier har <u>objekterne</u> været mængder forsynet med en eller anden form for struktur (F.eks. et udvalgt element, en (eller flere) indre kompositioner), andre former for kompositioner (f.eks. en metrik), visse udvalgte delmængder ...), <u>morfierne</u> har været afbildninger, der har bevaret denne struktur, og <u>sammensætningen</u> har været sædvanlig sammen-

sætning af afbildninger.

Fra sådanne kategorier kan vi definere "glemsomme" funktorer, der til hvert objekt glemmer strukturen (eller blot noget af strukturen).

F.eks. har vi glemsomme funktorer:

$(Sets_0) \to (Sets)$	"glem det udvalgte element"
$(Gr) \to (Sets)$	"glem kompositionen"
$(Top) \to (Sets)$	"glem topologien"
$(Trip) \to (Sets_0)$	"glem endomorfien"
$(Rings) \to (AG)$	"glem multiplikationen"
$(Rings) \to (Monoids)$	"glem additionen"
$(Rings) \to (Sets_0)$	"glem multiplikation og addition, men husk ét-elementet"
$(Rings) \to (Sets)$	"glem alt".

2.15. BESKRIVELSE. En delkategori $\mathcal{D}$ af en kategori $\mathcal{C}$ opfylder, at objekterne i $\mathcal{D}$ er objekter i $\mathcal{C}$, at vi for morfierne i $\mathcal{D}$ mellem objekter A, B i $\mathcal{D}$ har

$$Hom_{\mathcal{D}}(A,B) \subseteq Hom_{\mathcal{C}}(A,B),$$

at sammensætningen i $\mathcal{D}$ af morfier $A \xrightarrow{f} B$ og $B \xrightarrow{g} C$ i $\mathcal{D}$ er den samme som sammensætningen i $\mathcal{C}$, samt at identiteterne i $\mathcal{D}$ er identiteter i $\mathcal{C}$.

Vi skriver i så fald

$$\mathcal{D} \subseteq \mathcal{C},$$

og vi kan betragte inklusionsfunktoren: $\mathcal{D} \hookrightarrow \mathcal{C}$.

Hvis vi for alle objekter A, B i $\mathcal{D}$ har

$$Hom_{\mathcal{D}}(A,B) = Hom_{\mathcal{C}}(A,B),$$

kaldes $\mathcal{D}$ en fuld delkategori af $\mathcal{C}$. En sådan er helt bestemt ved en beskrivelse af hvilke objekter fra $\mathcal{C}$, som tilhører $\mathcal{D}$.

2.16. Eksempler. I kategorien $\mathcal{K}$ af mængder med en komposition har vi delkategorierne

$$\mathcal{K} \supseteq (\text{Semigr}) \supseteq (\text{Monoids}) \supseteq (\text{Gr}) \supseteq (\text{Ab}).$$

Bemærk, at (Monoids) ikke er en fuld delkategori.

3. Kategoriske definitioner

3.1. En definition vedrørende et system af objekter og morfier i en kategori $\mathcal{C}$ kaldes en kategorisk (eller universel) definition, hvis den i definitionen kun indgår kategoriens grundbestanddele (objekter, morfier, sammensætning). En således defineret egenskab kaldes en universel egenskab.

3.2. DEFINITION. Et objekt $\varnothing$ i kategorien $\mathcal{C}$ kaldes et initialobjekt, hvis der til ethvert objekt $Y \in \mathcal{C}$ findes netop én morfi

$$\varnothing \to Y.$$

Et objekt $*$ i $\mathcal{C}$ kaldes et finalobjekt, hvis der til ethvert objekt $X \in \mathcal{C}$ findes netop én morfi

$$X \to *.$$

3.3. SÆTNING. Hvis $\varnothing$ og $\tilde{\varnothing}$ er initialobjekter i en kategori $\mathcal{C}$, så findes netop én morfi $: \varnothing \to \tilde{\varnothing}$, og denne morfi er en isomorfi.

Bevis. Da $\varnothing$ er et initialobjekt i $\mathcal{C}$ findes netop en morfi: $\varnothing \xrightarrow{\varphi} \tilde{\varnothing}$. Vi skal vise, at φ er en isomorfi. Da $\tilde{\varnothing}$ er et initialobjekt, findes en morfi $\tilde{\varphi} : \tilde{\varnothing} \to \varnothing$. Nu er $\tilde{\varphi}\varphi$ og $1_{\varnothing}$ morfier $: \varnothing \to \varnothing$. Da $\varnothing$ er initialobjekt, slutter vi udfra entydigheden af morfier fra $\varnothing$, at $\tilde{\varphi}\varphi = 1_{\varnothing}$. Tilsvarende får vi $\varphi\tilde{\varphi} = 1_{\tilde{\varnothing}}$, men dette betyder, at φ er en isomorfi (med $\varphi^{-1} = \tilde{\varphi}$) ▨

Hvis en kategori $\mathcal{C}$ har initialobjekter, tænkes ofte udvalgt et bestemt, kaldet initialobjektet.

