Matematik 2. del 1964–65

Chr. U. Jensen

Forelæsninger over algebra

Noter fra forelæsninger over to semestre,
taget af Anders Thorup

~/local/manoter/indentryk/jensen65.tex 8-08-2012 12:25:30

chr.u.jensen algebra

KAPITEL I GRUPPER

En ikke tom mængde, $\mathcal{H}$, i en gruppe $(\mathcal{G},\cdot)$ er en undergruppe, hvis $a,b\in\mathcal{H} \Rightarrow ab^{-1}\in\mathcal{H}$.

For en gruppe, $\mathcal{G}$, er $\mathcal{Z} = \{h\in\mathcal{G} \mid \forall g\in\mathcal{G}: hg = gh\}$ en undergruppe, kaldet $\mathcal{G}$'s centrum.

Eks. Find centrum i GL(2,L). Vi har $\begin{pmatrix} a & b\\ c & d\end{pmatrix}\begin{pmatrix} 0 & 1\\ 1 & 0\end{pmatrix} = \begin{pmatrix} b & a\\ d & c\end{pmatrix}$ og $\begin{pmatrix} 0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix} a & b\\ c & d\end{pmatrix} = \begin{pmatrix} c & d\\ a & b\end{pmatrix}$, så at $\mathcal{Z}\subseteq\left\{\begin{pmatrix} a & b\\ b & a\end{pmatrix}\right\}$. Endvidere er $\begin{pmatrix} a & b\\ b & a\end{pmatrix}\begin{pmatrix} 1 & 0\\ 0 & -1\end{pmatrix} = \begin{pmatrix} a & -b\\ b & -a\end{pmatrix}$ og $\begin{pmatrix} 1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix} a & b\\ b & a\end{pmatrix} = \begin{pmatrix} a & b\\ -b & -a\end{pmatrix}$, altså $\mathcal{Z}\subseteq\left\{\begin{pmatrix} a & 0\\ 0 & a\end{pmatrix}\right\}\subseteq\mathcal{Z}$, så at $\mathcal{Z} = \{a\underline{\underline{E}} \mid a\in L\}$.

For undergrupper, $\mathcal{H}_1,\mathcal{H}_2$, i $\mathcal{G}$ er $\mathcal{H}_1\cap\mathcal{H}_2$ en undergruppe, hvorimod $\mathcal{H}_1\cup\mathcal{H}_2$ er en undergruppe, hvis og kun hvis $\mathcal{H}_1\supseteq\mathcal{H}_2$ eller $\mathcal{H}_2\supseteq\mathcal{H}_1$.

For $a\in\mathcal{G}$ defineres $a^0 = e$ (neutralt element), og for $n\geq 1$ induktivt $a^n = aa^{n-1}$. For $n>0$ sættes $a^{-n} = (a^{-1})^n$. Vi har potensreglerne $(a^n)^m = a^{nm}$ og $a^na^m = a^{n+m}$, hvorimod $(ab)^n = a^nb^n$ kun hvis a og b kommuterer.

Er $\mathcal{S}$ en vilkårlig delmængde, betegner $\bar{\mathcal{S}}$ den mindste undergruppe, der indeholder $\mathcal{S}$. Vi har $\bar{\varnothing} = \underline{\underline{E}}$ ($= \{e\}$), og $\bar{\mathcal{S}} = \{s_1^{m_1}\ldots s_n^{m_n} \mid s_1,\ldots,s_n\in\mathcal{G}\wedge n_1,\ldots,n_n\in\dot{Z}\}$. $\bar{\mathcal{S}}$ kaldes den af $\mathcal{S}$ frembragte undergruppe. Er specielt $\mathcal{S} = \{g\}$, bliver $\bar{\mathcal{S}} = \{g^n \mid n\in\dot{Z}\}$, som kaldes den af g frembragte cykliske undergruppe. Der kan indtræffe to mulligheder: 1) alle elementerne g^n, $n\in\dot{Z}$ er forskellige. eller 2) Der findes $m<n$, så at $g^n = g^m$, men da er $g^{n-m} = e$. Lad h være denmindste positive eksponent, for hvilken $g^h = e$, da er $(g) = \{g^n \mid n\in\dot{Z}\} = \{e,g,g^2,\ldots,g^{h-1}\}$. h kaldes g's orden, og $g^n = e \Leftrightarrow h\mid n$.

En gruppe $\mathcal{G}$ kaldes cyklisk, hvis der findes $g\in\mathcal{G}$, så at $\mathcal{G} = (g)$. Det ses, at en cyklisk gruppe er abelsk.

Sætning. Enhver undergruppe i en cyklisk gruppe er cyklisk.

Klart!

Tilføjelse. Hvis $\mathcal{G}$ er af den endelige orden, n, da har forskellige undergrupper forskellig orden, og til hver divisor d i n, findes netop en undergruppe af orden n.

Opg. 1) Vis, at a og a^{-1} har samme orden.

2) Vis, at ab og ba har samme orden.

3) Vis, at hvis alle elementer $g\neq e$ har orden 2, da er $\mathcal{G}$ abelsk.

4) Vis, at hvis $\mathcal{G}$ har netop ét element af orden 2, da ligger det i centrum.

5) For undergrupper, $\mathcal{H},\mathcal{K}$, i $\mathcal{G}$ gælder: $\mathcal{H}\cdot\mathcal{K}$ er en under-

dergruppe $\mathcal{H}\cdot\mathcal{K} = \mathcal{K}\cdot\mathcal{H}$ ($\mathcal{H}\cdot\mathcal{K} = \{hk \mid h\in\mathcal{H} \text{ og } k\in\mathcal{K}\}$).

Lad $\mathcal{O}$ være en gruppe, og $\mathcal{H}\subseteq\mathcal{O}$ en undergruppe. For $a,b\in\mathcal{O}$ sættes $a \underset{V}{\sim} b \Leftrightarrow a^{-1}b \in \mathcal{H}$. $\underset{V}{\sim}$ er en akvivalensrelation, kaldet <u>venstreækvivalent med</u>. $\underset{V}{\sim}$ giver en klasseinddeling af $\mathcal{O}$ i klasser $\textcircled{a}_V = \{x\in\mathcal{O} \mid a \underset{V}{\sim} x\}$. Da $a \underset{V}{\sim} b \Leftrightarrow b\in a\mathcal{H}$ og $a\in b\mathcal{H} \Leftrightarrow a\mathcal{H} = b\mathcal{H}$, er $\textcircled{a}_V = a\mathcal{H}$.

Er $\mathcal{H}$ endelig, er klasserne endelige, og vi finder: $\mathcal{O}$'s orden = (ant. af klasser) $\cdot$ ($\mathcal{H}$'s orden). Specielt fås:
<u>En gruppe af primtaltsorden er cyklisk.</u>
Tilsvarende indføres $\underset{H}{\sim}$ og højresideklasser.

Er $\mathcal{O}$ endelig finder vi $\text{ord}(\mathcal{O})/\text{ord}(\mathcal{H})$ = ant. af v.-sidekl. = ant. af h.-sidekl., som kaldes $\mathcal{H}$'s <u>index</u> i $\mathcal{O}$ og betegnes $(\mathcal{O}:\mathcal{H})$, altså

$$(\mathcal{O}:\mathcal{H}) = \text{ord}(\mathcal{O})/\text{ord}(\mathcal{H})$$

Vælges for hver v.-sidekl. en repræsentant a_ι, $\iota\in I$, da er a_ι^{-1}, $\iota\in I$ er repræsentantsystem for h.-sidekl.

Sætning. <u>Følgende betingelser er ækvivalente</u> (med ovennævnte betegnelser):

I <u>venstreækvivalens = højreækvivalens</u>
II <u>$\underset{V}{\sim}$ harmonerer med $\cdot$</u> (er en kongruensrelation)
III <u>$\underset{H}{\sim}$ harmonerer med $\cdot$</u>
IV <u>$x^{-1}\mathcal{H}x \subseteq \mathcal{H}$ for $x\in\mathcal{H}.\mathcal{O}$</u>
V <u>$x^{-1}\mathcal{H}x = \mathcal{H}$ for $x\in\mathcal{O}$.</u>

og en undergruppe, der opfylder én af disse betingelser kaldes <u>normal</u> eller <u>invariant,</u> og vi skriver $\mathcal{H}\lhd\mathcal{O}$.

Eks. I $\mathcal{O} = GL(n,L)$ er $\mathcal{H} = \{\underline{\underline{A}} \mid \det\underline{\underline{A}} = 1\}$ en normaldeler. Sideklasserne er mængder af matricer med samme determinant.

Nyttig er følgende trivielle
Sætning. <u>Hvis $(\mathcal{O}:\mathcal{H}) = 2$, er $\mathcal{H}$ normal i $\mathcal{O}$.</u>

Hvis $\mathcal{H}\lhd\mathcal{O}$ kan vi ved $\textcircled{a}\textcircled{b} = \textcircled{ab}$ definere en komposition i mængden af ækvivalensklasser, som gør denne til en gruppe kaldet <u>faktorgruppen</u> eller <u>kvotientgruppen</u> af $\mathcal{O}$ m.h.t. $\mathcal{H}$ og betegnes $\mathcal{O}/\mathcal{H}$. Vi har $\text{ord}(\mathcal{O}/\mathcal{H}) = (\mathcal{O}:\mathcal{H}) = \text{ord}(\mathcal{O})/\text{ord}(\mathcal{H})$.

$\mathcal{O}$ har altid trivielle normaldelere, nemlig $\mathcal{O}$ og $\mathcal{E} = \{e\}$.
Endvidere er <u>centrum, $\mathcal{Z}$, normaldeler.</u>

Eks. Lad Δ være en ligesidet trekant. I gruppen bestående af flytninger, der fører Δ over i sig selv =

{ident., to drejninger, 3 spejlinger} er $\mathcal{P}$ = {ident., en spejling} ikke normal, da drejn.$\circ\, \mathcal{S} \circ$ drejn.$^{-1}$ = {ident., en anden spejling}.

En gruppe, der kun har trivielle normaldelere, kaldes simpel. De simple abelske grupper er cykliske grupper af primtalsorden.

Opg. 1) $\mathcal{O}$ af lige orden $\Rightarrow$ antallet af elementer af orden 2 er ulige.
2) $\mathcal{H} \lhd \mathcal{O} \Rightarrow \mathcal{H} \cdot \mathcal{K}$ er en undergruppe.
3) $\mathcal{H} \lhd \mathcal{O}$ og $\mathcal{K} \lhd \mathcal{O} \Rightarrow \mathcal{H} \cdot \mathcal{K} \lhd \mathcal{O}$ og $\mathcal{H} \cap \mathcal{K} \lhd \mathcal{O}$.
4) Enhver kongruensrelation kommer fra en normaldeler $\circ$: $\{x \mid x \sim e\} \lhd \mathcal{O}$.

En afbildning $\varphi : \mathcal{O} \to \mathcal{O}'$ kaldes en homomorfi, hvis $\varphi(gh) = \varphi(g)\varphi(h)$. Hvis φ er surjektiv, resp. injektiv, resp. bijektiv, bruges også betegnelserne epimorfi, resp. monomorfi, resp. isomorfi Hvis $\mathcal{O} = \mathcal{O}'$ kaldes en homomorfi også en endomorfi, og en isomorfi kaldes så en automorfi.

Homomorfisætningen. Er $\varphi: \mathcal{O} \to \mathcal{O}'$ er epimorfi, da er kernen for φ ($\circ : \varphi^{-1}(e')$) en normaldeler i $\mathcal{O}$, og $\mathcal{O}/\ker\varphi \cong \mathcal{O}'$.

Korollar. Alle cykliske grupper af samme orden er isomorfe. nemlig isomorfe med $\grave{Z}$ (uendelig orden) eller $\grave{Z}/n\grave{Z}$ (orden n).

Eks. 1) log : $\grave{R}_+$ på $\grave{R}$ er en isomorfi mellem $(\grave{R}_+, \cdot)$ og $(\grave{R}, +)$.
2) ({drejninger om 0 i planen}, $\circ$) $\cong$ ($\{z \in \grave{C} \mid |z| = 1\}, \cdot$)

$\mathcal{O}$ er abelsk $\Leftrightarrow$ $x \to x^{-1}$ er en automorfi i $\mathcal{O}$.

$\mathcal{A}ut(\mathcal{O})$ betegner mængden af automorfier i gruppen $\mathcal{O}$, og udgør med sammensætning en gruppe, $\mathcal{O}$'s automorfigruppe. For hvert $s \in \mathcal{O}$ definerer $g \to sgs^{-1}$ en automorfi, φ_s, i $\mathcal{O}$, en såkaldt indre automorfi. Mængden af indre automorfier betegnes $\mathcal{A}ut_i(\mathcal{O}) = \{\varphi_s \mid s \in \mathcal{O}\}$ Da $\varphi_{ss'}(g) = ss'g(ss')^{-1} = ss'gs'^{-1}s^{-1} = \varphi_s \circ \varphi_{s'}(g)$ er afbildningen $s \to \varphi_s$ en homomorfi af $\mathcal{O}$ på $\mathcal{A}ut_i(\mathcal{O})$, så $\mathcal{A}ut_i(\mathcal{O})$ er en gruppe. Endvidere.

Sætning. $\mathcal{A}ut_i(\mathcal{O})$ er normaldeler i $\mathcal{A}ut(\mathcal{O})$, og $\mathcal{A}ut_i(\mathcal{O}) = \mathcal{O}/Z$.

Bevis. For $\psi \in \mathcal{A}ut(\mathcal{O})$ og $\varphi_s \in \mathcal{A}ut_i(\mathcal{O})$ får vi $\psi \circ \varphi_s \psi^{-1} = \varphi_{\psi(s)}$, så $\mathcal{A}ut_i(\mathcal{O}) \lhd \mathcal{A}ut(\mathcal{O})$.

Det er let at se, at $\mathrm{Ker}(s \to \varphi_s) = \mathfrak{Z}$.

Af definitionerne følger straks
En undergruppe er normal, hvis og kun hvis den er invariant over for alle $\varphi \in \mathrm{Aut}_i(\mathfrak{G})$.

En undergruppe kaldes karakteristisk, hvis den er invariant over for alle $\varphi \in \mathrm{Aut}(\mathfrak{G})$, og den kaldes fuldstændig invariant, hvis DEN ER invariant over for alle endomorfier i $\mathfrak{G}$.

Sætning. Centrum $\mathfrak{Z}$ i gruppen $\mathfrak{G}$ er karakteristisk.

For $a, b \in \mathfrak{G}$ og $x = aba^{-1}b^{-1}$ har vi $ab = xba$. x kaldes en kommutator, og undergruppen frembragt af alle kommutatorer kaldes $\mathfrak{G}$'s kommutatorgruppe eller første afledede og betegnes $\mathfrak{G}'$. Kommutatorgruppen er fuldstændig invariant.

Sætning. $\mathfrak{G}/\mathfrak{G}'$ er abelsk, og $\mathfrak{G}'$ er den mindste normaldeler, hvis faktorgruppe er abelsk.
Bevis. For (a), (b) $\in \mathfrak{G}/\mathfrak{H}$ gælder: (a)(b) = (b)(a) $\Leftrightarrow$ (ab) = (ba) $\Leftrightarrow$ $(aba^{-1}b^{-1})$ = (e) $\Leftrightarrow$ $aba^{-1}b^{-1} \in \mathfrak{H}$.

Eks. For $\mathfrak{G} = O(2,\mathbb{R})$ d: gruppen af egentl. og uegentl. ortogonale 2×2 matricer d: $\{\underline{\underline{A}} \mid \underline{\underline{A}}\underline{\underline{A}}' = \underline{\underline{E}}\}$, og $\mathfrak{G}_e = O^+(2,\mathbb{R})$ bestående af drejningerne $\begin{pmatrix} \cos v & -\sin v \\ \sin v & \cos v \end{pmatrix}$ finder vi: $\mathfrak{G}' = \mathfrak{G}_e$.

Eks. For $\mathfrak{G} = GL(n,L)$ finder vi $\mathfrak{G}' = \{\underline{\underline{A}} \mid \det \underline{\underline{A}} = 1\}$?

a kaldes konjugeret med b, skrives $a \sim b$, hvis der findes x så $a = xbx^{-1}$. "konjugeret med" er en ækvivalensrel., og deler derfor $\mathfrak{G}$ i akvivalensklasser. Elementerne i $\mathfrak{Z}$ udgør netop klasserne med kun ét element. Vi får straks.

Sætning. En undergruppe $\mathfrak{H} \subseteq \mathfrak{G}$ er normaldeler, hvis og kun hvis den er forening af $\sim$-klasser.

Ved $N_b = \{x \in \mathfrak{G} \mid xb = bx\}$ defineres en undergruppe, normalisatoren for b. b's ækvivalensklasse er $\{xbx^{-1} \mid x \in \mathfrak{G}\}$. Nu er $xbx^{\pm 1} = yby^{-1} \Leftrightarrow y^{-1}xb = by^{-1}x \Leftrightarrow y^{-1}x \in N_b \Leftrightarrow x \underset{v}{\sim} y\ (N_b)$. b's $\sim$-klasse indeholder altså $(\mathfrak{G} : N_b)$ elementer.

Sætning. I en p-gruppe $\mathfrak{G}$ er $\mathrm{ord}(\mathfrak{Z}) \geq p$.
Bevis. Vi har $\mathrm{ord}(\mathfrak{Z}) \mid p^n$, så vi skal blot vise, at $\mathfrak{Z}$ indeholder

mere end ét element. Deles G i konjugeret klasser B, da er

$$\mathrm{ord}(G) = p^\nu = \sum_B \mathrm{card}(B).$$

Har en klasse mere end ét element må den have p^n, $1 \leq n \leq \nu$, da $\mathrm{card}(B) = (G:N_b)$ med passende b. Vi har

$$p^\nu = \sum_{B \subseteq Z} \mathrm{card}(B) + \sum_{B \cap Z = \emptyset} \mathrm{card}(B)$$

$$= \mathrm{ord}(Z) + \sum_{B \cap Z = \emptyset} \mathrm{card}(B).$$

Da konjugeret-klasserne i den sidste sum har mere end ét element, vil p gå op heri, og dermed også i $\mathrm{ord}(Z)$, hvoraf $\mathrm{ord}(Z) \geq p$. □

Sætning. <u>En gruppe, G, af orden p^2 (p primtal) er abelsk.</u>

Bevis. Hvis $\mathrm{ord}(Z) = p^2$ er $G = Z$ abelsk, og ellers er $\mathrm{ord}(Z) = p$, så Z er cyklisk. Nu er $(G:Z) = p^2/p = p$, så at også G/Z er cyklisk. Lad

$$Z = \{e, z, \ldots, z^{p-1}\} \quad \text{og} \quad G/Z = \{\bar{e}, \bar{a}, \ldots, \bar{a}^{p-1}\}.$$

For $g, g' \in G$ er $g = a^i z$ og $g' = a^{i'} z'$, og $gg' = a^i z a^{i'} z' = z a^i a^{i'} z' = z a^{i'} a^i z' = a^{i'} z' a^i z = g'g$, så at G er abelsk (og $\mathrm{ord}(G) = p^2$) □

Sætning. <u>Der findes to gruppetyper af orden p^2,</u> nemlig $\dot{Z}/p^2\dot{Z}$ og $\dot{Z}/p\dot{Z} \times \dot{Z}/p\dot{Z}$.

Bevis. Hvis der findes et element af orden p^2 er G cyklisk, og alts så isomorf med $\dot{Z}/p^2\dot{Z}$. I modsat fald er alle elementer $\neq e$ af orden p. Er a af orden p, er $A = \{e, a, \ldots, a^{p-1}\}$ normal deler, og der findes $b \notin A$. Nu er $G/A = \{\bar{e}, \bar{b}, \ldots, \bar{b}^{p-1}\}$, da G/A har orden p. For $g \in G$ findes β, så at $\bar{g} = \bar{b}^\beta$: $g = b^\beta a^\alpha$. Afbildningen $g \to (\alpha, \beta)$ er $: G \to \dot{Z}/p\dot{Z} \times \dot{Z}/p\dot{Z}$, den er surjektiv, og derfor også bijektiv, og da b's orden er p er det en homomorfi, altså $G \cong \dot{Z}/p\dot{Z} \times \dot{Z}/p\dot{Z}$.