Tilsvarende vises, at to finalobjekter i en kategori

er kanonisk isomorfe.

3.4. I kategorien (Sets) er den tomme mængde $\emptyset$ initialobjekt, og enhver mængde med netop ét element er finalobjekt.

I kategorien (Trip) (jfr. 1.8). gælder, at $(\mathbb{N}, 1, \varepsilon)$ er initialobjekt. Dette er som bekendt den universelle egenskab ved de naturlige tal. Kategorien (Trip) har trivielt et finalobjekt.

Følgende kategorier har både initialobjekt og finalobjekt:

(Sets), (Gr), (Ab), (L-vect), (Rings), (R-alg), (Top), (Metr, cout), (Metr, $\text{dist}_{\leq}$).

Det samme gælder for følgende kategorier "med udvalgt element"

(Sets_0), (Semigr_0), (Gr_0), (Ab_0), (L-vect_0), (Rings_0) (R-alg_0), (Top_0), $(\text{Metr}_0, \text{cout})$, $(\text{Metr}_0, \text{dist}_{\leq})$.

Precisér selv disse kategorier, og deres initial- og finalobjekt.

Også kategorien (Arch_0) af arkimedisk ordnede kommutative grupper med et udvalgt positivt element har et initial- og et finalobjekt.

Initial- og finalobjekt i en kategori $\text{Cat}(T)$ hørende til en partielt ordnet mængde $T, \leqslant$ er et velkendt begreb.

Kategorien $\mathcal{M}_{H,S}$ (jfr. 1.12) har initialobjektet $H \xrightarrow{\square} H[S^{-1}]$ (og finalobjektet $H \to \{1\}$). Definér for en multiplikativ delmængde S i en kommutativring R en kategori $\mathcal{R}_{R,S}$, hvori

$$R \xrightarrow{\square} R[S^{-1}]$$

er initialobjekt.

Og definér for en kommutativ ordnet gruppe G en kategori $\mathcal{K}_G$, hvori

$$G \xrightarrow{\square} \hat{G}$$

er initialobjekt.

Et objekt $*$ i kategorien $\mathcal{C}$ kan også opfattes som objekt i den duale kategori $\mathcal{C}^{op}$. Vi ser, at $*$ er finalobjekt i $\mathcal{C}$, hvis og kun hvis $*$ er initialobjekt i $\mathcal{C}^{op}$.

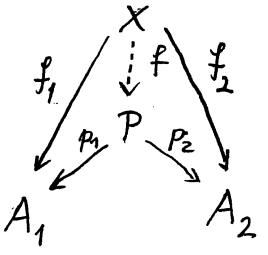
3.5. DEFINITION. Lad A_1 og A_2 være objekter i en kategori $\mathcal{C}$. Ved et <u>produkt</u> af A_1 og A_2 forstås et diagram i $\mathcal{C}$:

$$\begin{array}{ccc} & P & \\ {\scriptstyle p_1}\swarrow & & \searrow{\scriptstyle p_2} \\ A_1 & & A_2 \end{array}$$

med følgende egenskab: For hvert objekt $X \in \mathcal{C}$ og hvert par af morfier $f_1: X \to A_1$, $f_2: X \to A_2$ findes netop én morfi $f: X \to P$, således at $p_1 f = f_1$ og $p_2 f = f_2$. Definitionen udsiger altså, at der for hvert andet diagram

$$\begin{array}{ccc} & X & \\ {\scriptstyle f_1}\swarrow & & \searrow{\scriptstyle f_2} \\ A_1 & & A_2 \end{array}$$

findes netop én morfi $f: X \to P$, så at diagrammet

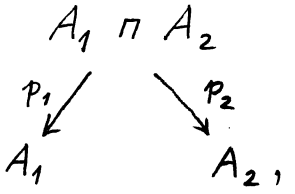


er kommutativt.

3.6. SÆTNING. *To produkter af A_1 og A_2 er kanonisk isomorfe* i følgende forstand: Er

produkter, så findes netop en morfi $\varphi : \overline{P} \to P$, således at $p_1 \circ \varphi = \overline{p}_1$, $p_2 \circ \varphi = \overline{p}_2$, og denne morfi er en isomorfi. □

3.7. For givne objekter A_1 og A_2 i en kategori $\mathcal{C}$ findes ikke nødvendigvis et produkt. Hvis produkter findes, tænkes ofte udvalgt et bestemt. Det betegnes



og kaldes *produktet* af A_1 og A_2; morfierne $p_1 : A_1 \sqcap A_2 \to A_1$ og $p_2 : A_1 \sqcap A_2 \to A_2$ kaldes *projektionerne* (Ofte siger vi, at objektet $A_1 \sqcap A_2$ er produktet af A_1 og A_2, idet projektionerne underforstås).