Oversigt over grupper af endelig orden ≤ 23:

Orden	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Antal	1	1	1	2	1	2	1	5	2	2	1	5	1	2	1	14	1	5	1	5	2	2	1
ikke-abelske	0	0	0	0	0	1	0	2	0	1	0	3	0	1	0	9	0	3	0	3	1	1	0

<u>Grupper af orden 6.</u>

Vi kender 2: Den cykliske $\dot{Z}/6\dot{Z}$, og trekants-flytning gruppen D_3. Vi vil vise, at der ikke findes andre.

1) <u>G er abelsk:</u> Hvis der findes et element af orden 6 er G cyklisk. Hvis alle elementer er af orden 2, og $a \neq e$, da er $Q = \{e, a\}$ en normaldeler, og $b = b^2 b = b^3 = b^{(G:Q)} \in Q$ for ethvert $b \in G$, hvilket er en modstrid. Hvis alle elementer er af orden 3, og $a \neq e$,

da er $\mathcal{S} = \{e,a,a^2\}$ en normaldeler, og $b = b^3b = (b^2)^2 = (b^2)^{(\mathcal{O}:\mathcal{S})}$ for ethvert $b \in \mathcal{O}$, hvilket er en modstrid. Vi kan således finde a af orden 2, og b af orden 3, men så er ab af orden 6, hvilket let indses, altså $\mathcal{O}$ cyklisk.

2) $\mathcal{O}$ er ikke abelsk: Der kan ikke findes elementer af orden 6, da $\mathcal{O}$ så var cyklisk. Iflg. ovenstående kan ikke alle elementer være af orden 3 (en undergruppe af orden 3 har index 2 og er altså normal). Heller ikke kan alle elementer være af orden 2, da $\mathcal{O}$ i så fald vær abelsk. Vi vælger a af orden 3 og b af orden 2. $\mathcal{O}$'s elementer er da $\{e,a,a^2,b,ab,a^2b\}$ Problemet er at bestemma ba. Da $ba \notin \{e,a,a^2\}$ som er normaldeler i $\mathcal{O}$, må $ba \in \{b,ab,a^2b\}$, sideklassen. Nu er $ba \neq b$, og $ba \neq ab$ (da ab ellers var af orden 6) altså $ba = a^2b$. Heraf følger let, at gruppestrukturen er entydigt bestemt, og da D_3 opfylder betingelserne, er der netop én ikke abelsk gruppe af orden 6.

Grupper af orden 8.

1) $\mathcal{O}$ er abelsk: Vi kan angive 3, nemlig $\dot{Z}/8\dot{Z}$, $\dot{Z}/4\dot{Z} \times \dot{Z}/2\dot{Z}$ og $\dot{Z}/2\dot{Z} \times \dot{Z}/2\dot{Z} \times \dot{Z}/2\dot{Z}$. Der er ikke flere! Er nemlig $\mathcal{O}$ cyklisk, er $\mathcal{O} \cong \dot{Z}/8\dot{Z}$. Er alle elementer af orden 2, vælges $A \neq B$; $\{E,A,B,AB\}$ er da en undergruppe af orden 4. Tilhører C ikke denne, får vi sideklassen $\{C,AC,BC,ABC\}$ d: $\mathcal{O} = \{A^\alpha B^\beta C^\gamma \mid \alpha,\beta,\gamma \bmod 2\}$ Hvis der findes et element A af orden 4 er $\mathcal{S} = \{E,A,A^2,A^3\}$ en undergruppe, og for $B \notin \mathcal{S}$ er $\{B,AB,A^2B,A^3B\}$ sideklassen. Nu er $B^2 = B^{(\mathcal{O}:\mathcal{S})} \in \mathcal{S}$ $B^2 \neq A$ og $B^2 \neq A^3$, da B ellers havde orden 8. ~~Endvidere er $B^2 \neq A^2$~~ Hvis $B^2 = A^2$, er $(A^3B)^2 = A^6B^2 = A^8 = E$, så vi kan antage, at $B^2 = E$. Følgelig er $\mathcal{O} = \{A^\alpha B^\beta \mid \alpha \bmod 4,\ \beta \bmod 2\}$.

2) $\mathcal{O}$ er ikke abelsk: Vi kan angive 2, nemlig gruppen af alle flytninger, der fører et kvadrat over i sig selv, D_4, bestående af ident. tre drejninger og fire spejlinger, samt kvaterniongruppen $\{\pm 1,\pm i,\pm j,\pm k\}$, hvor 1,i,j,k betegner kvaternionenhederne. Disse to grupper er forskellige, da der i flytningsgruppen findes 5 elementer af orden 2, hvorimod kun -1 har orden 2 i kvaterniongruppen. Der er ikke flere end disse to! Elementerne i en ikke abelsk gruppe $\mathcal{O}$ må have orden 2 og 4, og ikke alle elementer kan have orden 2, da $\mathcal{O}$ i så fald var abelsk. Er A af orden 4, og $\mathcal{S} = \{E,A,A^2,A^3\}$ da er $\mathcal{S}$ en normaldeler. Er $B \notin \mathcal{S}$, er $\mathcal{O} = \{E,A,A^2,A^3,B,AB,A^2B,A^3B\}$. Da $(\overline{BA}) = (\overline{B})$ er $BA \in \{B,AB,A^2B,A^3B\}$. Nu er $BA \neq B$, og $BA \neq AB$ (da $\mathcal{O}$ ellers var abelsk), og $BA \neq A^2B$ (da vi ellers havde $BAB^{-1} = A^2$, hvor BAB^{-1} har orden 4 og A^2 har orden 2). Følgelig er $BA = A^3B$. Vi har $B^2 = B^{(\mathcal{O}:\mathcal{S})} \in \mathcal{S}$, og $B^2 \neq A$, $B^2 \neq A^3$, da B ellers var af orden 8. $B^2 = E$ giver flytningsgruppen D_4 og $B^2 = A^2$ giver kva-

terniongruppen.

Sætning. I en ikke abelsk gruppe af orden p^3, er ord($\mathcal{Z}$) = p, og $\mathcal{G}' = \mathcal{Z}$.

Bevis. Vi har ord($\mathcal{Z}$) = p eller p^2. Hvis ord($\mathcal{Z}$) = p^2, er ($\mathcal{G}:\mathcal{Z}$) = p, så at $\mathcal{G}/\mathcal{Z}$ er cyklisk, og dermed $\mathcal{G}$ abelsk. Følgelig er ord($\mathcal{Z}$) = p. Af ($\mathcal{G}:\mathcal{Z}$) = p^2 følger nu, at $\mathcal{G}/\mathcal{Z}$ er abelsk, altså $\mathcal{Z} \supset \mathcal{G}'$, og da $\mathcal{G}/\mathcal{E} = \mathcal{G}$ ikke er abelsk, må endelig $\mathcal{G}' = \mathcal{Z}$ ∎

Gruppen af flytninger, der bringer en regulær n-kant over i sig selv, består af n drejninger, og n spejlinger og kaldes diedergruppen D_n. D_n er ikke abelsk, thi er A drejningen på $\frac{2\pi}{n}$ og B en spejling, er $BA = A^{-1}B$.

Sætning. Der findes netop 2 grupper af orden 2p, (p primtal), nemlig den cykliske gruppe $\mathbb{Z}/2p\mathbb{Z}$ og diedergruppen D_p.

Bevis. Vi ved, at de findes, og skal altså vise, at der ikke findes andre grupper, .

1) $\mathcal{G}$ er abelsk: Hvis alle elementer har orden p, og $a \neq e$, er $\mathcal{P} = \{e,a,\ldots,a^{p-1}\}$ af index 2, så at $b^2 \in \mathcal{P}$ for $b \in \mathcal{G}$, men så er også $b = b^p b = b^{p+1} = (b^2)^{\frac{p+1}{2}} \in \mathcal{P}$ for alle $b \in \mathcal{G}$, hvilket er en modstrid. Hvis alle elementer har orden 2, og $a \neq e$, er $\mathcal{P} = \{e,a^{\frac{p+1}{2}}\}$ en normaldeler af index p, så $b = (b^2)^p b = b^p b^{p+1} = b^p (b^2)^{\frac{p+1}{2}} = b^p \in \mathcal{P}$ for alle $b \in \mathcal{G}$, hvilket er en modstrid. Dette viser, at vi kan vælge a af orden p, og b af orden 2, og det ses nu, at ab har orden 2p.

2) $\mathcal{G}$ er ikke abelsk: Intet element er da af orden 2p, og ikke alle elementer kan være af orden 2. Er A et element af orden p, har $\mathcal{P} = \{E,A,\ldots,A^{p-1}\}$ index 2, og er altså normal. For $B \notin \mathcal{P}$ er $B^2 \in \mathcal{P}$, og $B^p = B(B^2)^{(p-1)/2} \in B\mathcal{P}$, så at $B^p \notin \mathcal{P}$. B har altså orden 2. På den anden side har alle elementer i $\mathcal{P} \setminus \{E\}$ orden p, idet: $B \notin \mathcal{P} \Leftrightarrow B^2 = E$. Sideklassen er $\mathcal{P}B = \{B,AB,A^2B,\ldots,A^{p-1}B\}$. Da $(BA) = (B)$, altså $BA \notin \mathcal{P}$, er $BA = A^\alpha B$, hvor $1 \leq \alpha \leq p-1$. Vi vil nu bestemme α: $\alpha \neq 1$, da $\mathcal{G}$ ellers var abelsk. $(AB)^2 = A(BA)B = A^{\alpha+1}B^2 = A^{\alpha+1}$. Endvidere $(AB)^3 = (AB)^2(AB) = A^{\alpha+1}AB = A^{\alpha+2}B$ og også $(AB)^3 = AB(AB)^2 = ABA^{\alpha+1} = A(BA)A^{\alpha+1} = AA^\alpha BA^\alpha = AA^\alpha(A^\alpha B)A^{\alpha-1} = \ldots = A^{1+(\alpha+1)\alpha}BA^{\alpha-\alpha} = A^{\alpha^2+\alpha+1}B$. Tilsammen: $A^{\alpha+2}B = A^{\alpha^2+\alpha+1}B$ eller $p \mid \alpha^2+\alpha+1-(\alpha+2) = (\alpha+1)(\alpha-1)$, og da $1 < \alpha \leq p-1$ fås $\alpha = p-1$. Efter at $BA = A^{p-1}B = A^{-1}B$ er bestemt, er hele gruppen bestemt, – og altså isomorf med D_p. ∎

Eksempel. De eneste endelige flytningsgrupper i planen er de cyk-

liske grupper C_n (bestående af de drejninger, der fører en regulær n-kant over i sig selv), samt diedergrupperne D_n.
Vi errindrer først om, at der til n punkter i planen findes netop ét, hvis afstandskvadratsum er mindst mulig. Er de n punkter nemlig givet ved $\underline{v}_1,\ldots,\underline{v}_n$, og sættes $\underline{v}^* = \frac{1}{n}\sum_\nu \underline{v}_\nu$ gælder jo for et vilkårligt $\underline{v}$, at $\sum_\nu(\underline{v}_\nu-\underline{v})^2 = \sum_\nu(\underline{v}_\nu-\underline{v}^*)^2 + n(\underline{v}^*-\underline{v})^2$.
Lad nu $\mathcal{G} = \{\sigma_1,\ldots,\sigma_n\}$ være en endelig flytningsgruppe af orden n. Vi vælger et vilkårligt punkt P. Til de n punkter $\sigma_1(P),\ldots,\sigma_n(P)$ findes ét punkt Q for hvilket afstandskvadratsummen er mundst mulig. For $\sigma\in\mathcal{G}$ har $\sigma(Q)$ (da σ er en flytning) samme afstande til punkterne $\sigma(\sigma_1(P)),\ldots,\sigma(\sigma_n(P))$, som Q til punkterne $\sigma_1(P),\ldots,\sigma_n(P)$, men da $\{\sigma\sigma_1,\ldots,\sigma\sigma_n\} = \mathcal{G}$ er $\{\sigma(\sigma_1(P)),\ldots,\sigma(\sigma_n(P))\} = \{\sigma_1(P),\ldots,\sigma_n(P)\}$, og da Q var entydigt bestemt, er $\sigma(Q) = Q$. Vi har således vist, at flytningerne $\sigma\in\mathcal{G}$ har et fælles fixpunkt, så $\mathcal{G}$ må bestå af den identiske afb., drejninger om fixpunktet og spejlinger i linier gennem fixpunktet.
$\mathcal{G}$ kan bestå af identiteten og én spejling, og bliver da diedergruppen D_1. Hvis $\mathcal{G}$ indeholder mere end én spejling, kan vi sammensætte to forskellige spejlinger, og ser da, at $\mathcal{G}$ også må indeholde drejninger. Vi kan nu betragte mængden C af alle drejninger i $\mathcal{G}$; det er oplagt en undergruppe. Lad os betragte drejningen v med mindst mulig positiv drejningsvinkel v. v er af formen $\frac{2\pi}{m}$. Nu vil også drejningerne $v,2v,\ldots,(m-1)v,mv$ = ident. tilhøre C, og på velkendt måde vises, at C ikke kan indeholde andre drejninger, altså $C = C_m$. Hvis $\mathcal{G} = C$ er vi færdige, og ellers findes spejlinger i $\mathcal{G}$. Lad l være spejlingsakse for en spejling l. En anden spejling l_w danner vinklen w med l. Sammensættes disse to spejlinger, fås en drejning med vinklen 2w eller -2w, så w er et multiplum af $\frac{1}{2}v$. Omvendt er sammensætning af spejlingen l og drejningen kv en spejling om en linie $l_{\frac{1}{2}kv}$ med vinklen $\frac{1}{2}kv$ med l. Hvis der altså er spejlinger med, er der n af dem, og samtlige flytninger i $\mathcal{G}$ fører en regulær n-kant over i sig selv, o: $\mathcal{G} = D_n$

PERMUTATIONSGRUPPER=

Sætning (Cayley). Enhver gruppe $\mathcal{O} = (M,\cdot)$ er isomorf med en transformationsgruppe af sin underliggende mængde, M.
Bevis. For $f\in\mathcal{O}$ defineres $f^*: M \to M$ ved $f^*(a) = fa$. f^* er bijektiv, og $f \to f^*$ er injektiv, og homomorf, da $(fg)^*(a) = (fg)a = f(ga) = f\cdot g^*(a) = f^*(g(a)) = f^*\circ g^*(a)$∎

En permutationsgruppe er en transformationsgruppe af en ende-

lig mængde. Af sætningen følger nu, at en endelig gruppe G af orden n er isomorf med en gruppe af premutationer af n elementer. Den fuldstændige transformationsgruppe for mængden $\{1,2,\ldots,n\}$ er af orden n!. Den kaldes den symmetriske gruppe af grad n og betegnes S_n. En gruppe af orden n er altså isomorf med en undergruppe i S_n.
En permutation $\sigma \in S_n$ skrives også $= \begin{pmatrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{pmatrix}$. Man undlader ofte her at skrive fixelementerne for σ.
En transposition er en permutation, hvor alle elementer på nær to er fixwelementer.
En permutation af formen $\begin{pmatrix} a_1 & a_2 & \cdots & a_{k-1} & a_k \\ a_2 & a_3 & & a_k & a_1 \end{pmatrix}$ kaldes en cykel, og betegnes også $(a_1,\ldots,a_k)$. Specielt skrives en transposition også (a_1,a_2)

Sætning. Enhver permutation $\sigma \in S_n$ er produkt af transpositioner.
Induktionsbevis. Klart rigtig for n = 2. Antag sætningen for $n-1$, og betragt $\sigma \in S_n$. Hvis $\sigma(n) = n$ er vi færdige, da vi så har $\sigma \in S_{n-1}$, og hvis $\sigma(n) \neq n$ er $(\sigma(n),n)$ en transposition, og for $\tau = (\sigma(n),n)\cdot\sigma$ er $\tau(n) = n$, og da $\sigma = (\sigma(n),n)\tau$ fås påstanden også i dette tilfælde. ∎

For $n \geq 3$ er fremstillingen ikke entydig, hvilket ses af $(a,b) = (a,c)\cdot(b,c)\cdot(a,c)$. Heraf

Tilføjelse. Enhver permutation i S_n er produkt af transpositioner af formen $(1,2), (1,3),\ldots,(1,n)$, og disse transpositioner udgør et minimalt frembringersystem for S_n.
Bevis. Klart i følge ovenstående.

Sætning. Enhver permutation i S_n er produkt af cykler med disjunkte elementer.
Bevis. Lad $\sigma \in S_n$, og sæt $M = \{a \mid \sigma(a) \neq a\}$. Vælg et $a \in M$, og lad k være den mindste positive exponent med $\sigma^k(a) = a$, da er $a,\sigma(a),\ldots,\sigma^{k-1}(a)$ forskellige, og altså elementer i M. Hvis de udgør hele M er vi færdige, da vi så har $\sigma = (a,\sigma(a),\ldots,\sigma^{k-1}(a))$. Ellers findes et b forskelligt fra $a,\sigma(a),\ldots,\sigma^{k-1}(a)$ og en til b svarende cykel $(b,\sigma(b),\ldots,\sigma^{m-1}(b))$, og det ses, at de to cykler har disjunkte elementer, c.s.v. ∎

Disjunkte cykler er åbenbart ombyttelige.

Af ovenstående får vi et nyt bevis for "transpositions"sætningen, thi ehvert cykel kan spaltes i transpositioner $(a_1,\ldots,a_k) = (a_k,a_1)(a_{k-1},a_1)\ldots(a_3,a_1)(a_2,a_1)$.

Vi betragter et sæt $(X_1,\ldots,X_n)$. Til hver permutation $\sigma \in S_n$ svarer en "permutation", også betegnet σ, af $(X_1,\ldots,X_n)$, defineret ved $\sigma(X_i) = X_{\sigma(i)}$, $i = 1,\ldots,n$. Sættes

$$\Delta = \prod_{i<j} (X_i - X_j)$$

da vil

$$\sigma(\Delta) = \prod_{i<j} (X_{\sigma(i)} - X_{\sigma(j)})$$

tilfredsstille

$$\sigma(\Delta) = \begin{cases} +\Delta \text{ hvis antallet af par } i<j, \text{ med } \sigma(i) > \sigma(j) \text{ er lige} \\ -\Delta \text{ hvis antallet af par } i \quad j, \text{ med } \sigma(i) > \sigma(j) \text{ er ulige.} \end{cases}$$

Ved $\sigma(\Delta) = \chi(\sigma)\Delta$ defineres en afbildning $\chi: S_n \longrightarrow \{1,-1\}$. Hvis $\chi(\sigma) = +1$ kaldes σ en lige permutation, og hvis $\chi(\sigma) = -1$ kaldes σ ulige.

Sætning. $\chi: S_n \longrightarrow \{1,-1\}$ er en homomorfi.

thi $(\sigma\tau)(\Delta) = \sigma(\tau(\Delta)) = \sigma(\chi(\tau)\Delta) = \chi(\tau)\sigma(\Delta) = \chi(\tau)\chi(\sigma)\Delta$, hvoraf $\chi(\sigma\tau) = \chi(\sigma)\chi(\tau)$. ∎

Korollar. De lige permutationer i S_n udgør en normal undergruppe, der kaldes den alternerende gruppe af grad n, og betegnes A_n.

For $n > 1$ har A_n orden $\frac{n!}{2}$, thi da en transposition er ulige, er χ i så fald surjektiv, så at $S_n/A_n \cong \{1,-1\}$, og dermed $\operatorname{ord}(A_n) = \frac{1}{2}\operatorname{ord}(S_n)$.

En cykel er lige, hvis den har et ulige antal elementer, og omvendt. Ethvert element i A_n er produkt af et lige antal transpositioner, altså også produkt af et lige antal af formen (1,a). Da (1,a)(1,a) = e, og (1,a)(1,b) = (1,b,a) slutter vi

Lemma. A_n frembringes af 3-cyklerne (1,b,a). = (1,2,a)(1,2,b)(1,2,b) (1 b
og dtg

Sætning. A_n er den eneste undergruppe i S_n af index 2.

Bevis. Har H index 2 i S_n, er ethvert kvadrat element i H. Da $(1,b,a)^3 = e$, er $(1,b,a) = (1,b,a)^3(1,b,a)^{-2} = (1,b,a)^{-2} \in H$, altså $H \supseteq A_n$, og dermed $H = A_n$ ∎

Eks. Eks. Bestem centrum i S_n. For n = 1,2 har vi $Z = S_n$. For $n \geq 3$ findes $a \neq 1$, og $b \neq 1,a$, men så er $\binom{1\cdots}{a\cdots} \cdot (a,b) = \binom{1\cdots}{a\cdots}$ og $(a,b)\cdot\binom{1\cdots}{a\cdots} = \binom{1\cdots}{b\cdots}$, hvilket viser. at ingen permutation af formen $\binom{1\cdots}{a\cdots}$ ligger i Z. Det følger nu, at $Z = E$.

Sætning. Centrum i S_n er $Z = E$ for $n \geq 3$.

En undergruppe, P, i S_n kaldes transitiv, hvis der til ethvert

findes $\sigma \in P$, så at $\sigma(i) = j$.

Eksempel. For en transitiv undergruppe P i S_n gælder:

1) P's orden er et multiplum af n
2) P indeholder (for $n > 1$) mindst én permutation uden fixelementer
3) Hvis P er abelsk, findes til hvert par (i,j) netop ét $\sigma \in P$, så at $\sigma(i) = j$.

Bevis. 1) Vi sætter $H_1 = \{\sigma \in P | \sigma(1) = 1\}$. H_1 er en undergruppe i P. For $\sigma, \tau \in P$ er $\sigma(1) = \tau(1) \Leftrightarrow \sigma\tau^{-1}\sigma(1) = 1 \Leftrightarrow \sigma \underset{v}{\sim} \tau$ (H_1). Da der for hvert j findes $\sigma \in P$ med $\sigma(1) = j$, er der n venstreækvivalensklasser, altså $\text{ord}(P) = n \cdot \text{ord}(H_1)$

2) Lad $n > 1$ og sæt $H_j = \{\sigma \in P | \sigma(j) = j\}$, da er $\text{ord}(H_j) = \frac{1}{n}\text{ord}(P)$. Hvis hvert $\sigma \in P$ havde et fixpunkt, var $P = \bigcup_{j=1}^{n} H_j$, og ovenstående ville da medføre, at H_j'erne var disjunkte, i modstrid med, at identiteten tilhører dem alle.

3) Antag P er abelsk, og lad $\sigma \in H_j$. Til vilkårligt a findes $\rho \in P$ så at $\rho(j) = a$, men så er $\sigma(a) = \sigma\rho(j) = \rho\sigma(j) = \rho(j) = a$, altså $\sigma = e$, og $H_j = E$. Er $\sigma(a) = \tau(a)$, er $\tau^{-1}\sigma \in H_a$, altså $\tau = \sigma$ (og $\text{ord}(P) = n\ \text{ord}(H_j) = n$. ∎

Er M en mængde, $\mathcal{G}$ en transformationsgruppe af M, og $\alpha \in M$, kaldes $H_\alpha = \{\varphi \in \mathcal{G} | \varphi(\alpha) = \alpha\}$ for stabilitetsgr. for α. Det er øjensynlig en undergruppe i $\mathcal{G}$.

Sætning. En normaldeler i en transformationsgruppe, $\mathcal{G}$, der indeholder en stabilitetsgruppe H_α, må indeholde alle $H_{\sigma(\alpha)}$, $\sigma \in \mathcal{G}$, thi $\sigma H_\alpha \sigma^{-1} = H_{\sigma(\alpha)}$.

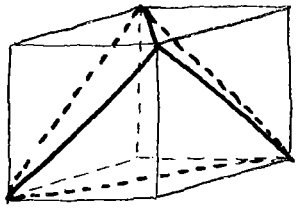
Heksaedergruppen (oktaedergruppen $\mathcal{O}$) er gruppen O af alle drejninger i rummet, der fører en terning over i sig selv.
Drejningsaksernе må gå gennem terningens centrum.
Aksen kan gå gennem (de 4) par af modstående hjørner, drejninger
på $\begin{matrix}120^\circ\\240^\circ\end{matrix}$ i alt 4×2
Aksen kan gå gennem midten af (de 6) par af modstående kanter,
drejning på 180° i alt 6×1
Aksen kan gå gennem midten af (de 3) par af modstående sider, drejninger på $\begin{matrix}90^\circ\\180^\circ\\270^\circ\end{matrix}$ i alt 3×3
Drejningen er identiteten i alt 1
Hexaedergruppens orden er altså 24.

Hver drejning giver anledning til en permutation af diagonalerne fra modstående hjørner/
vi har altså en afbildning $\cdot : O \to S_4$. Kernen består af de drejninger, der fører alle diagonaler over i sig selv, hvilket klart kun identiteten gør, altså

$$\underline{\text{Heksaedergruppen}} \cong S_4,$$

da S_4 har $4! = 24$ elementer.

I terningen kan indskrives et tetraeder; der findes altså en undergruppe i , bestående af de drejninger, der fører tetraederet over i sig selv.



Disse drejninger $\begin{matrix}120^\circ\\240^\circ\end{matrix}$ om hjørnediagonalerne, drejninger 180° om om sidediagonalerne, samt ident, i alt $4\times2 + 3\times1 + 1 = 12$ drejninger (som altså må udgøre <u>tetraedergruppen</u>, T) Da A_4 er den eneste undergruppe af orden 12 i S_4, er altså

$$\text{Tetraedergruppen} \cong A_4.$$

(Det kan naturligvis også direkte vises, at de til tetraedergruppen hørende permutationer af hjørnerne alle er lige)
Ved drejninger af terningen går terningens sidefladediagonaler over i hinanden; en drejning giver således anledning til en permutation af disse 3 diagonaler, altså en afbildning $S_4 \to S_3$, som let ses af være surjektiv. Kernen, V, kaldet Viergruppen, er isomorf med D_2, altså

$$E \lhd V \lhd A_4 \lhd S_4.$$

Tetraedergruppen A_4 og Viergruppen V er de eneste ikke trivielle normaldelere i S_4: Vi bemærker først, at hvis σ,τ er drejninger på 180° om en sidefladediagonal (altså elementer i V), da er $\sigma = x\sigma x^{-1}$ for en passende drejning om en kantdiagonal. For de øvrige drejningers vedkommende bemærker vi blot, at den af en sådan drejning frembragte cykliske undergruppe er stabilitetsgruppe i O.
En normaldeler må følgelig indeholde

$$4\times\begin{Bmatrix}2\\0\end{Bmatrix} + 6\times\begin{Bmatrix}1\\0\end{Bmatrix} + 3\times\begin{Bmatrix}3\\1\\0\end{Bmatrix} + 1$$

elementer, og her er $4\times2 + 0 + 3\times1 + 1 = 12$ og $0 + 0 + 3\times1 + 1 = 4$ de eneste muligheder for ikke trivielle undergrupper.
S_4's kommutatorgruppe er enten A_4 eller V, men da $S_4/V \cong S_3$, der ikke er abelsk, er kommutatorgruppen A_4. V er den eneste ikke trivielle normaldeler i A_4, thi en normaldeler i A_4 må indeholde

$4\times\binom{2}{0} + 3\times\binom{1}{0} + 1$ elementer, og her er $3\times1 + 1 = 4$ den eneste mulighed for en ikke triviel undergruppe. Da A_4/V har orden 3, og derfor er abelsk, er A_4's kommutatorgruppe altså V. V er abelsk, og dermed V's kommutatorgruppe = E, altså

$$0 = S_4 \quad 0' = A_4 \quad 0'' = V \quad 0''' = E.$$

Ikosaedergruppen (Dodekaedergruppen) I

er gruppen af drejninger i rummet, der fører et ikosaeder over i sig selv.

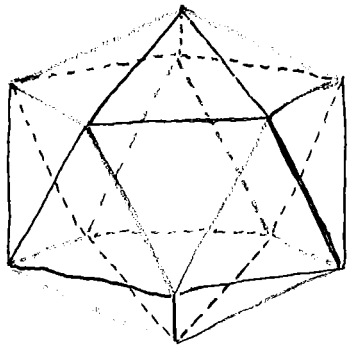
Aksen kan gå gennem (de 6) par af modstående hjørner, drejninger på $1,2,3,4 \times \frac{2\pi}{5}$ i alt 6×4

Aksen kan gå gennem (de 15) par af modstående kanter, drejninger på π i alt 15×1

Aksen kan gå gennem (de 10) par af modstående sider, drejninger på $1,2 \times\frac{2\pi}{3}$ i alt 10×2

Drejningen er identiteten i alt 1.

Ikosaedergruppens orden er altså 60.



Kanterne kan deles op i 5 grupper af 3 på hinanden vinkelrette par af modstående kanter. Til hver drejning i I svarer en permutation af disse grupper, så vi har en afbildning : $I \to S_5$, som øjensynlig er injektiv. Nu er en

drejning på $1,2,3,4 \times \frac{2\pi}{5}$ en 5-cykel

drejning på π er produkt af to transp.

drejning på $1,2 \times\frac{2\pi}{3}$ en 3-cykel,

så permutationerne er alle lige. Da A_5 har $\frac{1}{2}\cdot5! = 60$ elementer, har vi altså

Ikosaedergruppen $\cong A_5$.

Vi viser nu, at I er simpel: Ved hjælp af stabilitetsgrupper får vi nemlig for elementantallet i en normaldeler:

$$6\times\binom{4}{0} + 15\times\binom{1}{0} + 10\times\binom{2}{0} + 1,$$

hvilket kun giver trivielle divisorer i 60. Heraf ses, at $A_5' = A_5$, og dermed

$$S_5' = A_5 \quad A_5' = A_5 \ , \ \ldots$$

Bemærk. Det kan vises, at der af egentlige flytningsgrupper i rummet kun findes de cykliske grupper C_n, diedergrupperne D_n, samt tetraedergruppen T, hexaedergruppen O og Ikosaedergruppen I.

Sætning (Galois). $\underline{A_n \text{ er simpel for alle } n \geq 5.}$

Bevis. (L.Raeder). Lad $N \neq E$ være en normaldeler i A_n.

1) Vi viser først, at N indeholder en permutation af formen

(*) $(a,b)(c,d)$, a,b,c,d indb. forsk.

Lad $\nu \neq e$ være et element i N, da er $\alpha^{-1}\nu^{-1}\alpha \in N$, så at også $\alpha^{-1}\nu^{-1}\alpha\nu \in N$ for alle $\alpha \in A_n$. Vi tænker os nu ν opløst i produkt af disjunkte cykler. Der findes da flg. muligheder: I) produktet indeholder en cykel af længde > 3, II) der findes en cykel af længde 3, og produktet indeholder flere faktorer, III) ν er selv en 3-cykel, og IV) produktet består af transpositioner (bemærk at produktet da indeholder mindst 2 transpositioner, da er lige)

	ν	α	$\alpha^{-1}\nu^{-1}\alpha\nu$
I:	$(a,b,c,d,\ldots)(\ldots)\ldots$	(b,c,d)	(a,d,c)
II:	$(a,b,c)(d,e,\ldots)\ldots$	(b,c,e)	(a,e,c,b,d)
III:	(a,b,c)	(b,c,d)	$(a,d)(b,c)$
IV:	$(a,b)(c,d)\ldots$	(a,b,c)	$(a,d)(b,c)$

I ovenstående skema er de forskellige muligheder for ν opskrevet, og produktet $\alpha^{-1}\nu^{-1}\alpha\nu$ er udregnet for et passende $\alpha \in A_n$. Det ses, at dette produkt i tilfældene III,IV er af den ønskede form, i tilfælde I af formen III, og i tilfælde II af formen I. Hermed er 1) vist.

2) Vi viser nu, at N indeholder enhver permutation af formen (*). Antag fx, at $(1,2)(3,4) \in N$, og lad a,b,c,d, være indb. forsk. Af

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ b & a & c & d \end{pmatrix} = (a,b)\begin{pmatrix} 1 & 2 & 3 & 4 \\ a & b & c & d \end{pmatrix} = (a,b)\tau$$

ses, at enten σ eller τ er lige (d: elementer i A_n), og hvis fx $\tau \in A_n$ får vi

$$(a,b)(c,d) = \tau\{(1,2)(3,4)\}\tau^{-1} \in N$$

3) Beviset fuldføres nu ved, at vi viser, at enhver permutation $\tau \in A_n$ for $n \geq 5$ er produkt af elementer af formen (*): Vi ved af τ kan opløses i et lige antal transpositioner, altså i et vist antal par af transpositioner. Nu er $(a,b)(a,b) = \text{ident.}$, $(a,b)(c,d)$ er af formen (*), og er a,b,c forskellige, findes $x \neq y$, forskellige fra a,b,c (da $n \geq 5$), men så er $(a,b)(b,c) = \{(a,b)(x,y)\} \circ \{(x,y)(b,c)\}$ et produkt af elementer af formen (*) ∎

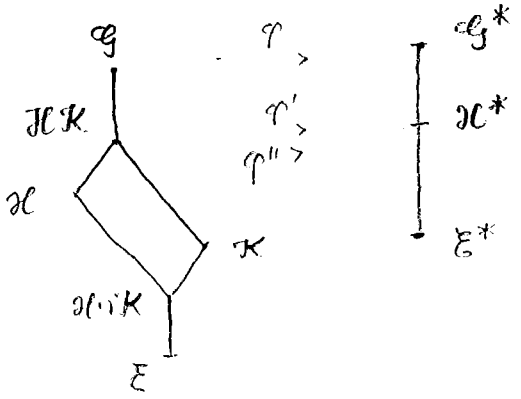
Korollar. <u>For $n \geq 5$ er A_n den eneste ikke trivielle normaldeler i S_n.</u>

Bevis. Er $N \lhd S_n$ er $A_n \cap N \lhd A_n$, hvoraf $A_n \cap N = A_n$ eller $A_n \cap N = E$. Hvis $A_n \cap N = A_n$, er $N = A_n$ eller $N = S_n$, og hvis $A_n \cap N = E$, er $N = E$, thi er $\sigma, \tau \in N$, og $\sigma, \tau \neq e$, er σ og τ ulige, så at $\sigma^{-1}\tau \in A_n$ og $\sigma^{-1}\tau \in N$, altså $\sigma = \tau$. Hvis $N = \{e, \sigma\}$, er $\tau^{-1}\sigma\tau \in N$ for alle $\tau \in S_n$. Er $\tau^{-1}\sigma\tau = e$ for et τ, er $\sigma = \tau e \tau^{-1} = e$, og er $\tau^{-1}\sigma\tau = \sigma$ for alle $\tau \in S_n$, er $\sigma \in Z$ og dermed $\sigma = e$ ∎

ISOMORFISÆTNINGER

Noethers første isomorfisætning. <u>Er $\mathcal{H}$ og $\mathcal{K}$ normaldelere i gruppen $\mathcal{G}$, er $\mathcal{HK}/\mathcal{K} \cong \mathcal{H}/\mathcal{H} \cap \mathcal{K}$.</u>

Bevis. Lad φ: $\mathcal{G} \longrightarrow \mathcal{G}/\mathcal{K} = \mathcal{G}^*$ være homomorfien med kerne $\mathcal{K}$. Nu er $\varphi(\mathcal{H}) = \varphi(\mathcal{HK})$, thi da $\mathcal{H} \subseteq \mathcal{HK}$, er $\varphi(\mathcal{H}) \subseteq \varphi(\mathcal{HK})$, og er $hk \in \mathcal{HK}$, er $\varphi(hk) = \varphi(h)\varphi(k) = \varphi(h)$, altså $\varphi(\mathcal{HK}) \subseteq \varphi(\mathcal{H})$. Vi sætter $\varphi(\mathcal{H}) = \varphi(\mathcal{HK}) = \mathcal{H}^*$. Da $\varphi' = \varphi_{|\mathcal{HK}} : \mathcal{HK} \to \mathcal{H}^*$ er surjektiv, er $\mathcal{H}^* \cong \mathcal{HK}/\mathrm{Ker}\,\varphi'$ og da $\varphi'' = \varphi_{|\mathcal{H}} : \mathcal{H} \to \mathcal{H}^*$ er surjektiv, er $\mathcal{H}^* \cong \mathcal{H}/\mathrm{Ker}\,\varphi'' = \mathcal{H}/\mathcal{H} \cap \mathcal{K}$. Altså $\mathcal{HK}/\mathcal{K} \cong \mathcal{H}^* \cong \mathcal{H}/\mathcal{H} \cap \mathcal{K}$



tilføjelse. <u>Det ses, at det er nok at forlange, at $\mathcal{K}$ er normaldeler i $\mathcal{G}$.</u>

Noethers anden isomorfisætning. <u>Lad $\mathcal{N}$ være normaldeler i gruppen $\mathcal{G}$, og lad φ: $\mathcal{G} \to \mathcal{G}^*$ være en surjektiv homomorfi med kernen $\mathcal{N}$, da vil $\mathcal{H} \to \varphi\mathcal{H}$ definere en entydig forbindelse mellem undergrupperne mellem $\mathcal{N}$ og $\mathcal{G}$ og undergrupperne i $\mathcal{G}^*$, endda således, at normaldeler svarer til formaldeler og omvendt, og så at tilsvarende faktorgrupper er isomorfe</u> (altså hvis $\mathcal{N} \subseteq \mathcal{H} \lhd \mathcal{G}$ er $\mathcal{G}/\mathcal{S} \cong \mathcal{G}^*/\varphi\mathcal{H}$, hvilket skrives $\mathcal{G}/\mathcal{H} = (\mathcal{G}/\mathcal{N})/(\mathcal{H}/\mathcal{N})$)

Bevis. Antag at $\mathcal{N} \subseteq \mathcal{H} \subseteq \mathcal{G}$, da er $\varphi^{-1}(\varphi\mathcal{H}) = \mathcal{H}$, thi $\varphi^{-1}(\varphi\mathcal{H}) \supseteq \mathcal{H}$, og er $g \in \varphi^{-1}(\varphi\mathcal{H})$, er $\varphi(g) = \varphi(h)$, så $gh^{-1} \in \mathcal{N} \subseteq \mathcal{H}$, hvoraf $g = (gh^{-1})h \in \mathcal{H}$.

Dette viser, at $\mathcal{H} \to \varphi\mathcal{H}$ er injektiv.
Lad $\mathcal{K}^*$ være en undergruppe i $\mathcal{G}^*$; da er $\varphi^{-1}(\mathcal{K}^*)$ en undergruppe i $\mathcal{G}$, $\mathcal{N} \subseteq \varphi^{-1}(\mathcal{K}^*) \subseteq \mathcal{G}$, og $\varphi(\varphi^{-1}(\mathcal{K}^*)) = \mathcal{K}^*$, hvilket viser, at $\varphi\colon \mathcal{K} \to \varphi\mathcal{K}$ er surjektiv. $\mathcal{H} \to \varphi\mathcal{H}$ er således bijektiv.
$\mathcal{H} \lhd \mathcal{G} \iff \varphi\mathcal{H} \lhd \mathcal{G}^*$, thi $g^*\varphi(h)g^{*-1} = \varphi(ghg^{-1}) \in \varphi\mathcal{H}$ viser "$\Rightarrow$", og af $\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1} \in \varphi(\mathcal{H})$, ses $ghg^{-1} \in \varphi^{-1}(\varphi\mathcal{H}) = \mathcal{H}$, hvoraf "$\Leftarrow$".
Lad nu $\mathcal{N} \subseteq \mathcal{H} \lhd \mathcal{G}$, og $\varkappa\colon \mathcal{G}^* \to \mathcal{G}^*/\varphi\mathcal{H}$ være den kannoniske homomorfi, da er $\varkappa \circ \varphi\colon \mathcal{G}$ på $\mathcal{G}^*/\varphi\mathcal{H}$ en homomorfi med kernen $\mathcal{H}$: $\mathcal{G}^*/\varphi\mathcal{H} \cong \mathcal{G}/\mathcal{H}$.