3.8. Eksempler. For mængder A_1 og A_2 i kategorien (Sets), er det sædvanlige kartesiske produkt $A_1 \times A_2$ med projektionerne

$$p_1 : (a_1, a_2) \longmapsto a_1$$

og

$$p_2 : (a_1, a_2) \longmapsto a_2$$

et produkt i kategorien (Sets). Den universelle egenskab udsiger blot, at afbildningen $f : X \to A_1 \times A_2$ er af formen

$$x \longmapsto (f_1(x), f_2(x))$$

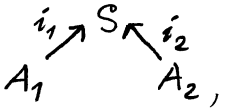
med (entydigt bestemte) afbildninger $f_1 : X \to A_1$, $f_2 : X \to A_2$.

Objekter i hver af følgende kategorier:

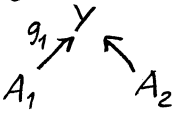
$(Sets_0)$, (Gr), $(L\text{-}vect)$, $(Rings)$, $(R\text{-}alg)$, (Top)
$(Met, dist_{\leq})$, $(Monoids)$, $(Semigr)$, (AG)

er mængder med en vis struktur. For objekter A_1 og A_2 i en af disse kategorier gælder, at produktmængden $A_1 \times A_2$ kan organiseres med en sådan struktur, at den bliver et produkt i den pågældende kategori. Hvad bliver disse "produktstrukturer"?

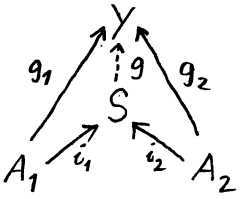
3.9. Til hver kategorisk definition hører en dual definition, der løst sagt fremkommer ved at "vende alle pilene". Til initialobjekt svarer således finalobjekt. Dualt svarer til produkt den såkaldte sum af objekter A_1 og A_2 i kategorien $\mathcal{C}$: Vi skal her betragte diagrammer



og den universelle egenskab er: For hvert andet diagram



findes netop en morfi $g : S \to Y$, så at diagrammet



er kommutativt.

Hvis der findes summer af A_1 og A_2, da er de parvis isomorfe (cfr. sætning 3.6). Ofte tænkes udvalgt en bestemt, kaldet <u>summen</u> af A_1 og A_2 og betegnet

$$\begin{array}{ccc} & A_1 \sqcup A_2 & \\ {\scriptstyle i_1}\nearrow & & \nwarrow{\scriptstyle i_2} \\ A_1 & & A_2 \end{array}.$$

Morfierne i_1 og i_2 er <u>injektionerne</u>.

3.10. Eksempler. For mængder A_1 og A_2 i kategorien (sets) er den sædvanlige **<u>disjunkte forening</u>** $S = A_1 \vee A_2$, med inklusionsafbildningerne

$$i_1 : A_1 \hookrightarrow S$$
$$i_2 : A_2 \hookrightarrow S \qquad \text{som injektionerne}$$

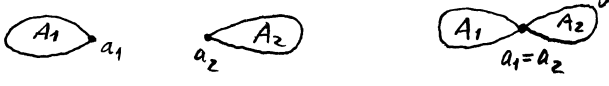
en sum i kategorien (sets). Den universelle egenskab udsiger, at en afbildning $g : A_1 \vee A_2 \to Y$ er helt bestemt ved sine restriktioner $g_1 = g/A_1 : A_1 \to Y$ og $g_2 = g/A_2 : A_2 \to Y$ (da $A_1 \cup A_2 = S$) og at disse restriktioner kan foreskrives vilkårligt (da $A_1 \cap A_2 = \varnothing$ i S).

For objekter A_1 og A_2 i kategorien (AG) (eller i (L-vect)) gælder, at produktet $A_1 \times A_2$ med afbildningerne

$$i_1 : a_1 \longmapsto (a_1, 0)$$
$$i_2 : a_2 \longmapsto (0, a_2) \qquad \text{som injektionerne}$$

er en <u>sum</u>. Ofte skrives $A_1 \oplus A_2$ for $A_1 \times A_2$.

For objekter (A_1, a_1) (A_2, a_2) i kategorien (Sets_0) defineres en sum ved i den disjunkte forening $A_1 \vee A_2$ at identificere elementet a_1 med a_2 og betragte dette element som udvalgt.



Denne sum betegnes $(A_1, a_1) \vee (A_2, a_2)$.

Også i kategorien (Top) findes summer, idet vi for objekter $A_1, A_2 \in (Top)$ kan definere en topologi på mængden $A_1 \vee A_2$; således at det derved fremkomne topologiske rum bliver en sum $A_1 \sqcup A_2$ i kategorien (Top). Tilsvarende med kategorien (Top_0).