En endelig række af undergrupper i $\mathcal{G}$: $\mathcal{G} = \mathcal{G}_0, \mathcal{G}_1, \ldots, \mathcal{G}_r = \mathcal{E}$, hvor $\mathcal{G}_{i-1} \lhd \mathcal{G}_i$ $i = 1.2, \ldots, r-1$, kaldes en normalrække:

$$(*) \qquad \mathcal{G} = \mathcal{G}_0 \rhd \mathcal{G}_1 \rhd \ldots \rhd \mathcal{G}_{r-1} \rhd \mathcal{G}_r = \mathcal{E}.$$

Rækken kaldes en absolut normalrække, hvi alle $\mathcal{G}_i$ er normaldelere i $\mathcal{G}$. Faktorgrupperne $\mathcal{G}_0/\mathcal{G}_1, \ldots, \mathcal{G}_{r-1}/\mathcal{G}_r$ kaldes rækkens faktorer, og r (= antallet af faktorer) kaldes rækkens længde. Rækken siges at være uden gentagelser, hvis $\mathcal{G}_{i-1} \subset \mathcal{G}_i$, $i = 1, \ldots, r$, altså hvis faktorerne $\neq \mathcal{E}$. En normalrække

$$\mathcal{G} = \mathcal{H}_0 \rhd \mathcal{H}_1 \rhd \ldots \rhd \mathcal{H}_s = \mathcal{E}$$

kaldes en forfining af $(*)$, hvis hvert $\mathcal{G}_i$ = et H_j.
En kompositionsrække er en normalrække uden gentagelser og uden ægte forfininger.

Sætning. En normalrække er en kompositionsrække, hvis og kun hvis faktorerne er simple grupper $\neq \mathcal{E}$.
følger straks af anden isomorfisætning.

Sætning. Enhver endelig gruppe har en kompositionsrække

Eks. $\dot{Z}$ har ingen kompositionsrække.

To normalrækker kaldes isomorfe, hvis de tilsvarende faktorer (bortset fra rækkefølge) er isomorfe.

Eks. $\dot{Z}/6\dot{Z} \rhd \dot{Z}/2\dot{Z} \rhd 0$ og $\dot{Z}/6\dot{z} \rhd \dot{Z}/3\dot{Z} \rhd 0$ er isomorfe normalrækker.

Sætning. (Jordan - Hölder) Lad $\mathcal{G}$ være en gruppe, der har en kompositionsrække, da er hvilkesomhelst to kompositionsrækker isomorfe og har specielt samme længde.

en umiddelbar følge af

Schreiers forfiningssætning. To vilkårlige normalrækker, $\mathcal{G} \rhd \mathcal{G}_1$

$G_2 \triangleright \dots \triangleright G_r = E$ og $G \triangleright H_1 \triangleright H_2 \triangleright \dots \triangleright H_s = E$ har isomorfe forfininger.

Beviset føres ved induktion i tre skridt: 1) sætningen vises for r = 1 og s = 1 2) Hvis sætningen gælder for s = 2 og r, da også for r+1 3) Hvis sætningen gælder for s og alle r, da også for s+1 og alle r.

1) intet at bevise.

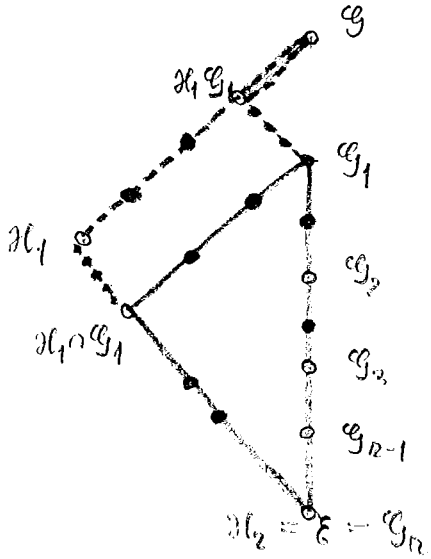
2) For s = 2 og r = 1 er sætningen klar. Vi betragter nu $G \triangleright G_1 \triangleright \dots \triangleright G_r =$ og $G \triangleright H_1 \triangleright H_2 = E$. Induktionsantagelsen kan anvendes på $G_1 \triangleright G_2 \triangleright \dots \triangleright G_r =$ og $G_1 \triangleright G_1 \cap H_1 \triangleright H_2 = E$; disse har altså isomorfe forfininger: $G_1 \triangleright \dots \triangleright G_2 \triangleright \dots \triangleright \dots \triangleright G_r = E$ og $G_1 \triangleright \dots \triangleright G_1 \cap H_1 \triangleright \dots \triangleright H_2 = E$. Da $H_1 G_1 / H_1\cong G_1 / G_1 \cap H_1$, viser anden isomorfisætning, at der til normalrækken $G_1 \triangleright \dots \triangleright G_1 \cap H$ findes en isomorf normalrække $H_1 G_1 \triangleright \dots \triangleright H_1$. Det følger nu, at

$$G \triangleright H_1 G_1 \triangleright G_1 \triangleright \dots \triangleright G_2 \triangleright \dots \triangleright G_r = E$$

og

$$G \triangleright H_1 G_1 \triangleright \dots \triangleright H_1 \triangleright H_1 \cap G_1 \triangleright \dots \triangleright H_2 = E$$

er isomorfe (vi benytter atter $H_1 G_1 / G_1 \cong H_1 / H_1 \cap G_1$), og de er forfininger af de oprindelige rækker.



3) Lad $G \triangleright G_1 \triangleright \dots \triangleright G_r = E$ og $G \triangleright H_1 \triangleright \dots \triangleright H_s = E$ være givne rækker, og antag sætningen for s-1 og alle r. I følge 2) har $G \triangleright G_1 \triangleright \dots \triangleright G_r = E$ og $G \triangleright H_1 \triangleright E$ isomorfe forfininger: $G \triangleright \dots \triangleright G_1 \triangleright \dots \triangleright \dots \triangleright G_r = E$ og $G \triangleright \dots \triangleright H_1 \triangleright \dots \triangleright E$. I følge induktionsantagelsen har $H_1 \triangleright \dots \triangleright E$ og $H_1 \triangleright H_2 \triangleright \dots \triangleright H_s = E$ isomorfe forfininger:

$$H_1 \triangleright \dots \triangleright \dots \triangleright E \quad \text{og} \quad H_1 \triangleright \dots \triangleright H_2 \triangleright \dots \triangleright \dots \triangleright H_s = E$$

Den første af disse rækker kan i følge 2.isomorfisætning "plantes

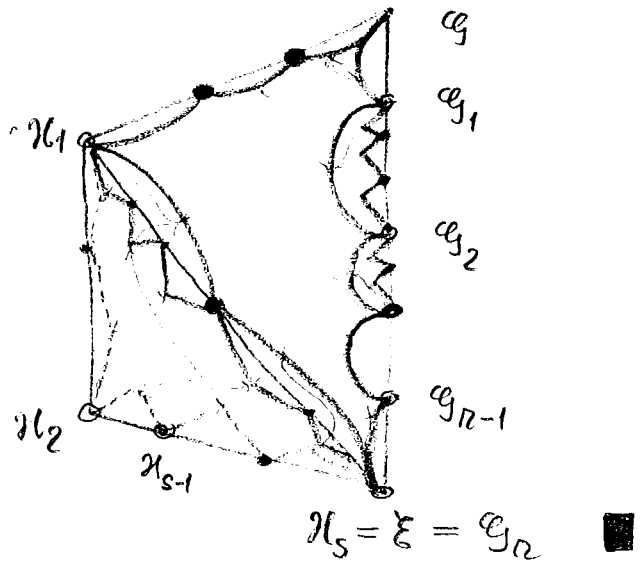
over" i $\mathcal{G}$-rækkens forfining, så at vi får en forfining af $\mathcal{G}$-rækken

$$\mathcal{G} \triangleright \ldots \triangleright \ldots \triangleright \mathcal{G}_1 \triangleright \ldots \triangleright \ldots \triangleright \ldots \triangleright \mathcal{G}_r = \mathcal{E},$$

der er isomorf med

$$\mathcal{G} \triangleright \ldots \triangleright \mathcal{H}_1 \triangleright \ldots \triangleright \mathcal{H}_2 \triangleright \ldots \triangleright \ldots \triangleright \mathcal{H}_s = \mathcal{E}$$

jfr. Hasse-diagrammet.



Korollar. Hvis $\mathcal{G}$ har en kompositionsrække, da har enhver normaldeler, $\mathcal{N}$, i $\mathcal{G}$ det også.
thi $\mathcal{G} \triangleright \mathcal{N} \triangleright \mathcal{E}$ kan forfines til en kompositionsrække for $\mathcal{G}$ ∎

Eks. Vis at $l(N)+l(N') = l(NN')+l(N \cap N')$ for normaldelere $N \trianglelefteq N'$ i G. En umiddelbar følge af formlen $l(G) = l(G/N) + l(N)$, som øjensynlig er rigtig.

En gruppe, $\mathcal{G}$, kaldes opløselig, hvis den har en normalrække med abelske faktorer.

Sætning. $\mathcal{G}$ er opløselig, hvis og kun hvis der findes s, så at $\mathcal{G}^{(s)} = \mathcal{E}$.

Bevis. Lad $\mathcal{G} \triangleright \mathcal{G}_1 \triangleright \ldots \triangleright \mathcal{G}_r = \mathcal{E}$ være en normalrække med abelske faktorer, da er $\mathcal{G}' \subseteq \mathcal{G}_1$, $\mathcal{G}'' \subseteq \mathcal{G}_1' \subseteq \mathcal{G}_2, \ldots, \mathcal{G}^{(r)} \subseteq \mathcal{G}_{r-1}' \subseteq \mathcal{G}_r = \mathcal{E}$.
Er omvendt $\mathcal{G}^{(s)} = \mathcal{E}$ for et vist s, er $\mathcal{G} \triangleright \mathcal{G}' \triangleright \ldots \triangleright \mathcal{G}^{(s)} = \mathcal{E}$ en (absolut) normalrække med abelske faktorer. ∎

Sætning. Hvis $\mathcal{G}$ er opløselig, er også undergrupper i $\mathcal{G}$ og homomorfe billeder af $\mathcal{G}$ opløselige.

Lemma. Lad $\mathcal{N}$ være en normaldeler i $\mathcal{G}$, så at $\mathcal{N}$ og $\mathcal{G}/\mathcal{N}$ er opløselige, da er også $\mathcal{G}$ opløselig.

Sætning. En opløselig gruppe, $\mathcal{G}$, der har en kompositionsrække, har en normalrække med cykliske faktorer,
thi en normalrække med abelske faktorer kan forfines til en kompositionsrække, der ligeledes får abelske faktorer, og da disse er simple, er de cykliske af primtalsorden

Eks. S_3 er opløselig, da $S_3' = A_3$, $S_3'' = A_3' = E$.
S_4 er opløselig, da $S_4' = A_4$, $S_4'' = A_4' = V$, $S_4''' = A_4'' = V' = E$.
S_5 er ikke opløselig, da $S_5' = A_5$, $S_5'' = A_5' = A_5$.

Lætning. S_n er ikke opløselig for $n \geq 5$.
Bevis. Det er nok at vise, at $A_n' = A_n$. Vi har $A_n' \subseteq A_n$, og er (a,b,c) en 3-cykel, vil $(a,b,c) \in A_n'$, thi der findes $\sigma = (d,b,a)$ og $\tau = (a,e,c) \in A_n$, hvor $d \neq e$ er forskellig fra a,b,c, men så er $\sigma^{-1}\tau^{-1}\sigma\tau = (a,b,d)(c,e,a)(d,b,a)(a,e,c) = (a,b,c) \in A_n'$, og da A_n frembringes af alle 3-cykler følger påstanden. ∎

ENDELIGE GRUPPER

Sætning. Enhver p-gruppe $\mathcal{G}$ er opløselig. $\text{ord}(\mathcal{G}) = p^n$.
Induktion efter n. Rigtig for n = 1,2, da $\mathcal{G}$ i så fald er abelsk. Antag sætningen for grupper af orden $\leq p^{n-1}$. Da $\text{ord}(\mathcal{G}/\mathcal{Z}) \leq p^n/p = p^{n-1}$ er $\mathcal{G}/\mathcal{Z}$ opløselig, og da $\mathcal{Z}$ er abelsk, og derfor opløselig, er også $\mathcal{G}$ opløselig. ∎

En gruppe $\mathcal{G}$ kaldes overopløselig, hvis den har en absolut normalrække med cykliske faktorer, og nilpotent, hvis der findes en absolut normalrække $\mathcal{G} \supseteq \mathcal{G}_1 \supseteq \ldots \supseteq \mathcal{G}_r = \mathcal{E}$, så at $\mathcal{G}_i/\mathcal{G}_{i+1} \subseteq \mathcal{Z}(\mathcal{G}/\mathcal{G}_{i+1})$. Af $\mathcal{G}_{r-1}/\mathcal{E} \subseteq \mathcal{Z}(\mathcal{G}/\mathcal{E})$ ses, at en nilpotent gruppe har ikke trivielt centrum.

Sætning. Enhver p-gruppe er nilpotent.
Induktion efter n. Rigtig for n = 1,2. Antages sætningen for grupper af orden $\leq p^{n-1}$, er $\mathcal{G}/\mathcal{Z}$ nilpotent. Da også $\mathcal{Z}$ er nilpotent, må også $\mathcal{G}$ være nilpotent. ∎

Følgende inklusioner er trivielt opfyldt:
$\mathcal{G}$ abelsk $\Rightarrow$ $\mathcal{G}$ nilpotent $\Rightarrow$ $\mathcal{G}$ overopløselig $\Rightarrow$ $\mathcal{G}$ opløselig.
Disse inklusioner er skarpe, thi 1) der findes ikke-abelske p-

grupper, 2) S_3 er overopløselig, da $S_3 \supseteq A_3 \supseteq E$ er en absolut normalrække med cykliske faktorer, men da $Z(S_3) = E$, er S_3 ikke nilpotent. 3) S_4 er opløselig, da $S_4 \rhd A_4 \rhd V \rhd E$ er en normalrække med abelske faktorer, men da dette er den eneste normalrække, og da V ikke er cyklisk, er S_4 ikke overopløselig.

Iwasawa har vist: $\mathcal{G}$ er overopløselig, hvis og kun hvis alle maximale kæder af undergrupper har samme længde. (fx. er $A_4 \supset V \supset \dot{Z}/2\dot{Z} \supset 0$ og $A_4 \supset A_3 \supset E$ maximale kæder af forskellig længde).

Feit & Thompson har vist: Enhver gruppe af ulige orden er opløselig (Pac.Jour. 13 (1963) p.775-1027)

SYLOW GRUPPER

Lemma. <u>En endelig abelsk gruppe, hvis orden har en primdivisor p, indeholder et element af orden p.</u>

Bevis. Induktion efter $\mathrm{ord}(\mathcal{G})$. Lad $\mathrm{ord}(\mathcal{G}) = p^r m$, $p \nmid m$, og antag sætningen for grupper af orden $< p^r m$. Er $\mathcal{H} \subset \mathcal{G}$ en maximal undergruppe, er $(\mathcal{G}:\mathcal{H}) = q$ et primtal, da $\mathcal{G}/\mathcal{H}$ er simpel.
Hvis $q \neq p$ er $p \mid \mathrm{ord}(\mathcal{H})$, og i flg.induktionsantagelsen findes et element i $\mathcal{H}$ af orden p. Hvis $q = p$ og $p \mid \mathrm{ord}(\mathcal{H})$ er vi færdige (som før), og hvis $p \nmid \mathrm{ord}(\mathcal{H})$, vælger vi $g \in \mathcal{G} \setminus \mathcal{H}$ Nu er $(g^{\mathrm{ord}(\mathcal{H})})^p = g^{\mathrm{ord}(\mathcal{G})} = e$, og $g^{\mathrm{ord}(\mathcal{H})} \neq e$, thi var $g^{\mathrm{ord}(\mathcal{H})} = e$ ville også $\textcircled{g}^{\mathrm{ord}(\mathcal{H})} = \textcircled{e}$, og også $\textcircled{g}^{p} = \textcircled{e}$; nu er $x\,\mathrm{ord}(\mathcal{H}) + yp = 1$ for passende x,y, men så er $\textcircled{g} = \textcircled{g}^{x\,\mathrm{ord}(\mathcal{H})+yp} = \textcircled{e}$, i modstrid med at $g \notin \mathcal{H}$. Vi har således vist, at $g^{\mathrm{ord}(\mathcal{H})}$ har orden p. ∎

Lemmaet følger også af
Sætning. <u>En endelig abelsk gruppes orden n er divisor i produktet af samtlige elementordener $h_{a_1} \ldots h_{a_n}$.</u>
Bevis. Lad $\mathcal{G} = \{a_1, \ldots, a_n\}$. $(a_1) \times \ldots \times (a_n)$ har da orden $h_{a_1} \ldots h_{a_n}$ og da der ved $(a_1^{\alpha_1}, \ldots, a_n^{\alpha_n}) \to a_1^{\alpha_1} \ldots a_n^{\alpha_n}$ defineres en surjektiv homomorfi, følger påstanden. ∎

Lad $\mathcal{G}$ være en endelig gruppe af orden $p^r m$, $p \nmid m$. En undergruppe $\mathcal{H}$ i $\mathcal{G}$ kaldes en <u>p-sylow-undergruppe</u>, hvis $\mathrm{ord}(\mathcal{H}) = p^r$.