For objekter $(A_1, dist_1)$ og $(A_2, dist_2)$ i kategorien $(Metr, dist_{\leqslant})$ findes i almindelighed ikke en sum (betragt f.eks. tilfældet, hvor A_1 og A_2 kun indeholder ét element). [Men summer findes "næsten": Tillader vi afstandsfunktionen, den kan antage værdien ∞, så kan vi definere en afstandsfunktion i mængden $A_1 \vee A_2$, således at det fremkomne "metriske" rum bliver en sum i denne større kategori] Derimod findes der altid summer i kategorien $(Metr_0, dist_{\leqslant})$.

Man kan vise, at der for objekter A_1, A_2 i kategorien (Gr) findes en sum. Den betegnes $A_1 * A_2$.

Ligeledes findes der for objekter A_1, A_2 i kategorien (Comm. R-alg) af kommutative R-algebraer en sum. Den betegnes $A_1 \underset{R}{\otimes} A_2$. Vi skal ikke her komme ind på de to konstruktioner, der ikke er triviele.

3.11. En funktor $F: \mathcal{C} \to \mathcal{D}$ afbilder i diagram

$\#$ $\quad$ P (med pile til A_1 og A_2) $\quad$ i $\mathcal{C}$

på et diagram

$F(\#)$ $\quad$ $F(P)$ (med pile til $F(A_1)$ og $F(A_2)$) $\quad$ i $\mathcal{D}$.

DEFINITION. Funktoren $F: \mathcal{C} \to \mathcal{D}$ siges at <u>kommutere med produkt</u> (eller at <u>respektere produktet</u>), hvis vi, når # er et produkt i $\mathcal{C}$ af A_1 og A_2, kan slutte, at $F(\#)$ er et produkt i $\mathcal{D}$ af $F(A_1)$ og $F(A_2)$.

Hvis produkter eksisterer i $\mathcal{C}$ og $\mathcal{D}$ vil en funktor F afbilde

$$\begin{array}{ccc} & A_1 \sqcap A_2 & \\ \swarrow & & \searrow \\ A_1 & & A_2 \end{array} \quad \text{i } \mathcal{C} \quad \text{på} \quad \begin{array}{ccc} & F(A_1 \sqcap A_2) & \\ \swarrow & & \searrow \\ F(A_1) & & F(A_2) \end{array} \quad \text{i } \mathcal{D}.$$

Herfra fås en morfi: $F(A_1 \sqcap A_2) \longrightarrow F(A_1) \sqcap F(A_2)$, og vi ser, at F kommuterer med produkt, hvis og kun hvis denne morfi er en isomorfi for alle $A_1, A_2 \in \mathcal{C}$.

Tilsvarende defineres funktorer, der <u>respekterer summen</u>.

En kontravariant funktor $F: \mathcal{C} \to \mathcal{D}$ vender pilene og afbilder altså

$$\begin{array}{ccc} & P & \\ \swarrow & & \searrow \\ A_1 & & A_2 \end{array} \quad \text{i } \mathcal{C} \quad \text{på} \quad F(\#) \quad \begin{array}{ccc} & F(P) & \\ \nearrow & & \nwarrow \\ F(A_1) & & F(A_2) \end{array}.$$

En sådan funktor F siges at <u>respektere produktet</u>, hvis vi, når # er et produkt af A_1 og A_2 i $\mathcal{C}$, kan slutte, at $F(\#)$ er en sum af $F(A_1)$ og $F(A_2)$ i $\mathcal{D}$. [Tilsvarende definition med summen].

3.12. Eksempler. Den kontravariante funktor $V \mapsto V^*$ af $(L\text{-vect}) \to (L\text{-vect})$ respekterer både sum og produkt.

Funktoren $T: (\mathrm{Diff}_0) \to (\mathbb{R}\text{-vect})$ beskrevet i eksempel 2.6 respekterer produkt.

Funktorem $H \mapsto \tilde{H}$: (Comm. semigr) $\to$ (AG) fra eksempel 2.7 ① respekterer produkt. (øvelse!).

Funktorem $\Lambda \mapsto \Lambda[X]$: (Rings) $\to$ (Rings) fra eksempel 2.7 ④ respekterer produktet.

Funktorem : $\Lambda \mapsto \Lambda^*$: (Rings) $\to$ (Gr) fra eksempel 2.7 ⑤ respekterer produktet.

Funktorem : $M \mapsto \mathbb{Z}^{(M)}$: (Sets) $\to$ (AG) fra eksempel 2.7 ⑥ respekterer summen (men ikke produktet).

For hvert objekt A i en kategori $\mathcal{C}$ gælder, at funktoren $\mathrm{Hom}_{\mathcal{C}}(A,-) : \mathcal{C} \to (\mathrm{Sets})$ respekterer produktet. (At dette gælder for hvert objekt $A \in \mathcal{C}$ er simpelthen definitionen af produkt i $\mathcal{C}$!).

Tilsvarende gælder for hvert objekt A i $\mathcal{C}$, at den kontravariante funktor

$$\mathrm{Hom}_{\mathcal{C}}(-,A) : \mathcal{C} \to (\mathrm{Sets})$$

respekterer summen (dette er definitionen af sum i $\mathcal{C}$).

Funktorerne $\Omega : (\mathrm{Top}_0) \to (\mathrm{Sets})$ og $\pi : (\mathrm{Top}_0) \to (\mathrm{Gr})$ respekterer produkt.

De glemsomme funktorer : $(\mathrm{Sets}_0) \to (\mathrm{Sets})$ $(\mathrm{Gr}) \to (\mathrm{Sets})$, $(\mathrm{AG}) \to (\mathrm{Sets})$, $(\mathrm{Top}) \to (\mathrm{Sets})$, $(\mathrm{Rings}) \to (\mathrm{Sets})$, jfr. 2.14, vil alle respektere produktet (jfr. eksempel 3.8). De glemsomme funktorer respekterer i almindelighed ikke summen.

[Vis, at de nævnte glemsomme funktorer alle har formen $\mathrm{Hom}_{\mathcal{C}}(A,-)$ med et passende objekt A].

OPGAVER

1. For et element s i en semigruppe M betegner vi med $l_s: M \to M$ venstremultiplikationen $l_s: x \mapsto sx$. Elementet $s \in M$ kaldes venstre-regulært, hvis l_s er injektiv. Elementet s kaldes venstre-invertibelt, hvis der findes et element t (en venstre-invers til s), således at $t \circ l_s = 1_M$. Definer tilsvarende "højre-regulær", "højre-invertibel" og "højre-invers", og vis, at følgende betingelser er ækvivalente:
   (1) s er venstre-invertibel og højre-invertibel.
   (2) s er venstre-invertibel og højre-regulær.
   (3) s har en venstre-invers, der er venstreregulær, og der findes et højre-regulært element i M.
   (4) l_s er bijektiv, og der findes et højreregulært element i M
   (5) M har et neutralt element, og s er invertibel i velkendt forstand (d.v.s. der findes $t \in M$, så at $ts = st =$ neutrale element).

2. Lad R være en relation i en mængde M. Gør rede for at der findes en mindste refleksiv relation R_r (resp. symmetrisk relation R_s, resp. transitiv relation R_t, resp. ækvivalensrelation $\tilde{R}$), som indeholder R [som delmængde af $M \times M$].
   Vis, at $R_{rs} = R_{sr}$, og beskriv R_{rs}.
   Beskriv R_t.
   Vis, at hvis R er refleksiv og symmetrisk, så er $R_t = \tilde{R}$.
   Vis, at der altid gælder $R_{rst} = \tilde{R}$.
   Kvotienten $M/\tilde{R}$ betegnes ofte blot M/R. Vis, at en afbildning $f: M \to R$, som respekterer R [d.v.s. opfylder $xRy \Rightarrow f(x) = f(y)$] entydigt kan udvides til en afbildning $\bar{f}: M/R \to P$.
   Antag nu at der i M desuden er givet en komposition $*$. Gør rede for at der findes en mindste kongruensrelation $\bar{\bar{R}}$, som indeholder R. Vis, at en homomorfi $f: (M,*) \to (P,*)$, som respekterer R, også vil respektere $\bar{\bar{R}}$. Vis, at hvis R er refleksiv og symmetrisk, og harmonerer med $*$, så er $R_t = \bar{\bar{R}}$.

3. Lad A være en mængde (et "alfabet"). Med $\mathcal{S}(A)$ betegnes mængden af tuplen ("ord")

$$(a_1, \dots, a_n), \quad n \in \mathbb{N}, \ a_1, \dots, a_n \in A.$$

I mængden $\mathcal{S}(A)$ defineres en komposition $*$ ved at

$$(a_1, \dots, a_n) * (b_1, \dots, b_m) = (a_1, \dots, a_n, b_1, \dots, b_m).$$

Overvej, at kompositionen $*$ er associativ. $(\mathcal{S}(A), *)$ kaldes den frie semigruppe frembragt af (alfabetet) A. Via afbildningen $a \mapsto (a)$ kan vi opfatte A som en delmængde af $\mathcal{S}(A)$. Med denne identifikation kan elementet $(a_1, \dots, a_n)$ i $\mathcal{M}(A)$ skrives

$$(a_1, \dots, a_n) = a_1 * \cdots * a_n.$$

Vis, at der for enhver semigruppe M gælder: Enhver afbildning $f: A \to M$ kan entydigt udvides til en homomorfi $\hat{f}: \mathcal{S}(A) \to M$.