1. Sylow-sætning. <u>En endelig gruppe $\mathcal{G}$, hvis orden har en primdivisor p, indeholder en p-Sylow-undergruppe</u>.
Bevis. Induktion efter $\mathrm{ord}(\mathcal{G})$. Lad $\mathrm{ord}(\mathcal{G}) = p^n m$, $p \nmid m$, og antag sætningen for grupper af orden $< p^n m$. Så enten indeholder $\mathcal{G}$ en ægte undergruppe $\mathcal{H}$ for hvilken $p \nmid (\mathcal{G}:\mathcal{H})$, men så er $\mathrm{ord}(\mathcal{H}) = p^n m'$

hvor $m' < m$, og $\mathcal{H}$ indeholder iflg. induktionsantagelsen en undergruppe af orden p^r. Eller: Alle ægte undergrupper har index deleligt med p. Deles $\mathcal{G}$ i konjugeretklasser B er $\text{ord}(\mathcal{G}) =$

$$p^n m = \sum_B \text{card}(B) = \sum_{B \subseteq \mathcal{Z}} \text{card}(B) + \sum_{B \cap \mathcal{Z} = \emptyset} \text{card}(B)$$
$$= \text{ord}(\mathcal{Z}) + \sum (\mathcal{G} : N_b).$$

Da $p \mid (\mathcal{G} : N_b)$ i følge den gjorte antagelse, er $p \mid \text{ord}(\mathcal{Z})$, og i følge lemma vil $\mathcal{Z}$ derfor indeholde en cyklisk undergruppe $\mathcal{C}$ af orden p. Hvis $r = 1$ er vi således færdige, og hvis $r > 1$, sættes $\mathcal{G}^* = \mathcal{G}/\mathcal{C}$. Da $\text{ord}(\mathcal{G}^*) = p^{r-1}m$, vil $\mathcal{G}^*$ iflg induktionsantagelsen indeholde en p-Sylow-undergruppe, $\mathcal{P}^*$, i $\mathcal{G}^*$, altså af orden p^{r-1}. og index m. Hertil svarer nu en undergruppe, $\mathcal{P}$, i $\mathcal{G}$ af index m, altså en p-Sylow-undergruppe i $\mathcal{G}$ ∎

Korollar. (Cauchy). <u>En endelig gruppe, hvis orden har en primdivisor p, har et element af orden p</u> (cfr.lemma)
thi enhver p-gruppe indeholder elementer af orden p. ∎

Er $\mathcal{P}$ en undergruppe i $\mathcal{G}$, og $g \in \mathcal{G}$, kaldes $g\mathcal{P}g^{-1}$ en med $\mathcal{P}$ <u>konjugeret</u> undergruppe. $N_{\mathcal{P}} = \{g \in \mathcal{G} \mid g\mathcal{P}g^{-1} = \mathcal{P}\}$ kaldes $\mathcal{P}$'s <u>normalisator</u>. Det er øjensynlig den største undergruppe i $\mathcal{G}$, der har $\mathcal{P}$ som normaldeler. Endvidere ses, at <u>antallet af de med $\mathcal{P}$ konjugerede undergrupper er $(\mathcal{G} : N_{\mathcal{P}})$</u>.
Lad nu $\mathcal{P}_1, \ldots, \mathcal{P}_{(\mathcal{G}:N_{\mathcal{P}})}$ være de med konjugerede undergrupper, og lad $\mathcal{S} \subseteq \mathcal{G}$ være en vilkårlig undergruppe i $\mathcal{G}$. $\mathcal{P}_i$ og $\mathcal{P}_j$ kaldes $\mathcal{S}$-ækvivalente, hvis der findes $s \in \mathcal{G}$, så at $P_i = sP_js^{-1}$.
Af $s_1\mathcal{P}_is_1^{-1} = s_2\mathcal{P}_is_2^{-1} \Leftrightarrow s_2^{-1}s_1\mathcal{P}_i(s_2^{-1}s_1)^{-1} = \mathcal{P}_i \Leftrightarrow s_2^{-1}s_1 \in \mathcal{S} \cap N\mathcal{P}_i$
$\Leftrightarrow s_2 \underset{v}{\sim} s_1 \ (\mathcal{S} \cap N_{\mathcal{P}_i})$, følger at antallet af konjugerede undergrupper i $\mathcal{S}$-ækvivalensklassen, der indeholder $\mathcal{P}_i$ er $(\mathcal{S} : \mathcal{S} \cap N\mathcal{P}_i)$.
Heraf følger også, at

$$(*) \qquad (\mathcal{G} : N_{\mathcal{P}}) = \sum_{\text{visse } \mathcal{P}_i} (\mathcal{S} : \mathcal{S} \cap N\mathcal{P}_i).$$

Lemma. <u>Er $\mathcal{P}$ en p-Sylow-undergruppe i $\mathcal{G}$ og $\mathcal{S}$ en vilkårlig p-undergruppe i $\mathcal{G}$, da er $\mathcal{S} \cap N_{\mathcal{P}} = \mathcal{S} \cap \mathcal{P}$.</u>
Bevis. Da $\mathcal{P} \subseteq N_{\mathcal{P}}$, er $\mathcal{S} \cap \mathcal{P} \subseteq \mathcal{S} \cap N_{\mathcal{P}}$. Sæt $\mathcal{S}^* = \mathcal{S} \cap N_{\mathcal{P}}$, da er $\mathcal{S}^* \subseteq N_{\mathcal{P}}$ og $\mathcal{P} \subseteq \mathcal{S}^*\mathcal{P} \subseteq N_{\mathcal{P}}$. Da $\mathcal{P} \lhd N_{\mathcal{P}}$, er $\mathcal{P} \lhd \mathcal{S}^*\mathcal{P}$, så i følge Noethers 2.isomorfisætning er $\mathcal{S}^*\mathcal{P}/\mathcal{P} = \mathcal{S}^*/\mathcal{P} \cap \mathcal{S}^*$. Da $\mathcal{P}$ er p-Sylow-undergruppe er $p \nmid (\mathcal{S}^*\mathcal{P}/\mathcal{P})$, men da $\mathcal{S}^* \subseteq \mathcal{S}$ er en p-gruppe er er $\mathcal{S}^*/\mathcal{P} \cap \mathcal{S}^*$ en p-gruppe, men så må $\mathcal{S}^* = \mathcal{P} \cap \mathcal{S}^*$, og dermed $\mathcal{S}^* \subseteq \mathcal{P}$, som sammenholdt med $\mathcal{S}^* \subseteq \mathcal{S}$ giver $\mathcal{S} \cap N_{\mathcal{P}} = \mathcal{S}^* \subseteq \mathcal{S} \cap \mathcal{P}$. ∎

2.Sylow-sætning. <u>I en gruppe $\mathcal{G}$ er alle p-Sylow-undergrupper indbyrdes konjugerede, og enhver p-undergruppe er indeholdt i en</u>

af dem.

Bevis. Lad $\mathcal{P}$ være en p-Sylow-undergruppe og $\mathcal{S}$ en p-undergruppe. Da $\mathcal{P} \subseteq N_{\mathcal{P}}$ gælder

$$p \nmid (\mathcal{G}:N_{\mathcal{P}}) = \sum{}^{*} (\mathcal{S}:\mathcal{S}\cap N_{\mathcal{P}_i}),$$

og da $\mathcal{S}$ er en p-gruppe, er højre side en sum af p-potenser. Relationen viser derfor, at der findes $\mathcal{P}_i$ så at $(\mathcal{S}:\mathcal{S}\cap N_{\mathcal{P}_i}) = p^0 = 1$. Iflg. lemma er $\mathcal{S}\cap N_{\mathcal{P}_i} = \mathcal{S}\cap\mathcal{P}_i$, så at $(\mathcal{S}:\mathcal{S}\cap\mathcal{P}_i) = 1$, o: $\mathcal{S} \subseteq \mathcal{P}_i$. Da $\mathcal{P}_i$ er konjugeret med $\mathcal{P}$, er $\mathcal{P}_i$ selv en p-Sylow-undergruppe. ∎

3.Sylow-sætning. Antallet af p-Sylow-undergrupper i $\mathcal{G}$ er divisor i $\mathcal{G}$'s orden, og $\equiv 1 \pmod{p}$.

Bevis. Lad $\mathcal{P}$ være en p-Sylow-undergruppe i $\mathcal{G}$ (1.Sylow-sætning). Iflg. 2.Sylow-sætning er antallet af p-Sylow-undergrupper i $\mathcal{G}$ netop antallet af de med $\mathcal{P}$ konjugerede, altså $= (\mathcal{G}:N_{\mathcal{P}})$, som er divisor i ord($\mathcal{G}$). Nu er

$$(\mathcal{G}:N_{\mathcal{P}}) = \sum{}^{*} (\mathcal{P}:\mathcal{P}\cap\mathcal{P}_i).$$

Da addenderne på højre side er potenser af p, og da $p \nmid (\mathcal{G}:N_{\mathcal{P}})$, er mindst én af addenderne $(\mathcal{P}:\mathcal{P}\cap\mathcal{P}_i) = 1$, men $(\mathcal{P}:\mathcal{P}\cap\mathcal{P}_i) = 1 \Longrightarrow \mathcal{P} \subseteq \mathcal{P}_i$, så at $\mathcal{P}_i = \mathcal{P}$. Følgelig er netop én af addenderne $= 1$, hvoraf den anden påstand. ∎

Lemma. Hvis $\mathcal{P}$ er den eneste p-Sylow-undergruppe i $\mathcal{G}$, da er $\mathcal{P}$ normaldeler.

Korollar 1. Enhver gruppe, $\mathcal{G}$, af orden $2p^n$ er opløselig.

Bevis. $\mathcal{G}$ indeholder en p-Sylow-undergruppe $\mathcal{P}$, som har index 2, og derfor er normal. Da $\mathcal{P}$ er opløselig, og da $\mathcal{G}/\mathcal{P}$ har orden 2, og derfor er abelsk og opløselig, er også $\mathcal{G}$ opløselig. ∎

Korollar 2. Enhver gruppe, $\mathcal{G}$, af orden pq er opløselig.

Bevis. Hvis $p = q$ er $\mathcal{G}$ endda abelsk. Antag $p < q$, og lad $\mathcal{Q}$ være en q-Sylow-undergruppe. Antallet af q-Sylow-undergrupper er 1, p,q eller pq, og af formen 1+qh. Det ses, at $h = 0$, så at $\mathcal{Q}$ iflg. lemma er normal, og nu er $\mathcal{G} \rhd \mathcal{Q} \rhd \mathcal{E}$ en absolut normalrække, hvis faktorer har orden $(\mathcal{G}:\mathcal{Q}) = p$ og $(\mathcal{Q}/\mathcal{E}) = q$. $\mathcal{G}$ er altså endda overopløselig. ∎

Korollar 3. Enhver gruppe, $\mathcal{G}$, af orden pq, hvor $p \nmid (q-1)$ og $q \nmid (p-1)$ er abelsk; endda cyklisk hvis $p \neq q$.

Bevis. For $p = q$ er $\mathcal{G}$ abelsk, men ikke nødvendigvis cyklisk. An-

tages $p < q$, ved vi fra korollar 2, at der findes netop én q-Sylow-undergruppe, Q, i G. Antallet af p-Sylow-undergrupper er $1, p.q$ eller pq, og af formen $1+ph$. Da $p \nmid q-1$, slutter vi heraf, at $h = 0$, ɔ: der findes netop én p-Sylow-undergruppe, P, i G. Iflg lemma er $G \rhd P$. Af $\text{ord}(Q) = q$ og $\text{ord}(P) = p$ fås $\text{ord}(P \cap Q) = 1$, altså $P \cap Q = E$. Heraf ses, at elementerne i P og Q er ombyttelige, thi er $g \in P$, $h \in Q$, er $ghg^{-1} \in Q$, og $hg^{-1}h^{-1} \in P$, men så er $(ghg^{-1})h^{-1} = g(hg^{-1}h^{-1}) \in P \cap Q$ɔ: $gh = hg$. Lad nu g frembringe P og h frembringe Q, da vil gh øjensynlig frembringe G.

Eks. Der findes kun én gruppe af orden $15 = 3 \times 5$, og den er cyklisk.

Korollar 4. Enhver gruppe, G, af orden p^2q er opløselig.
Bevis. 1) Hvis $p = q$ er G enten abelsk, og dermed ikke opløselig, eller $G' = Z$ og $G'' = Z' = E$, så at G også i dette tilfælde er opløselig. 2) Hvis der kun findes én p-Sylow-undergruppe P i G, er P normal, og $\text{ord}(P) = p^2$, så at P er abelsk, og $(G:P) = q$, så at G/P er cyklisk; $G \rhd P \rhd E$ er da en normalrække med abelske faktorer. 3) Hvis der findes én q-Sylow-undergruppe, Q, da er Q normal og abelsk, og også G/Q er abelsk ($(G:Q) = p^2$). 4) antag endelig, at der findes flere p-Sylow-grupper, og flere q-Sylow-undergrupper. Antallet af p-Sylowgrupper er $1+ph > 1$, og $1+ph \mid p^2q$, hvoraf $1+ph = q$. Antallet af q-Sylowgrupper er $1+qk > 1$, og $1+qk \mid p^2q$, hvoraf $1+qk = \begin{cases} p \\ p^2 \end{cases}$. Imidlertid er $1+qk \neq p$, da man ellers havde $p = 1+qk = 1+(1+ph)k = 1+k+phk$. Altså er $1+qk = p^2$. Det ses, at to forskellige q-Sylowundergrupper kun har e fælles, så at de p^2 q-Sylowgrupper indeholder

$$p^2q - (p^2-1)$$

forsk. elementer. En p-Sylow-gruppe og en q-Sylowgruppe har kun e fælles. Der findes mindst 2 forskellige p-Sylowundergrupper, som højst kan have p elementer fælles, og som derfor indeholder mindst

$$2p^2-p$$

forsk. elementer. G vil følgelig indeholde mindst

$$(p^2q-p^2+1) + (2p^2-p) - 1 = p^2q+p^2-p > p^2q$$

elementer, hvilket er en modstrid. Tilfældet 4) kan således slet ikke forekomme. ∎

Man kan vise: Enhver gruppe af kvadratfri orden er opløselig.
Og: Enhver gruppe af orden p^nq^m er opløselig.
En ikke-opløselig gruppe må således indeholde mindst $2^2 \times 3 \times 5$ elementer (= 60). A_5 har orden 60 og er ikke opløselig.

ABELSKE GRUPPER

I det følgende betegner $(\mathcal{G},+)$ en abelsk gruppe. Mængden af elementer af endelig orden udgør en undergruppe, $\mathcal{G}_T$, i $\mathcal{G}$, som kaldes $\mathcal{G}$'s torsionsgruppe. $\mathcal{G}$ kaldes torsionsfri, hvis $\mathcal{G}_T = 0$. Det ses, at $\mathcal{G}/\mathcal{G}_T$ er torsionsfri.
Et sæt $g_1,\ldots,g_n$ i en torsionsgri gruppe $\mathcal{G}$ kaldes uafhængigt, hvis $a_1,\ldots,a_n \in \dot{Z}$ og $a_1g_1+\ldots+a_ng_n = 0$ medfører $a_1 = a_2 = \ldots = a_n = 0$.

En endeligt frembragt bruppe kaldes fri abelsk, hvis den er direkte sum af endelig mange cykliske grupper af uendelig orden. Frembringerne for d⁻ cykliske grupper kaldes en basis.

Sætning. Hvis $\mathcal{G}$ er en endeligt frembragt fri abelsk gruppe, har alle baser samme elementantal, r, og r kaldes $\mathcal{G}$'s rang.
Bevis. Er $(g_1,\ldots,g_n)$ en basis, vil vilkårlige r+1 elementer $h_1,\ldots,h_n$ være afhængige, thi $\underline{\underline{h}}_1 = \underline{\underline{A}}\underline{\underline{g}}_1$, hvor $\underline{\underline{A}}$ er en $(r+1)\times r$ matrix. Da $\underline{\underline{A}}$'s rang således højst er r, findes en egentlig relation med rationale koefficienter mellem rækkerne, og derfor også en relation med hele koefficienter. Det er nu klart, at ingen basis kan være mindre, større, men heller ikke mindre, da $g_1,\ldots,g_n$ i så fald var afhængige. ∎

Sætning. Hvis $(g_1,\ldots,g_n)$ er en basis for en fri abelksk gruppe af endelig rang, fås samtlige baser ud fra denne ved unimodulære substitutioner.
Bevis. Lad $\underline{\underline{A}}$ være en unimodulær matrix, ɔ: en heltalsmatrix med determinant ± 1, og sæt $\underline{\underline{h}}_1 = \underline{\underline{A}}\underline{\underline{g}}_1$, da er $\underline{\underline{h}}_1$ uafhængigt, og da $\underline{\underline{g}}_1 = \underline{\underline{A}}^{-1}\underline{\underline{h}}_1$, hvor $\underline{\underline{A}}^{-1}$ er en heltalsmatrix, er $\underline{\underline{h}}_1$ et frembringersystem.
Lad omvendt $\underline{\underline{h}}_1$ være en basis, da er $\underline{\underline{g}}_1 = \underline{\underline{B}}\underline{\underline{h}}_1$ og $\underline{\underline{h}}_1 = \underline{\underline{A}}\underline{\underline{g}}_1$, hvor $\underline{\underline{A}}$ og $\underline{\underline{B}}$ er heltalsmatricer. Af $\underline{\underline{A}}\underline{\underline{B}} = \underline{\underline{E}}$ følger nu at $\underline{\underline{A}}$ er unimodulær. ∎

Sætning. Er $\mathcal{G}$ en fri abelsk gruppe af endelig rang r, og er $\mathcal{H}$ en undergruppe, da er $\mathcal{H}$ fri abelsk og af rang $\leq r$.
Bevis. Induktion efter r. r = 1: Enhver fra (0) forskellig undergruppe er isomorf med $\dot{Z}$. Antag nu sætningen for grupper af rang < r, og lad $g_1,\ldots,g_n$ være en basis for $\mathcal{G}$. For $h \in \mathcal{H}$ er $h = n_1g_1+\ldots+n_ng_n$, $n_1,\ldots,n_n \in \dot{Z}$. Hvis $n_n = 0$ for alle $h \in \mathcal{H}$ er vi færdige. I modsat fald er $\{n_n \mid h \in \mathcal{H}\}$ en fra (0) forskellig undergruppe i $\dot{Z}$, altså af formen $m\dot{Z}$, $m \neq 0$. Da $m \in m\dot{Z}$ findes et $h^* \in \mathcal{H}$, så at $h^* = n_1^*g_1+\ldots+n_{n-1}^*g_{n-1}+mg_n$. $\tilde{\mathcal{G}} = \{n_1g_1+\ldots+n_{n-1}g_{n-1} \mid n_i \in \dot{Z}\}$ er en fri abelsk gruppe af rang r-1. Iflg. induktionsantagelsen

er $\tilde{\mathcal{G}} \cap \mathcal{H}$ fri abelsk og har en basis $h_1', \ldots, h_s'$, hvor $s \leq r-1$. Nu er $h_1', \ldots, h_s', h^*$ uafhængige, thi er $n_1'h_1' + \ldots + n_s'h_s' + n^*h^* = 0$, er $n^*h^* \in \tilde{\mathcal{G}} \cap \mathcal{H}$, og dermed $n^* m g_r = 0$, så at $n^* = 0$ og således også $n_1' = \ldots = n_s' = 0$, da $h_1', \ldots, h_s'$ var uafhængige. $h_1', \ldots, h_s', h^*$ frembringer $\mathcal{H}$, thi er $h \in \mathcal{H}$, $h = n_1 g_1 + \ldots + n_r g_r = n_1 g_1 + \ldots + n_{r-1} g_{r-1} + n^* m g_r$, er $h - n^*h^* \in \tilde{\mathcal{G}} \cap \mathcal{H}$, : $h - n^*h^* = n_1'h_1' + \ldots + n_s'h_s'$. Vi har således vist, at $\mathcal{H}$ har en basis af rang $s+1 \leq (r-1)+1 = r$. ∎

Elementardivisorsætningen. Lad $\mathcal{G}$ være en fri abelsk gruppe af rang r, og $\mathcal{H}$ en undergruppe af rang s, da findes en basis $(g_1, \ldots, g_r)$ for $\mathcal{G}$ og en basis $(h_1, \ldots, h_s)$ for $\mathcal{H}$, så at $h_i = n_i g_i$, $n_i \in Z$, $i = 1, \ldots, s$.

Bevis. Det gælder om af finde en basis $(g_1, \ldots, g_r)$ for $\mathcal{G}$ og en basis $(h_1, \ldots, h_s)$ for $\mathcal{H}$ så at

$$\begin{pmatrix} h_1 \\ h_2 \\ \vdots \\ h_s \end{pmatrix} = \begin{pmatrix} n_1 & 0 \ldots 0 & \\ 0 & n_2 \ldots 0 & \underline{\underline{0}} \\ \vdots & \vdots \quad \vdots & \\ 0 & 0 \ldots n_s & \end{pmatrix} \begin{pmatrix} g_1 \\ g_2 \\ \vdots \\ g_r \end{pmatrix}$$

Lad $\underline{\underline{f}}_1$ være en basis for $\mathcal{G}$ og $\underline{\underline{k}}_1$ en basis for $\mathcal{H}$, altså $\underline{\underline{k}}_1 = \underline{\underline{A}}\underline{\underline{f}}_1$, hvor $\underline{\underline{A}}$ er en $(s \times r)$-heltalsmatrix. Er $\underline{\underline{g}}_1$ en anden basis for $\mathcal{G}$ og $\underline{\underline{h}}_1$ en anden basis for $\mathcal{H}$, altså $\underline{\underline{f}}_1 = \underline{\underline{P}}\underline{\underline{g}}_1$ og $\underline{\underline{k}}_1 = \underline{\underline{Q}}\underline{\underline{h}}_1$, er $\underline{\underline{h}}_1 = \underline{\underline{Q}}^{-1}\underline{\underline{A}}\underline{\underline{P}}\underline{\underline{g}}_1$. Det gælder om at vise, at der findes $\underline{\underline{P}}, \underline{\underline{Q}}$, så at $\underline{\underline{Q}}^{-1}\underline{\underline{A}}\underline{\underline{P}}$ HAR den ønskede form. Vi bemærker nu:

1) Hvis $\underline{\underline{g}}_1$ fremgår af $\underline{\underline{f}}_1$ ved permutation vil $\underline{\underline{Q}}^{-1}\underline{\underline{A}}\underline{\underline{P}}$ være en permutation af søjlerne i $\underline{\underline{A}}$.