Tillades det tomme tupel $()$ får vi det frie monoid $\mathcal{M}(A)$. [monoid = semigruppe med neutralt element, monoid-homomorfi = homomorfi mellem monoider, som afbilder neutralt element i neutralt element].
Vis, at der for ethvert monoid M gælder: Enhver afbildning $f: A \to M$ kan entydigt udvides til en monoid-homomorfi $\hat{f}: \mathcal{M}(A) \to M$.

4. Lad S være en delmængde af mængden A. Med $A \vee S$ betegner vi den disjunkte forening af A med S, d.v.s. delmængden

$$A \vee S = \{(x, i) \in A \times \{1, 2\} \mid i = 2 \Rightarrow x \in S\}.$$

Vi identificerer elementet $a \in A$ med det tilsvarende element $(a, 1) \in A \vee S$, og vi sætter for $s \in S$, $\bar{s} = (s, 2)$.

Lad $\equiv$ være den mindste kongruensrelation i $\mathcal{M}(A \vee S)$, som opfylder at $(\bar{s}, s) \equiv (s, \bar{s}) \equiv ()$, for alle $s \in S$, sæt $\mathcal{M}(A, S^{-1}) = \mathcal{M}(A \vee S)/\equiv$, og lad $\theta: A \to \mathcal{M}(A, S^{-1})$ være den sammensatte afbildning $A \hookrightarrow \mathcal{M}(A \vee S) \to \mathcal{M}(A \vee S)/\equiv$

Vis, at der for hvert $s \in S$ gælder, at $\textcircled{s}$ er invertibel i $\mathcal{M}(A, S^{-1})$, og vis, at der for hvert monoid M gælder: Enhver afbildning $f: A \to M$, som opfylder at $f(s)$ er invertibel i M for alle $s \in S$, kan entydigt udvides til en homomorfi $\tilde{f}: \mathcal{M}(A, S^{-1}) \to M$.
Vis, at $\mathcal{M}(A, A^{-1})$ er en gruppe. Den kaldes <u>den frie gruppe</u> frembragt af A.
⊡ Beskriv kongruensrelationen $\equiv$ i $\mathcal{M}(A \vee S)$.

Antag nu yderligere, at der er i A er givet en komposition $\cdot$, og betragt i $\mathcal{M}(A, S^{-1})$ den mindste kongruensrelation $\bar{\sim}$, som opfylder, at $\textcircled{a \cdot b} \bar{\sim} \textcircled{a} * \textcircled{b}$, hvor $*$ er kompositionen i $\mathcal{M}(A, S^{-1})$. Lad $A[S^{-1}]$ betegne kvotientm $\mathcal{M}(A, S^{-1})/\bar{\sim}$, og lad $\square: A \to A[S^{-1}]$ betegne den sammensatte afbildning:

$$A \to \mathcal{M}(A \vee S) \to \mathcal{M}(A \vee S)/\equiv \; = \mathcal{M}(A, S^{-1}) \to A[S^{-1}].$$

Vis, at $\square$ er en homomorfi, og formuler og bevis en tilhørende udvidelsessætning.

5. En semigruppe M siges at <u>operere fra venstre</u> på mængden X, hvis der er givet en en homomorfi af semigruppen

$$\lambda: M \to End(X), \qquad s \longmapsto \lambda_s$$

hvor $End(X)$ er semigruppen af afbildninger af X ind i sig selv. At λ er en homomorfi betyder, at

$$\lambda_s(\lambda_t(x)) = \lambda_{st}(x), \quad s,t \in M, \; x \in X.$$

Ofte skrives $s.x$ i stedet for $\lambda_s(x)$, og $(s,x) \longmapsto s.x$ opfattes som en ydre komposition $M \times X \to X$. Betingelsen er, at

$$s.(t.x) = (st).x, \quad s,t \in M, \; x \in X.$$

Med $\underset{M}{\sim}$ betegnes den mindste ækvivalensrelation i X, som opfylder, at $s.x \underset{M}{\sim} x$ for $s \in M, x \in X$. Ækvivalensklasserne kaldes <u>baner</u> (engelsk: Orbits), og den tilsvarende kvotient kaldes <u>banerummet</u> og betegnes $M\backslash X$.

Semigruppen M siges at <u>operere fra højre</u> på X, hvis der er givet en afbildning $\rho: M \to End(X)$, som opfylder, at

$$\rho_{st} = \rho_t \circ \rho_s$$

[ρ er en såkaldt <u>antihomomorfi</u>]. Idet vi i dette tilfælde bekvemt skriver $x.s$ for $\rho_s(x)$ bliver betingelsen, at

$$(x.s).t = x.(st), \quad s,t \in M, \ x \in X.$$

Tilsvarende defineres bane og banerummet X/M.

Beskriv ækvivalensrelationen i tilfældet, hvor M er kommutativ.

Vis, at vi for en ikke-tom stabil delmængde S i en kommutativ semigruppe H på naturlig måde har

$$H[S^{-1}] = {}_S\backslash H \times S.$$

6. En gruppe G siges at operere fra venstre på X, hvis homomorfien $\lambda: G \to End(X)$ opfylder, at $\lambda_1 = 1_M$, altså

$$1.x = x, \quad x \in X.$$

Vis, at λ i dette tilfælde kan opfattes som en gruppehomomorfi $\lambda: G \to Aut(X)$.

Vis, at ækvivalensrelationen $\underset{G}{\sim}$ i dette tilfælde er givet ved

$$x \underset{G}{\sim} x' \Leftrightarrow \exists s \in G : x' = s.x$$

og at bane, der indeholder x, er delmængden $G.x$.

Et element $x \in X$ kaldes et <u>fixelement</u>, hvis $s.x = x$ for alle $s \in G$. Mængden af fixelementer betegnes X^G.

Vis, at gruppen G opererer fra venstre på sig selv ved fastsættelsen $s.x = sxs^{-1}$ ("konjugering"). Ækvivalensklasserne kaldes konjugerentklasser. Hvilke elementer er fixe.

Vis, at gruppen G opererer på mængden af sine undergrupper ved fastsættelsen $s.H = sHs^{-1}$! Hvilke "elementer" er her fixe.

Vis, at en undergruppe H i G opererer fra venstre på G ved fastsættelsen $s.x = sx$, $s \in H$, $x \in G$. ("Translation").

Hvilke elementer er fixe. Banenummet betegnes $_H\backslash G$. Operatør H tilsvarende fra højre på G bruges betegnelsen G/H for banenummet.

Vis, at hvis gruppen G operer fra venstre på mængden X, så er for hvert $x \in X$ delmængden

$$I_x = \{s \in G \mid s.x = x\} \subseteq G$$

en undergruppe. [Isotropigruppen]. Vis, at afbildningen $s \mapsto s.x$ af G ind i X inducerer en bijektiv afbildning

$$G/I_x \xrightarrow{\sim} G.x$$

og udled i tilfældet, hvor mængden X er endelig, følgende klassetalmel

$$|X| = |X^G| + \sum |G : I_{x_i}|,$$

hvor der i Σ summeres over et repræsentantsystem for baneme, der indeholder mere end ét element. Slut specielt: Hvis antallet af elementer i G er en potens af et primtal p, så er $|X| \equiv |X^G| \pmod p$.

7. En endelig gruppe G, hvis orden $|G|$ er en potens af primtallet p, kaldes en p-gruppe. Vis, at en p-gruppe $G \neq (e)$ har et ikke-trivielt centrum, dvs at $Z := \{x \in G \mid \forall s \in G : sx = xs\} \supset (e)$.
[Vink: Lad G operere på sig selv ved konjugering, og anvend klasseformlen]

8. Vis, at en p-gruppe G af orden p^n for hvert $\nu \leqslant n$ har en normal undergruppe af orden p^ν.
[Vink: Vis, at centret Z indeholder et element c af orden p, og at undergruppen $\langle c \rangle$ frembragt af c er normal. Betragt nu kvotienten $G/\langle c \rangle$ af orden p^{n-1} og anvend induktion efter n]

9. Lad H, K være undergrupper i den endelige gruppe G, og sæt

$$\mathcal{N}_G(K,H) = \{ s \in G \mid sKs^{-1} \subseteq H \}.$$

Vis, at $|H|$ er divisor i $|\mathcal{N}_G(K,H)|$ [Vink: $\mathcal{N}_G(K,H)$ er en forening af visse højre sideklasser Hs]
Vis for $H = K$, at $\mathcal{N}_G(H) := \mathcal{N}_G(H,H)$ er en undergruppe i G, at H er normal undergruppe i $\mathcal{N}_G(H)$, og at

$$|G : \mathcal{N}_G(H)| = \#\text{ undergrupper i } G \text{ konjugerede med } H \ (\text{dvs af formen } sHs^{-1}).$$

Slut specielt, at dette antal er divisor i $|G:H|$.

10. Vis, at når K er en p-gruppe, så er

$$\frac{|\mathcal{N}_G(K,H)|}{|H|} \equiv |G:H| \mod p.$$

[Vink: G (og dermed også K) opererer fra venstre på G/H. Bestem nu $(G/H)^K$ og anvend klasseformlen].

Slut heraf: Hvis $|G:H| \not\equiv 0 \mod p$, så findes $x \in G$ så at $xKx^{-1} \subseteq H$. Sylows 1ste sætning udsiger, at en gruppe G af orden $|G| = p^r m$, hvor p er et primtal, $p \nmid m$ har undergrupper af orden p^r, de såkaldte Sylow-p-undergrupper i G. Vis Sylow's 2den sætning:
Enhver p-gruppe $K \subseteq G$ er indeholdt i en Sylow-p-undergruppe, og alle Sylow-p-undergrupper i G er konjugerede. Antallet af Sylow-p-undergrupper er divisor i m og $\equiv 1 \mod p$.