2) Hvis $\underline{\underline{h}}_1$ fremgår af $\underline{\underline{k}}_1$ ved permutation, er $\underline{\underline{Q}}^{-1}\underline{\underline{A}}\underline{\underline{P}}$ en permutation af rækkerne i $\underline{\underline{A}}$.

3) Hvis $g_j = f_i + \gamma f_j$ (og ellers ingen forandring), er den j-te søjle i $\underline{\underline{Q}}^{-1}\underline{\underline{A}}\underline{\underline{P}}$ = (den j-te søjle - $\gamma \times$ i-te søjle) i $\underline{\underline{A}}$.

4) Hvis $h_i = k_i + \gamma k_j$ (og ellers ingen forandring), er den i-te række i $\underline{\underline{Q}}^{-1}\underline{\underline{A}}\underline{\underline{P}}$ = (den i-te række + $\gamma \times$ j-te række) i $\underline{\underline{A}}$.

Vi betragter nu alle matricer $\underline{\underline{Q}}^{-1}\underline{\underline{A}}\underline{\underline{P}}$, der fremgår af $\underline{\underline{A}}$ ved sukcessiv anvendelse af 1)-4). Lad a være det mindste positive tal, der forekommer i en af disse matricer, og lad $\underline{\underline{\tilde{A}}} = (\tilde{a}_{ij})$ være en tilsvarende matrix. Vi kan (1) og 2)) antage, at $a = \tilde{a}_{11}$. Nu er $\tilde{a}_{1j} = aq + r$, hvor $0 \leq r < a$, så at vi iflg. 3) kan antage, at $\tilde{a}_{1j} = r$, men definitionen af a giver nu $\tilde{a}_{1j} = 0$. Analogt kan vi iflg. 4) antage, at $\tilde{a}_{i1} = 0$, altså

$$\underline{\underline{A}} = \begin{pmatrix} a & 0 \ldots 0 \\ 0 & \\ \vdots & \underline{\underline{B}} \\ 0 & \end{pmatrix}$$

Den samme proces anvendes nu på delmatricen $\underline{\underline{B}}$, o.s.v. og til sidst

har $\underline{A}$ den ønskede form. ∎

Hovedsætning. Enhver endeligt frembragt abelsk gruppe er direkte sum af endelig mange cykliske grupper.

Bevis. Enhver endelig frembragt abelsk gruppe, $\mathcal{K}$, er homomorft billede af en fri abelsk gruppe, $\mathcal{G}$, af endelig rang (fx. r). Følgelig er $\mathcal{K} \cong \mathcal{G}/\mathcal{H}$. Iflg. det foregående findes baser $(g_1,..,g_r)$ og $(h_1,...,h_s)$ for $\mathcal{G}$, resp. $\mathcal{H}$, så at $h_i = n_i g_i$, men så $g = a_1g_1+...+a_rg_r \in \mathcal{H} \Leftrightarrow a_1g_1+...+a_rg_r = b_1h_1+...+b_sh_s \Leftrightarrow g = b_1n_1g_1+...+b_sn_sg_s \Leftrightarrow n_1 \mid a_1 \wedge ... \wedge n_s \mid a_s \wedge a_{s+1} = ... = a_r = 0$. Følgelig er $a_1g_1+...+a_rg_r = a_1'g_1+...+a_r'g \Leftrightarrow a_1 \equiv a_1' \pmod{n_1} \wedge ... \wedge a_s \equiv a_s' \pmod{n_s} \wedge a_{s+1} = a_{s+1}' \wedge ... \wedge a_r = a_r'$. Følgelig er $\mathcal{K} \cong \mathcal{G}/\mathcal{H} \cong \dot{Z}/n_1\dot{Z} \oplus ... \oplus \dot{Z}/n_s\dot{Z} \oplus \dot{Z} \oplus ... \oplus \dot{Z}$. ∎

Korollar 1. En endelig frembragt torsionsfri abelsk gruppe, $\mathcal{G}$, er fri abelsk af endelig rang.

thi $\mathcal{G}$ er direkte sum af cykliske grupper, som hver må være $\dot{Z}$. ∎

Korollar 2. En endelig frembragt abelsk gruppe, $\mathcal{G}$, er direkte sum af cykliske grupper af uendelig og primtalspotens orden.

thi for $n = p_1^{\mu_1}...p_r^{\mu_r}$ er $\dot{Z}/n\dot{Z} \cong \dot{Z}/p_1^{\mu_1}\dot{Z} \oplus ... \oplus \dot{Z}/p_r^{\mu_r}\dot{Z}$ ∎

ENDELIGE ABELSKE GRUPPER

Basissætning. En endelig abelsk gruppe, $\mathcal{G}$, af orden n er direkte sum af ~~primtalspotenscykliske~~ cykliske grupper af primtalspotensordener, q_i, $n = q_1...q_r$, og $q_1,...,q_r$ er entydigt bestemt (med multiplicitet).

Bevis. Sætningens første påstand følger straks af korollar 2. For hvert primtal $p \mid n$, er den direkte sum af de cykliske grupper, hvis orden er en potens af p, entydigt bestemt, nemlig som mængden af de elementer, hvis orden er en potens af p, d.v.s. som p-Sylow-undergruppen. (Specielt er en endelig abelsk gruppe direkte sum af sine Sylow-undergrupper). Det er derfor nok at betragte tilfældet, hvor $n = p^N$. Lad altså

$$\mathcal{G} = \mathcal{H}_1 \oplus ... \oplus \mathcal{H}_r = \mathcal{K}_1 \oplus ... \oplus \mathcal{K}_s,$$

hvor $\text{ord}(\mathcal{H}_i) = p^{n_i}$, $i = 1,...,r$ og $\text{ord}(\mathcal{K}_j) = p^{m_j}$, $j = 1,...,s$. Vi har $N = n_1+...+n_r = m_1+...+m_s$, og vi kan antage, at $n_1 \geq n_2 \geq ... \geq n_r$ og $m_1 \geq ... \geq m_s$. Vi tænker os valgt frembringere h_i for $\mathcal{H}_i$ og k_j for $\mathcal{K}_j$.

Induktion efter N. N = 1: Klart. Antag sætningen for grupper af orden p^M, med $M < N$. Sæt $\mathrm{Ann}(p) = \{g \in \mathcal{G} \mid pg = 0\}$, da er Ann(p) en undergruppe (annulatoren for p). Vi har $g = a_1h_1 + \ldots + a_rh_r \in \mathrm{Ann}(p) \Leftrightarrow pg = pa_1h_1 + \ldots + pa_rh_r = 0 \Leftrightarrow p^{n_1} \mid pa_1 \wedge \ldots\ p^{n_r} \mid pa_r$. $\Leftrightarrow p^{n_1-1} \mid a_1 \wedge \ldots \wedge p^{n_r-1} \mid a_r$. $\Leftrightarrow a_i = p^{n_i-1}\ell_i$, $\ell_i = 0, \ldots, p-1$. Da der således er p mulige værdier for a_i, er $\mathrm{ord}(\mathrm{Ann}(p)) = p^r$. Specielt er altså r = s.

Antag nu, at $n_1 \geq n_2 \geq \ldots \geq n_\nu > n_{\nu+1} = \ldots = n_r = 1$

og $m_1 \geq m_2 \geq \ldots \geq m_\mu > m_{\mu+1} = \ldots = m_r = 1$,

$0 \leq \nu, \mu \leq r$.

Vi har $\mathrm{ord}(p\mathcal{G}) = \mathrm{ord}(\mathcal{G}/\mathrm{Ann}(p)) = p^N/p^r < p^N$. og

$$p\mathcal{G} = p\mathcal{H}_1 \oplus \ldots \oplus p\mathcal{H}_n = p\mathcal{K}_1 \oplus \ldots \oplus p\mathcal{K}_n$$
$$= p\mathcal{H}_1 \oplus \ldots \oplus p\mathcal{H}_\nu = p\mathcal{K}_1 \oplus \ldots \oplus p\mathcal{K}_\mu$$

og $\mathrm{ord}(p\mathcal{H}_1) = p^{n_1-1}, \ldots, \mathrm{ord}(p\mathcal{H}_\nu) = p^{n_\nu-1}$ og $\mathrm{ord}(p\mathcal{K}_1) = p^{m_1-1}, \ldots,$ $\mathrm{ord}(p\mathcal{K}_\mu) = p^{m_\mu-1}$. Induktionsantagelsen giver derfor $\nu = \mu$ og $p^{m_1-1} = p^{n_1-1}, \ldots, p^{m_\mu-1} = p^{n_\nu-1}$, hvoraf påstanden følger. ∎

Vi har fundet en bijektiv forbindelse mellem mængden af endelige abelske grupper (på isomorfi nær) og mængden af endelige mængder af primtalspotenser med multiplicitet. Specielt er antallet af abelske grupper af orden p^n = antallet af partitioner af n, betegnet p(n). (fx. er 3 = 3 = 2+1 = 1+1+1 så at p(3) = 3 og 4 = 4 = 3+1 = 2+2 = 2+1+1 = 1+1+1+1, så at p(4) = 5. Der gælder i øvrigt $\prod_{\nu=1}^{\infty} \frac{1}{1-x} = \sum_{n=1}^{\infty} p(n)x^n$.)

KAPITEL II RINGE

KEksempler på ringe:

Eks.1) Hvis man i den additive gruppe R af kontinuerte afb : $\grave{R} \longrightarrow \grave{R}$ (elller : $\grave{R} \longrightarrow \grave{C}$) definerer $(f*g)(x) = \int f(x-t)g(t)dt$ fremkommer en ring $(R,+,*)$ uden 1-element.

2) Lad V være et uendeligtdimmensionalt vektorrum. Underrummet $R \subseteq \mathcal{L}(V,V)$ bestående af de lineære afbildf, med dim $f(V) < \infty$ udgør med sammensætning en ring $(R,+,\circ)$ ligeledes uden 1-element.

3) For en abelsk gruppe, $\mathcal{G}$, udgør gruppen R af endomorfier $f : \mathcal{G} \to \mathcal{G}$ med sammensætning en ikke-kommutativ ring $(R,+,\circ)$, ~~k~~kaldet endomorfiringen for $\mathcal{G}$.

4) Hvis $\mathcal{G}$ er en fri abelsk gruppe af rang, da er endomorfiringen $(R,+,\circ) \cong (M_{r\times r}(\grave{Z}),+,\times)$.

En delmængde $I \subseteq R$ kaldes et venstre ideal, hvis I er en undergruppe i $(R,+)$, og hvis $RI \subseteq I$. Et højreideal defineres på analog måde.

Eks. I $R = M_{n\times n}$ er $\left\{\begin{pmatrix} 0 & A \\ 0 & \end{pmatrix}\right\}$ et venstreideal, der ikke er højreideal.

$I \subseteq R$ kaldes et bilateralt ideal (eller tosidet) , eller blot et ideal, hvis I er både højre- og venstreideal. R kaldes simpel, hvis der kun findes trivielle idealer.

Homomorfisætningen. Er $\varphi: R \to R'$ en epimorfi, da er $\mathrm{Ker}(\varphi) = \{r \in R \mid \varphi(r) = 0\}$ et ideal i R, og $R' \cong R/\mathrm{Ker}(\varphi)$.

Opgaver. Et endeligt integritetsområde er et lememe.
Endda: Et integritetsområde, der kun indeholder endelig mange idealer er et legeme. (Betragt idealerne $(a),(a^2),\ldots$ for et $a \in R^*$.)

Er R et integritetsområde, da findes et (og på isomorfi nær kun ét) legeme K, der indeholder R (ɔ: har et med R isomorft delintegritetsområde), og som er mindst i den forstand, at ethvert skævlegeme L med samme egenskab indeholder et med K ~~s~~ isomorft dellegeme. K kaldes R's kvotientlegeme. K kan også karakteriseres ved at indeholde et med R isomorft delintegritetsområde R^* og at ethvert element $\alpha \in K$ kan skrives $\alpha = a^* b^{*-1}$, med $a^*, b^* \in R^*$, $b^* \neq 0$.

Eks. $\dot{Z}$ har kvotientlegemet $\dot{Q}$.

I en kommutativ ring med 1-element, R, er (a) = Ra det mindste ideal, der indeholder a; det kaldes det af a frembragte hovedideal.

Eks. I $\dot{Z}$ er som bekendt ethvert ideal af formen $a\dot{Z}$, altså et hovedideal. Det er klart, at $\dot{Z}/a\dot{Z}$ er et integritetsområde, hvis og kun hvis a = 0 eller a = $\pm$ primtal p. Følgelig er $\dot{Z}/a\dot{Z}$ et legeme, hvis og kun hvis a = $\pm$ primtal p, og dette legeme betegnes GF(p).

Lad K være et skævlegeme, og lad R være den mindste undergruppe i K, der indeholder 1_K. Ved $\varphi(1_Z) = 1_K$ defineres øjensynlig en epimorfi φ: $\dot{Z} \longrightarrow R$. Enten er φ bijektiv (og altså Ker(φ) = (0),)i hvilket tilfælde K siges at have Karakteristik 0. K vil da indeholde et med $\dot{Q}$ isomorft dellegeme, og for $a \in K^*$ er na = 0 kun hvis n = 0. Eller: Ker(φ) = (a) $\neq$ (0), da er $R \cong \dot{Z}/(a)$. Da $R \subseteq K$ er et integritetsområde, er $\dot{Z}/(a)$ et integritetsområde, og derfor et legeme, og a = primtal p. K siges at have karakteristik p, og R er et legeme isomorft med $\dot{Z}/p\dot{Z}$. For $a \in K^*$ er na = 0 kun hvis $p \mid n$ (og omvendt).
Det herved i skævlegemet K bestemte legeme kaldes K's primlegeme.

Eks. I et legeme af karakteristik $p \neq 0$ definerer a a^p en homomorfi (binomialformlen), som øjensynlig er injektiv. Den er surjektiv, hvis K er et endeligt legeme, men ikke surjektiv i almindelighed.

Et ideal $\mathfrak{P}$ i en ring R kaldes et primideal, hvis $a, b \in \mathfrak{P} \Rightarrow a \in \mathfrak{P} \vee b \in \mathfrak{P}$.
Sætning. I en kommutativ ring R med 1-element gælder: $\mathfrak{P}$ er et primideal, hvis og kun hvis $R/\mathfrak{P}$ er et legeme.

Et ideal $\mathfrak{M}$ i en ring R kaldes maximalt, hvis $\mathfrak{M} \subset R$, og hvis der ikke findes idealer $\mathfrak{A}$ med $\mathfrak{M} \subset \mathfrak{A} \subset R$.
Sætning. I en kommutativ ring R med 1-element gælder: Ethvert egentligt ideal, $\mathfrak{A}$, er indeholdt i et maximalt ideal $\mathfrak{M}$.
Bevis. Zorn's lemma.
Sætning. I en kommutativ ring R med 1-element gælder: $\mathfrak{M}$ er et max. ideal hvis og kun hvis $R/\mathfrak{M}$ er et legeme.

Eks. I den additive gruppe $\dot{Z}/p\dot{Z}$ defineres $\odot$ ved $a \odot b = 0$. $(\dot{Z}/p\dot{Z}, +, \odot)$ er en ring uden 1-element. Da $\dot{Z}/p\dot{Z}$ kun har

de additive undergrupper (0) og $\grave{Z}/p\grave{Z}$, er (0) et maximalt ideal, men $\grave{Z}/\grave{p}Z$ / (0) er ikke et legeme.

2) $2^{-\infty}\grave{Z} = \{\frac{h}{2^n} \mid h \in \grave{Z} \text{ og } n \in N_0\}$ er en additiv gruppe. Enhver undergruppe i $2^{-\infty}\grave{Z}/\grave{Z}$ er endelig og cyklisk, med en frembringer $\left(\frac{1}{2^n}\right)$. Defineres $\circ$ som i det foregående eksempel fås en ring uden maximale idealer.

I en kommutativ ring R, med 1-element, kaldes $\mathrm{Rad}(\mathcal{a}) = \{b \in R \mid \exists n \in \grave{N}: b^n \in \mathcal{a}\}$ radikalet for $\mathcal{a}$. $\mathrm{Rad}(\mathcal{a})$ er igen et ideal (Binomialformlen)

Sætning. I en kommutativ ring R med 1-element gælder:

$\mathrm{Rad}(\mathcal{a}) = \bigcap_{\varphi \supseteq \mathcal{a}} \varphi$.

~~Bevis. Er b Rad(..), : b^n, og , da er b^n, og dermed b .~~

~~Antag nu, at / Rad(..) : n N: b^n/ . Vi~~

Vi viser først

Lemma. Lad R være en kommutativ ring, og $S \subseteq R^*$ en multiplikativ semigruppe, da er $\mathcal{g} = \{\mathcal{a} \subseteq R \mid \mathcal{a} \cap S = \emptyset\}$ induktivt ordnet, og et maximalt element i $\mathcal{g}$ er et primideal.

Det er klart, at $\mathcal{g}$ er induktivt ordnet. Lad φ være et maximalt element i $\mathcal{g}$, og antag, at der findes $a,b \in R$, $ab \in \varphi$ $a,b \notin \varphi$. Vi har $\varphi \subset (\varphi,b)$ og $\varphi \subset (\varphi,a)$, så at $(\varphi,a) \notin \mathcal{g}$ og $(\varphi,b) \notin \mathcal{g}$, ɔ: der findes $s,t \in S$ så at $s = p+ra+na$ og $t = p'+r'b+n'b$. Nu er $st \in S$ og $st \in \varphi$, i modstrid med at $\varphi \cap S = \emptyset$ ∎

Bevis. Ved overgang til $R/\mathcal{a}$ kan vi øjensynlig antage, at $\mathcal{a} = (0)$. Hvis $a \in \mathrm{Rad}(0)$ er $a^n = 0$, og dermed $a^n \in \varphi$ for alle φ og $a \in \varphi$ for alle φ. Er omvendt $a^n \neq 0$ for alle n, er $S = \{a,a^2,a^3,\ldots\}$ en semigruppe, så der findes et primideal φ_0 med $S \cap \varphi_0 = \emptyset$; specielt er $a \notin \varphi$, og dermed $a \notin \bigcap_{\varphi} \varphi$. ∎

Eks. $R = (\hat{C}_L[0,1],+,\ )$, hvor $L = \grave{R}$ eller $L = \grave{C}$. For $\alpha \in [0,1]$ er $M_\alpha = \{f \in R \mid f(\alpha) = 0\}$ et ideal, og det er maximalt, da $R/M_\alpha \cong L$ er et legeme. Der findes ikke andre maximale idealer i R, thi er $\mathcal{a}$ et ideal, der ikke er indeholdt i noget M_α, findes til hvert $\alpha \in [0,1]$ et $f_\alpha \in M_\alpha$ så at $f_\alpha(\alpha) \neq 0$. Nu er $f_\alpha \neq 0$ i en omegn U_α af α og da $[0,1]$ er kompakt, findes $\alpha_1,\ldots,\alpha_m \in [0,1]$, så at $[0,1] = U_{\alpha_1} \cup \ldots \cup U_{\alpha_m}$. Sættes $f = \overline{f_{\alpha_1}}\, f_{\alpha_1} + \ldots + \overline{f_{\alpha_m}}\, f_{\alpha_m}$, da er $f \in \mathcal{a}$, og $f \neq 0$, men så er $f^{-1} \in R$ og dermed $1 = f^{-1} f \in \mathcal{a}$: $\mathcal{a} = R$.