11. Lad n være et naturligt tal af formen $n = mp^{r+s}$, hvor p er et primtal. Vis, at

$$\binom{n}{p^r} \equiv mp^s \pmod{p^{s+1}}$$

[Vink: Slut v.hj.a. binomialformlen, at $(1+X)^{p^r} = 1+X^{p^r} + pg_0(X)$, $(1+X)^{p^{r+1}} = (1+X^{p^r})^p + p^2 g_1(X), \ldots, (1+X)^{p^{r+s}} = (1+X^{p^r})^{p^s} + p^{s+1} g_s(X)$, $(1+X)^{mp^{r+s}} = (1+X^{p^r})^{mp^s} + p^{s+1} g(X)$, hvor $g_0, \ldots, g_s, g \in \mathbb{Z}[X]$]

12. Lad G være en gruppe af orden $|G| = mp^{r+s}$, hvor primtallet p ikke går op i m, og lad d_r være antallet af undergrupper af orden p^r i G. Vis, at $d_r \equiv 1 \pmod{p}$, specielt altså at $d_r \neq 0$. [Vink: Lad X være mængden af delmængder $F \subseteq G$ med p^r elementer, og lad G operere fra venstre på X ved translation. Vis, at når $x \in F \subseteq X$, så er $I_F x \subseteq F$, og slut, at $|I_F|$ er divisor i $|F| = p^r$. Slut heraf: Hvis $|I_F| < |p^r|$, så vil den tilsvarende bane have elementantal $\equiv 0 \mod p^{s+1}$, og antallet af sådanne F'er er altså $\equiv 0 \mod p^{s+1}$. De $F \in X$, der har $|I_F| = p^r$, er netop delmængderne af formen Hx, $x \in G$ og H er en undergruppe med p^r elementer, og antallet af sådanne F'er er $= d_r m p^s$. Anvend nu opg. 11].

13. Lad G være en p-gruppe, og lad $H \subset G$. Vis, at $H \subset N_G(H)$, og slut specielt for $|G:H| = p$, at H er normal i G [Vink: anvend opgave 10]

14. Lad $(G,+)$ være en kommutativ gruppe af orden $|G|$ $n = p_1^{\nu_1} \cdots p_s^{\nu_s}$, hvor p_i'erne er indbyrdes forskellige primtal. Vis, at G har netop én Sylow-p_i-gruppe G_i, $i = 1, \ldots, s$ og vis, at homomorfien

$$G_1 \times \cdots \times G_s \longrightarrow G : (x_1, \ldots, x_s) \longmapsto x_1 + \cdots + x_s$$

er injektiv, og dermed en isomorfi.

15. Lad G være en gruppe, og definer for hver delmængde $K \subseteq G$ en relation R_K i G ved

$$x R_K y \Leftrightarrow x^{-1}y \in K.$$

Vis, at relationerne R i G, som respekterer venstremultiplikation [d: opfylder $xRy \Rightarrow zx\,R\,zy$], netop er relationerne af formen R_K med en entydigt bestemt delmængde $K \subseteq G$. Karakterisér, ved egenskaber for K, at R_K er ① refleksiv, ② irrefleksiv, ③ symmetrisk, ④ asymmetrisk, ⑤ transitiv, ⑥ total eller ⑦ at R_K respekterer højremultiplikation.

16. En partielt ordnet mængde $(M, \prec)$ siges at være noethersk ordnet, hvis der i enhver opstigende følge

$$a_1 \preceq a_2 \preceq a_3 \preceq \cdots$$

gælder "$=$" fra et vist trin [d: hvis der for en hver homomorfi $a : (\mathbb{N}, \leqslant) \to (M, \preceq)$ findes et $N \in \mathbb{N}$ så at $a_n = a_{n+1}$ når $n \geqslant N$]. Vis, at betingelsen er ækvivalent med, at enhver ikke-tom delmængde $S \subseteq M$ har et maksimalt element.

Vis, at de opstigende følger i M naturligt ordnes ved definitionen $a \preceq b \Leftrightarrow \forall n \in \mathbb{N} : a_n \preceq b_n$, og vis, at hvis M er noethersk ordnet, så er også de opstigende følger noethersk ordnet.

17. Lad R være en symmetrisk og transitiv relation i M, og lad $x \in M$. Hvis xRy, følger det af symmetrien, at yRx og dernæst af transitiviteten, at xRx. Følgelig er R refleksiv. Find fejlen.

18. I $\mathbb{N}$ defineres relationen $/$ ved $a/b \Leftrightarrow \exists d \in \mathbb{N} : da = b$. Vis, at $\mathbb{N}$ med den modsatte ordning af $/$ er noethersk ordnet. Hvad bliver de minimale elementer (m.h.t. "$/$") i $S = \mathbb{N} \setminus \{1\}$.