$J = \{f \in R \mid f(t) = 0$ i en omegn af $0\}$ er et ideal, og $\mathrm{Rad}(J) = J$. Heraf følger, at der i R findes primidealer, der ikke er maximale.

Lad R være et integritetsområde. Et element $\varepsilon \in R$ kaldes en enhed, hvis der findes $\varepsilon' \in R$, så at $\varepsilon\varepsilon' = 1$, altså hvis $(\varepsilon) = R$. To elementer $a,b \in R$ kaldes associerede, hvis $a,b \neq 0$, og der findes en enhed ε så at $a = b\varepsilon$, altså hvis $(a) = (b) \neq (0)$. For a,b R, $a \neq 0$, siger vi "a går op i b" eller "a er divisor i b",og skriver $a|b$, hvis der findes $r \in R$, så $ar = b$, altså hvis $b \in (a)$.
$a|b \wedge b|a \Leftrightarrow$ a og b er associerede.
Et element $p \in R$ kaldes irreducibelt eller et primelement, hvis det er forskelligt fra 0, k ikke er en enhed og kun har trivielle divisorer.
Et integritetsområde R kaldes et F.D. (factorization Domain), hvis ethvert $a \neq 0$ ikke enhed kan skrives som produkt af endelig mange irreducible elementer.

Eks. Mængden af polynomier $R = \{a_0+a_1X+\ldots+a_nX^n \mid a_0 \in \grave{Z} \wedge a_1,\ldots,a_n \in \grave{Q}\}$ er et integritetsområde med enhederne ± 1. De eneste muligheder for opløsning af X er $X = p_1\ldots p_r$ $(\frac{1}{p_1\ldots p_r}X)$, hvor $p_1,\ldots,p_r$ er primelementer i $\grave{Z}$ (ɔ: $\pm$ primtallene), men $\frac{1}{p_1\ldots p_r} = 2 \cdot \frac{1}{2p_1\ldots p_r}$ er aldrig irreducibel. R er således ikke et F.D.

Et integritetsområde R kaldes et U.F.D. (Unique Factorization Domain), hvis det er F.D. og der af $p_1\ldots p_r = q_1\ldots q_s$, (primelementer) følger, at $r = s$ og at p_i er associeret med $q_{\sigma(i)}$ for en passende permutation $\sigma \in S_n$.

Eks. $R = \grave{Z}[\sqrt{-5}]$ er et integritetsområde med enhederne ± 1. For $\alpha = x+y\sqrt{-5}$ sættes $N(\alpha) = \alpha\bar{\alpha} = x^2+5y^2$. $N : R^* \to \grave{N}$ er en homomorfi. Idet $N(\alpha) \neq 3,7$ for alle $\alpha \in R$, og da $N(3) = 3\cdot3$, $N(7) = 7\cdot7$, $N(1 \pm 2\sqrt{-5}) = 21 = 3\cdot7$, følger det, at $3,7,1\pm2\sqrt{-5}$ er primelementer i R, men $21 = 3\cdot7 = (1+2\sqrt{-5})(1-2\sqrt{-5})$.

Et integritetsområde R kaldes et P.I.D. (Prime Ideal Domain), hvis ethvert ideal er et hovedideal.

Sætning. Et P.I.D., R, er et U.F.D.

Beviset føres i flere skridt:
Lemma. Hvis et primelement $p|ab$, da vil $p|a$ eller $p|b$.
Bevis. Sættes $(a,p) = (c)$, da vil $c|p$. Enten er c en enhed, så at $(a,p) = R$, og dermed $1 = ax+py$ og $b = abx+pby$, hvoraf $p|b$, eller c er associeret med p, så at $p|c$, hvilket med $c|a$ giver $p|a$ ∎

Af dette lemma følger, at hvis der findes en primopløsning, da er

den entydig. Vi bemærker nu, at et P≠I.D. er et Noethersk integritetsområde, og afslutter beviset med

Lemma. Et Noethersk integritetsområde er et F.D.
Bevis. Indirekte. Fandtes der et $a \neq 0$, ikke enhed, der ikke var produkt af primelementer, ville a specielt ikke selv være primelement, så $a = a_1 a_1'$, hvor a_1, a_1' er ikke trivielle divisorer i a; endvidere måtte mindst en af disse, fx a_1 være uden primopløsning. Vi finder således $(a) \subset (a_1) \subset \ldots$ i modstrid med at R vær Noethersk. ∎

Eks. I eksemplet p.4 er $(\frac{X}{2}) \subset (\frac{X}{4}) \subset (\frac{X}{8}) \subset \ldots$

Sætning. I et P.I.D., R, er (p) et primideal (ikke-trivielt), hvis og kun hvis p er et primelement.
Bevis. "$\Rightarrow$" Indirekte: Hvis $p = aa'$, og $p \nmid a$ og $p \nmid a'$, da var $\bar{a}\bar{a}' = \bar{0}$, $\bar{a}, \bar{a}' \neq 0$ i modstrid med at (p) var et primideal.
"$\Leftarrow$" Hvis $\bar{a}\bar{a}' = \bar{0}$ i R/(p), er $aa' \in (p)$ ↄ: $p \mid aa'$, men så er fx $p \mid a$, og altså $\bar{a} = \bar{0}$ i R/(p). ∎

Sætning. I et P.I.D., R, er ethvert ikketrivielt primideal, (p), maximalt.
Bevis. Lad $\bar{a} \in R/(p)$, $\bar{a} \neq \bar{0}$, altså $a \notin (p)$. Sættes $(a,p) = (d)$, er $d \mid p$; nu er d en enhed, thi var d associeret med p, ville $p \mid d$, som samkmen med $d \mid a$ giver $p \mid a$, i modstrid med $a \notin (p)$.
Da $(a,p) = R$, har vi $1 = ax+py$ og dermed $\bar{a}\bar{x} = \bar{1}$. R/(p) er således et legeme. ∎

Lad R være en kommutativ ring med 1-element, da kan vi danne potensrækkeringen over R : R[[X]], og polynomiumsringen over R: R[X], og har da

$$R \subset R[X] \subset R[[X]].$$

Sætning. R er et integritetsområde $\Leftrightarrow$ R[[X]] er et integritetsområde.
Korollar. R er et int.omr. $\Leftrightarrow$ R[X] er et int.omr.

Sætning. Hvis R[[X]] er et int.omr., da er $(a_0, a_1, \ldots)$ en enhed $\Leftrightarrow$ a_0 er en enhed i R.
Bevis. "$\Rightarrow$" er trivielt. "$\Leftarrow$" Hvis a_0 er enhed i R kan ligningerne $a_0 b_0 = 1$, $a_0 b_1 + a_1 b_0 = 0$, $a_0 b_2 + a_1 b_1 + a_2 b_0 = 0, \ldots$ successivt løses.
Sætning. Hvis R[X] er et int.omr., da er $(a_0, \ldots, a_n, 0, 0, \ldots)$ en enhed, hvis og kun hvis a_0 er enhed i R og $a_1 = \ldots = a_n = 0$.

Bevis. "$\Leftarrow$" er trivielt. "$\Rightarrow$": For $f = (a_0,a_1,\ldots) \in R[X]$ defineres f's grad, grad(f), som $-\infty$, hvis $f = 0$, og som det største n, for hvilket $a_n \neq 0$ ellers. Her er $\text{grad}(f+g) \leq \text{grad}(f) \vee \text{grad}(g)$ og $\text{grad}(fg) = \text{grad}(f) + \text{grad}(g)$. Af den sidste relation følger, at der for en enhed $f \in R[X]$ må gælde $\text{grad}(f) = 0$, altså $a_0 \neq 0$, $a_1 = a_2 = \ldots = 0$. Nu er a_0 endda en enhed i R, thi f^{-1} er en enhed i $R[X]$, altså $f^{-1} = b_0$ og dermed $a_0b_0 = ff^{-1} = (1,0,0,\ldots) = 1$. ∎

Sætning. Er K et legeme, da er K[[X]]et P.I.D.
Velkendt, idet man viser
Sætning. Idealerne i K[[X]] er netop $K[[X]] = (1) \supset (X) \supset (X^2) \supset \ldots \supset (0)$.

Sætning. Er K et legeme, da er K[X] et P.I.D.
En følge af Euklids algoritme.

Hvis R er et int.omr., $f(X) = a_0+a_1X+\ldots+a_nX^n \in R[X]$ og $c \in R$, kan vi danne $a_0+a_1c+\ldots+a_nc^n \in R$, et element, vi vil betegne f(c). Ved $c \to f(c)$ defineres således en afbildning, igen betegnet f, af $R \to R$. Vi siger, at $c \in R$ er rod i f, hvis $f(c) = 0$. At er klart at $f \to f(c)$ er en homomorfi $R[X] \to R$

Sætning. Hvis K er et legeme, og $f(X) \in K[X]$ af $\text{grad}(f) = n > -\infty$, da har f højst n rødder forskellige rødder.
Bevis. Lad $\alpha_1,\ldots,\alpha_\nu$ være forskellige rødder i f. I følge divisionsalgoritmen findes $q,r \in K[X]$, så at $f(X) = (X-\alpha_1)q(X)+r(X)$, hvor $\text{grad}(r) < \text{grad}(X-\alpha_1) = 1$, altså $\text{grad}(r) \leq 0$ ↔: r konstant. Da $f(\alpha_1) = 0 + r(\alpha_1)$, er $r = 0$, og dermed $f(X) = (X-\alpha_1)q(X)$. Nu er $0 = f(\alpha_2) = (\alpha_2-\alpha_1)q(\alpha_2)$, altså $q(\alpha_2) = 0$, så vi finder $q(X) = (X-\alpha_2)q_1(X)$, o.s.v. $f(X) = (X-\alpha_1)\ldots(X-\alpha_\nu)q_{\nu-1}(X)$ ∎

Korollar. Hvis R er et int.omr., og $f(X) \in R[X]$ af $\text{grad}(f) = n > -\infty$ da har f højst n forskellige rødder.
thi $f \in K[X]$, hvor K er R's kvotientlegeme. ∎

Hvis R er et int.omr. betegner R(X) kvotientlegemet for R[X].

Eks. R = GF(p). Da $GF(p)(X) \supset GF(p)[X] \supset GF(p)$, har også GF(p)(X) karakteristik p. Der findes altså uendelige legemer af karakteristik $p \neq 0$.

Eks. Lad K = GF(p), og lad $f(X) = a_0+\ldots+a_nX^n \in K[X]$, p, da er $f(X)^p = f(X^p)$, i følge polynomialformlen og

relationen $a^p = a$ for $a \in K$. For $\frac{f(X)}{g(X)} \in K(X)$ gælder: $(\frac{f(x)}{g(X)})^p = \frac{f(X^p)}{g(X^p)} \neq X$, idet $g(X^p)X \neq f(X^p)$. Afbildningen $c \longrightarrow c^p$ af $K(X) \longrightarrow K(X)$ er altså ikke surjektiv.

Hvis R, R^* er kommutative ringe med 1-elementer, og $\varphi : R \longrightarrow R^*$ en homomorfi, induceres ved $a_0+\ldots+a_nX^n \longrightarrow \varphi(a_0)+\ldots+\varphi(a_n)X^n$, en udvidelse af φ til en afbildning, også kaldet, $\varphi : R[X] \longrightarrow R^*[X]$, der let ses at være en homomorfi.

Vi vil nu undersøge polynomiumsringen over et U.F.D. , R. Et $f(X) = a_0+\ldots+a_nX^n \in R[X]$ kaldes primitivt, hvis $(a_0,\ldots,a_n) = 1$.

Gauss' lamma. Lad R være U.F.D., da er produkt af primitive polynomier over R igen et primitivt polynomium.

Indirekte bevis. Lad $g(X), h(X) \in R[X]$ være primitive, $f(X) = g(X)h(X) = a_0+\ldots+a_nX^n \in R[X]$, og antag, at der findes et primelement $\pi \in R$, så $\pi \mid (a_0,\ldots,a_n)$. (π) er et primideal, thi er $ab \in (\pi)$, er $\pi \mid ab$, hvoraf $\pi \mid a$ eller $\pi \mid b$ ↄ: $a \in (\pi)$ eller $b \in (\pi)$. $R/(\pi)$ er følgelig et integritetsområde, og den kannoniske homomorfi: $\mathcal{H}: R$ på $R/(\pi)$ inducerer en homomorfi $\mathcal{H} : R[X] \longrightarrow R/(\pi)[X]$, ved hvilken vi har $\mathcal{H}(g)\mathcal{H}(h) = \mathcal{H}(gh) = \mathcal{H}(f) = 0$. Da $R/(\pi)[X]$ er et int.-omr. er således $\mathcal{H}(g) = 0$ eller $\mathcal{H}(h) = 0$, i modstrid med at g og h var primitive. ∎

Korollar til Gauss' lemma. Lad R være U.F.D. med kvotientlegemet K. Hvis $f(X) = g(X)h(X)$, med $f(X) \in R[X]$, $g(X)$ primitiv $\in R[X]$, og $h(X) \in K[X]$, da er $h(X) \in R[X]$.

Bevis. h(X)'s koefficienter kan skrives som uforkortelige brøker $\in K$, så der findes $a \in R$, at at $ah(X) \in R[X]$. Følgelig findes $a, b \in R$ med $(a,b) = 1$, så at $\frac{a}{b}h(X)$ er primitivt $\in R[X]$. Iflg. Gauss' lemma er $\frac{a}{b} f(X) = g(X)(\frac{a}{b}h(X))$ primitivt. Da koefficienterne er hele, og da $(a,b) = 1$, må b gå op i disse, men så må a være en enhed. $h(X) = a^{-1}b(\frac{a}{b}h(X))$ er da $\in R[X]$. ∎

Sætning. Hvis R er U.F.D., da er også R[X] et U.F.D.

Enhederne i R[X] er som bekendt netop enhederne i R. Vi undersøger nu de irreducible elementer.

Lemma. Hvis grad(f) = 0, da er f(X) irreducibel, hvis og kun hvis $f(X) = \pi$, hvor π er irreducibel i R.

Hvis grad(f) ≥ 1, da er f(X) irreducibel, hvis og kun hvis f(X) er primitiv $\in R[X]$ og irreducibel som element i K[X].

Bevis. Den første påstand er triviel. Antag grad(f) ≥ 1. Hvis

$f(X)$ er primitiv og irreducibel i $K[X]$, da også i $R[X]$, er oplagt. Lad omvendt $f(X)$ være irreducibel i $R[X]$, da er $f(X)$ primitiv. Antag, at $f(X)$ er reducibel i $K[X]$, da findes $g(X), h(X) \in K[X]$, så $f(X) = g(X)h(X)$ og $1 \leq \text{grad}(g) < \text{grad}(f)$. Nu kan vi finde $c \in K$, så $cg(X)$ er primitiv $\in R[X]$, men så er $f(X) = [cg(X)][\frac{1}{c}h(X)]$, og $\frac{1}{c}h(X)$ er iflg. korollar $\in R[X]$, så at $f(X)$ ikke er irreducibel i $R[X]$. ∎

Lemma. <u>Hvis et irreducibelt polynomium $p(X) \mid f(X)g(X)$, da vis1 $p(X) \mid f(X)$ eller $p(X) \mid g(X)$.</u>

Bevis. 1) $\text{grad}(p) = 0$, da er $p(X) = \pi$, hvor π er irreducibel i R, og $f(X)g(X) = \pi h(X)$. Nu er (π) et primideal, så $R/(\pi)$ er et integritetsområde. Er $\varkappa : R[X] \longrightarrow R/(\pi)[X]$ den kannoniske homomorfi, er $\varkappa(f)\varkappa(g) = \varkappa(fg) = \varkappa(\pi h) = \varkappa(\pi)\varkappa(h) = 0$, så at $\varkappa(f) = 0$ eller $\varkappa(g) = 0$ ↔: $\pi \mid f$ eller $\pi \mid g$.

2) $\text{grad}(p) \geq 1$. Da $p(X) \mid f(X)g(X)$ i $R[X]$, gælder dette specielt også i $K[X]$. Da $p(X)$ er irreducibel i $K[X]$ og $K[X]$ er et P.I.D., er fx. $p(X) \mid f(X)$ i $K[X]$ ↔: $f(X) = p(X)h(X)$, hvor $h(X) \in K[X]$. Af korollar får vi nu $h(X) \in R[X]$, altså $p(X) \mid f(X)$ i $R[X]$. ∎

Af dette lemma følger primopløsningens entydighed. Vi viser nu eksistensen: Lad altså $f(X) \in R[X]$, $f \neq 0$, ikke enhed.

1) Hvis $\text{grad}(f) = 0$ er vi færdige, thi da er $f(X) \in R$, og en primopløsning i R er en primopløsning i $R[X]$.

2) Hvis $\text{grad}(f) \geq 1$, er $f(X) = df_1(X)$, hvor d er største fælles divisor for $f(X)$'s koefficienter, og $f_1(X)$ er primitiv. Hvis $f_1(X)$ er irreducibel er vi færdige i flg. 1) Ellers er $f_1(X) = g_1(X)h_1(X)$, hvor g_1, h_1 er primitive, og $1 \leq \text{grad}(g_1) < \text{grad}(f_1)$ og $1 \leq \text{grad}(h_1) < \text{grad}(f_1)$ o.s.v. men dette må nødvendigvis stoppe. ∎

Hermed er beviset for sætningen afsluttet ∎

Eks. $\dot{Z}[X]$ er et U.F.D.

Korollar. <u>For et legeme K er $K[X_1, \ldots, X_n]$ et U.F.D.</u>

Bemærkning. Dette gælder også for $K[X_1, X_2, \ldots]$

Eks. $\dot{Z}[X]$ er ikke et P.I.D., thi $\mathfrak{J} = \{f(X) \in \dot{Z}[X] \mid 2 \mid f(0)\}$ er et ideal, der ikke er hovedideal. Det viser sig, at $\dot{Z}[X]$ ikke engang er Noethersk.

Vi har tidligere vist, at hvis R er i P.I.D., da er R et U.F.D. og ethvert ikke-trivielt primideal er maximalt. Der gælder omvendt:

Sætning. Et U.F.D., R, hvori ethvert ægte primideal er maximalt, er et P.I.D.

Bevis. 1) Vi bemærker først, at ethvert maximalt ideal, $\mathfrak{M}$, i R er et hovedideal, thi er $\mathfrak{M} \supset (0)$, findes $a \in \mathfrak{M}$, $a \neq 0$, ikke enhed. Er $a = \pi_1 \dots \pi_n \in \mathfrak{M}$, vil (da et max.ideal altid er primideal) fx. $\pi_1 \in \mathfrak{M}$, og dermed $(\pi_1) \subseteq \mathfrak{M}$. Da (π_1) er et primideal og derfor maximalt ifølge forudsætning, er $(\pi_1) = \mathfrak{M}$.

2) Er $\mathfrak{A}$ et ikketrivielt ideal i R, vil $\mathfrak{A}$ være indeholdt i mindst et maximalt ideal $\mathfrak{M} = (\pi)$, men det kan kun være indeholdt i endelig mange maximale idealer $\mathfrak{M}_i = (\pi_i)$, thi er $a \in \mathfrak{A} \setminus (0)$, vil $\pi_i \mid a$.

3) Lad $\mathfrak{M}_\iota = (\pi_\nu)$, $\iota = 1, \dots, \nu$ være samtlige forskellige maximale idealer, der indeholder $\mathfrak{A}$. For $a \in \mathfrak{A}$ vil $\pi_1 \dots \pi_\nu \mid a$, så $\mathfrak{A} \subseteq (\pi_1 \dots \pi_\nu)$. Vi betragter nu alle eksponentsystemer $(\alpha_1, \dots, \alpha_\nu)$, for hvilke $\mathfrak{A} \subseteq (\pi_1^{\alpha_1} \dots \pi_\nu^{\alpha_\nu})$. For et $a \in \mathfrak{A} \setminus (0)$, er $a = \pi_1^{m_1} \cdot \dots \cdot \pi_\nu^{m_\nu} q$, hvor $\pi_\iota \nmid q$, så $\alpha_1 \leq m_1, \dots, \alpha_\nu \leq m_\nu$. Lad $(\alpha_1, \dots, \alpha_\nu)$ være et højeste eksponentsystem, for hvilket $\mathfrak{A} \subseteq (\pi_1^{\alpha_1} \dots \pi_\nu^{\alpha_\nu})$; det påstås, at $\mathfrak{A} = (\pi_1^{\alpha_1} \dots \pi_\nu^{\alpha_\nu})$

4) For $a \in \mathfrak{A}$ er $a = \pi_1^{\alpha_1} \dots \pi_\nu^{\alpha_\nu} r$. Sættes $\mathfrak{J} = \{r \in R \mid \pi_1^{\alpha_1} \dots \pi_\nu^{\alpha_\nu} r \in \mathfrak{A}\}$ er $\mathfrak{J}$ et ideal i R, og $(0) \subset \mathfrak{J}$. Nu er $\mathfrak{J} = R$, thi ellers fandtes et maximalt ideal (π), så at $\mathfrak{J} \subseteq (\pi)$, og dermed $\mathfrak{A} \subseteq (\pi_1^{\alpha_1} \dots \pi_\nu^{\alpha_\nu} \pi) \subseteq (\pi)$. Heraf følger for det første, at π er associeret med et π_ι (iflg. def. på π_ι'erne), så vi kan antage $\pi = \pi_\iota$ men så vil $\mathfrak{A} \subseteq (\pi_1^{\alpha_1} \dots \pi_\iota^{\alpha_\iota + 1} \dots \pi_\nu^{\alpha_\nu})$ være i strid med at $(\alpha_1, \dots, \alpha_\nu)$ var højest. Af $\mathfrak{J} = R$ følger specielt, at $1 \in \mathfrak{J} : (\pi_1^{\alpha_1} \dots \pi_\nu^{\alpha_\nu}) \subseteq \mathfrak{A} \subseteq (\pi_1^{\alpha_1} \dots \pi_\nu^{\alpha_\nu})$ ∎

Schönemann-Eisensteins irreducibilitetskriterium. Lad R være et U.F.D., $f(X) = a_0 + a_1 X + \dots + a_{n-1} X^{n-1} + X^n \in R[X]$, og antag, der findes et primelement $\pi \in R$, så at $\pi \mid a_0, \dots, \pi \mid a_{n-1}$ og $\pi^2 \nmid a_0$, da er $f(X)$ irreducibel over $K[X]$ (og dermed over $R[X]$).

Bevis. Det er nok at vise, at $f(X)$ er irreducibel over $R[X]$. Indirekte: Antag at $f(X) = (b_0 + \dots + b_{m-1} X^{m-1} + X^m)(c_0 + \dots + c_{n-m-1} X^{n-m-1} + X^{n-m})$, $1 \leq m < n$, så er $a_0 = b_0 c_0$. Ved den kannoniske homomorfi $\varkappa : R[X] \longrightarrow R/(\pi)[X]$ får vi $X^n = \varkappa(f) = (\varkappa(b_0) + \dots + X^m)(\varkappa(c_0) + \dots + X^{n-m})$. Heraf følger imidlertid let, at $\varkappa(b_i) = 0$ og $\varkappa(c_j) = 0$. hvilket specielt giver $\varkappa(c_0) = 0$ og $\varkappa(b_0) = 0$, altså $\pi \mid b_0$ og $\pi \mid c_0$, og dermed $\pi^2 \mid b_0 c_0 = a_0$. ∎

Eks. $X^n \pm p$ er irreducibel over $\mathbb{Z}$ ($\mathbb{Q}$), hvis p er et primtal

Sætning. $f(X) = \frac{X^n - 1}{X - 1} = X^{n-1} + \dots + X + 1$ er irreducibel over $\mathbb{Z}$ ($\mathbb{Q}$),

hvis og kun hvis n er et primtal.

Bevis. Hvis n er et primtal, er f(X+1) er Eisensteinpol. ∎

Eks. Hvis Kar(K) = 2 er $X^2+Y^2-1 \in K[X,Y]$ reducibel, thi $X^2+y^2-1 = (X+Y)^2-1 = (X+Y-1)(X+Y+1)$

Sætning. X^n+Y^n-1 er irreducibel over legemet K $\iff$ Kar(K) = 0 eller $0 < Kar(K) \nmid n$.

Bevis. "$\Rightarrow$" Indirekte: Hvis $Kar(K) = p \mid n$, er $X^n+Y^n-1 = (X^{\frac{n}{p}})^p+(Y^{\frac{n}{p}})^p-$
$= (X^{\frac{n}{p}}+Y^{\frac{n}{p}})^p-1 = (X^{\frac{n}{p}}+Y^{\frac{n}{p}}-1)((X^{\frac{n}{p}}+Y^{\frac{n}{p}})^{p-1}+\ldots+(X^{\frac{n}{p}}+Y^{\frac{n}{p}})+1)$
"$\Leftarrow$" Vi har $f(X,Y) \in K[X,Y] = K[Y][X] = R[X]$. Nu er $X^n+Y^n-1 = X^n+(Y^n-1) = X^n+((Y-1)+1)^n-1 = X^n+((Y-1)^n+\binom{n}{1}(Y-1)^{n-1}+\ldots+n(Y-1))$.
Det ses, at Y-1 går op, men $(Y-1)^2$ går ikke op, da $n(Y-1) \neq 0$.
Da Y-1 er primelement i R, følger påstanden af kriteriet. ∎

Lad K være et legeme og sæt $R = K[X_1,\ldots,X_n]$. Til $\tau \in S_n$ svarer en automorfi τ af R defineret ved $\tau(a) = a$ for $a \in K$, $\tau(X_i) = X_{\tau(i)}$ $i = 1,\ldots,n$. For $f(X_1,\ldots,X_n) = \sum a_{m_1,\ldots,m_n} X_1^{m_1}\ldots X_n^{m_n}$, har vi altså $\tau f = \sum a_{m_1,\ldots,m_n} X_{\tau(1)}^{m_1}\ldots X_{\tau(n)}^{m_n} = \sum a_{m_1,\ldots,m_n} X_1^{m_{\tau^{-1}(1)}} \ldots X_n^{m_{\tau^{-1}(n)}}$
$f \in R$ kaldes symmetrisk, hvis $\tau f = f$ for alle $\tau \in S_n$.

Vi betragter nu $R[Z] = K[X_1,\ldots,X_n][Z]$. Automorfien τ i R inducerer en automorfi τ i R[Z] ved $\tau(b_0+b_1Z+\ldots+b_mZ^m) = \tau(b_0)+\tau(b_1)Z+\ldots+\tau(b_m)Z^m$. Nu defineres elementer $s_0,s_1,\ldots,s_n \in R$ ved

$$F(Z) = (Z-X_1)\ldots(Z-X_n) = s_0Z^n-s_1Z^{n-1}+\ldots+(-1)^n s_n$$

og da $\tau(F) = (Z-X_{\tau(1)})\ldots(Z-X_{\tau(n)}) = (Z-X_1)\ldots(Z-X_n) = F$, er $\tau s_0 = s_0$, $\tau(s_1) = s_1,\ldots,\tau s_n = s_n$ for alle τ $\circlearrowright$: $s_0,s_1,\ldots,s_n$ er symmetriske
Vi finder:

$s_0 = 1$
$s_1 = X_1+\ldots+X_n$
$s_2 = X_1X_2+\ldots+X_{n-1}X_n$
$\vdots$
$s_n = X_1\ldots X_n$

og de kaldes de elementære symmetriske polynomier.

Sætning. Ethvert symmetrisk polynomium $f(X_1,\ldots,X_n) \in K[X_1,\ldots,X_n]$ kan på entydig måde skrives som polynomium i $s_1,\ldots,s_n$.

Bevis. Eksistens: For et potensprodukt $p = X_1^{m_1}\ldots X_n^{m_n}$ definerer vi signaturen som $sign(p) = (m_i) = (m_1,\ldots,m_n)$. Det ses let, at der ved $(\ell_i) \prec (m_i) \iff (\sum_i \ell_i < \sum_i m_i) \vee (\sum_i \ell_i = \sum_i m_i$ og $\ell_1 = m_1,\ldots,\ell_{\nu-1} = m_{\nu-1}, \ell_\nu < m_\nu$ for et vist ν) defineres en to-

tal ordning, $\succ$, af signaturerne. For $0 \neq f \in R$ defineres signaturen for f, sign(f), som den højest forekommende signatur i potensprodukterne i $f(X_1,\ldots,X_n)$. Idet vi bemærker, at $(\ell_i) \succ (m_i)$ og $(r_i) \succeq (s_i)$ medfører $(\ell_i+r_i) \succ (m_i+s_i)$, får vi let: For $f,g \neq 0$ er

$$\operatorname{sign}(fg) = \operatorname{sign}(f)+\operatorname{sign}(g).$$

Lad nu $0 \neq f(X_1,\ldots,X_n)$ være et symmetrisk polynomium, og lad $aX_1^{m_1}\ldots X_n^{m_n}$ være leddet med højest forekommende signatur (m_i), da er $m_1 \geq m_2 \geq \ldots \geq m_n$, thi var et $m_i < m_{i+1}$, og betragtes $\tau = (i,i+1) \in S_n$, ville $\tau(aX_1^{m_1}\ldots X_n^{m_n}) = aX_1^{m_1}\ldots X_i^{m_{i+1}}X_{i+1}^{m_i}\ldots X_n^{m_n}$ være et led i $f(X_1,\ldots,X_n)$ med signatur $(\ldots,m_{i+1},m_i,\ldots) \succ (\ldots,m_i,m_{i+1},\ldots)$

Vi bemærker nu, at $\operatorname{sign}(s_\nu) = (\overbrace{1,\ldots,1}^{\nu},0,\ldots,0)$, så at $\operatorname{sign}(s_\nu^{\alpha_\nu}) = \alpha_\nu(1,\ldots,1,0,\ldots,0) = (\alpha_\nu,\ldots,\alpha_\nu,0,\ldots,0)$ og dermed $\operatorname{sign}(s_1^{\alpha_1}\ldots s_n^{\alpha_n}) = (\alpha_1+\ldots+\alpha_n, \alpha_2+\ldots+\alpha_n, \ldots, \alpha_{n-1}+\alpha_n, \alpha_n)$.

Sættes $\alpha_n = m_n, \alpha_{n-1} = m_{n-1}-m_n, \ldots, \alpha_1 = m_1-m_2$, får vi altså $\operatorname{sign}(s_1^{\alpha_1}\ldots s_n^{\alpha_n}) = (m_i)$. For $f_1 = f - as_1^{\alpha_1}\ldots s_n^{\alpha_n} = f - as_1^{m_1-m_2}s_2^{m_2-m_3}\ldots s_{n-1}^{m_{n-1}-m_n}s_n^{m_n}$ gælder altså enten $f_1 = 0$, og så er vi færdige, eller $\operatorname{sign}(f_1) \prec \operatorname{sign}(f)$. Da f_1 er symmetrisk, kan denne proces anvendes på f_1, men dette må stoppe, da der kun findes endelig mange signaturer $\prec$ en given. ∎

Entydighed: Det er øjensynlig nok at vise, at vi for $\varphi(X_1,\ldots,X_n) \neq 0$ har $\varphi(s_1,\ldots,s_n) \neq 0$. For et potensprodukt $X_1^{\mu_1}\ldots X_n^{\mu_n}$ definerer vi den summatoriske signatur som $(\mu_1+\ldots+\mu_n, \mu_2+\ldots+\mu_n, \ldots, \mu_{n-1}+\mu_n, \mu_n)$. Lad $aX_1^{\mu_1}\ldots X_n^{\mu_n}$ være leddet med højest summatorisk signatur. Indsættes s'erne finder vi $\operatorname{sign}(as_1^{\mu_1}\ldots s_n^{\mu_n}) = \operatorname{sign}(a(X_1+\ldots+X_n)^{\mu_1}\ldots(X_1\ldots X_n)^{\mu_n}) = (\mu_1+\ldots+\mu_n, \ldots, \mu_{n-1}+\mu_n, \mu_n)$, og dette led i $\varphi(s_1,\ldots,s_n) = \varphi(X_1+\ldots+X_n,\ldots,X_1\ldots X_n)$ vil have højere signatur end noget andet led. Altså er $\varphi(s_1,\ldots,s_n) \neq 0$. ∎

Eks. Specielle symmetriske polynomier er potenssummerne $p_i = X_1^i+\ldots+X_n^i$, $i = 0,1,2,\ldots$ Disse kan iflg. sætningen entydigt udtrykkes ved de elementarsymmetriske polynomier. At der omvendt gælder: De elementarsymmetriske polynomier $s_1,\ldots,s_n$ kan entydigt skrives som polynomium i potenssummerne $p_1,\ldots,p_n$, vil følge af Newtons formel: Sættes $a_\nu = (-1)^\nu s_\nu$, $\nu = 0,1,\ldots,n$ og $a_\nu = 0$ for $\nu > n$ gælder:

Newtons formel: $\sum_{\nu=0}^{q-1} p_{q-\nu}a_\nu + qa_q = 0$, $q = 1,2,\ldots$

Bevis. For $\nu = 1,2,\ldots,q$ gælder (idet $\sum^*$ betegner summation over indb.forsk. indices fra 1 til n):

$$p_{q-\nu}(\nu! a_\nu) = (\sum_i X_i{}^{q-\nu})(-1)^\nu \sum^{*}_{i_1,\cdots,i_\nu} X_{i_1}\cdots X_{i_\nu} =$$

$$= (-1)^\nu \sum^{*}_{i_1,\cdots,i_\nu} \sum_{i_{\nu+1}} X_{i_1}\cdots X_{i_\nu} X_{i_{\nu+1}}{}^{q-\nu}$$

$$= (-1)^\nu \nu \sum^{*}_{i_1,\cdots,i_\nu} X_{i_1}\cdots X_{i_\nu}{}^{1+q-\nu} + (-1)^\nu \sum^{*}_{i_1,\cdots,i_{\nu+1}} X_{i_1}\cdots X_{i_\nu} X_{i_{\nu+1}}{}^{q-\nu}$$

hvoraf

$$(*)\quad p_{q-\nu} a_\nu = \frac{(-1)^\nu}{(\nu-1)!} \sum^{*}_{i_1,\cdots,i_\nu} X_{i_1}\cdots X_{i_\nu}{}^{q-(\nu-1)} + \frac{(-1)^\nu}{\nu!} \sum^{*}_{i_1,\cdots,i_{\nu+1}} X_{i_1}\cdots X_{i_\nu} X_{i_{\nu+1}}{}^{q-\nu}$$

$$= -S(\nu-1)+S(\nu),$$

hvor

$$S(\mu) = \frac{(-1)^\mu}{\mu!} \sum^{*}_{i_1,\cdots,i_{\mu+1}} X_{i_1}\cdots X_{i_\mu} X_{i_{\mu+1}}{}^{q-\mu}, \quad \mu = 0,\ldots,q$$

Specielt er

$S(0) = \sum_{i_1} X_{i_1}{}^q = p_q$,

$S(q) = 0$ for $q \geq n$ og for $q < n$ er

$$S(q) = \frac{(-1)^q}{q!} \sum^{*}_{i_1,\cdots,i_{q+1}} X_{i_1}\cdots X_{i_q} X_{i_{q+1}}{}^0 = \frac{(-1)^q}{q!} \sum_{i_1,\cdots,i_q} X_{i_1}\cdots X_{i_q}(n-q)$$

$= (n-q)a_q$. Altså for alle q:

$S(q) = (n-q)a_q$

Newtons formel følger nu af (*) ∎

KAPITEL III ALGEBRAISKE UDVIDELSER

Lad $K \subseteq L$ være legemer, og $\alpha \in L$. Ved $\varphi(f) = f(\alpha)$ defineres en surjektiv homomorfi $\varphi : K[X] \to K[\alpha] \subseteq L$, så $K[\alpha]$ er et integritetsområde, og det er den mindste ring, der indeholder K og $\alpha \in L$. Nu er $\mathrm{Ker}\varphi$ et ideal i $K[X]$, der er P.I.D., så $\mathrm{Ker}\varphi = (p(X))$. Da $K[X]/(p(X)) \cong K[\alpha]$ er et integritetsområde, er $(p(X))$ et primideal. Der er nu to muligheder: 1) $p(X) = 0$, da er α ikke rod i noget polynomium over K; α kaldes transcendent over K. $K[\alpha] \cong K[X]$ er ikke et legeme, og vi har $K[\alpha] \cong K[X] \subset K(X) \cong K(\alpha) \subseteq L$. 2) $p(X) \neq 0$, da er $p(X)$ irreducibel, og $(p(X))$ er maximalt, så $K[\alpha] \cong K[X]/(p(X))$ er et legeme, altså $K[\alpha] = K(\alpha)$. α kaldes algebraisk over K. α er rod i et egentligt polunomium over K, og alle polynomier med α som rod er multipla af $p(X)$. Hvis $p(X)$ er normeret, er det altså entydigt fastlagt og betegnes $p(X) = \mathrm{Irr}(\alpha, K)$, undertiden kaldet α's minimale polynomium over K. Hvis $\mathrm{grad}(p) = n$, siges α at have grad n over K. Ethvert element i $K[X]/(p(X))$ kan da entydigt skrives $a_0+a_1X+\ldots+a_{n-1}X^{n-1}$ iflg. divisionsalgoritmen; da $a_0+\ldots+a_{n-1}X^{n-1} \leftrightarrow a_0+\ldots+a_{n-1}\alpha^{n-1}$, får vi

Sætning. *Hvis α er algebraisk over K, af grad n, da kan ethvert element i $K(\alpha) = K[\alpha]$ på entydig måde skrives $a_0+a_1\alpha+\ldots+a_{n-1}\alpha^{n-1}$*

Sagt på en anden måde: Hvis vi opfatter $K[\alpha]$ som vektorrum over K, ser vi: Hvis α er transcendent, er $[K[\alpha]:K] = \infty$ og en K-basis for $K[\alpha]$ er $1, \alpha, \alpha^2, \ldots$; Hvis α er algebraisk af grad n, er $[K[\alpha]:K] = n$, og en basis er $1, \alpha, \ldots, \alpha^{n-1}$.

Sætning. *Mængden af de elementer i L, der er algebraiske over K, er et dellegeme, L_1, af L.*

Bevis. Lad $\alpha, \beta \in L$, $\mathrm{grad}\alpha = m$, $\mathrm{grad}\beta = n$. Enhver potens α^ν tilhører $K[\alpha]$, og er altså en K-lin.komb. af α^i, $i = 0,\ldots,m-1$. Ligeledes er enhver potens β^μ en K-lin.komb. af β^j, $j = 0,\ldots,n-1$. Ethvert produkt $\alpha^\nu\beta^\mu$ er således en K-lin.komb. af $\alpha^i\beta^j$ $i = 0,,,m-1$, $j = 0,\ldots,n-1$.

Til $\alpha+\beta$ findes følgelig en $(mn \times mn)$- matrix $\underline{\underline{A}}$ med elementer fra K, så

$$(\alpha+\beta)\begin{Bmatrix} 1 \\ \alpha \\ \vdots \\ \alpha^{m-1} \\ \beta \\ \alpha\beta \\ \vdots \\ \alpha^{m-1}\beta^{n-1} \end{Bmatrix} = \underline{\underline{A}} \begin{Bmatrix} 1 \\ \alpha \\ \vdots \\ \alpha^{m-1} \\ \beta \\ \alpha\beta \\ \vdots \\ \alpha^{m-1}\beta^{n-1} \end{Bmatrix}$$

og dermed

$\det(\underline{\underline{A}} - (\alpha+\beta)\underline{\underline{E}}) = 0$. $\det(\underline{\underline{A}} - X\underline{\underline{E}}) \in K[X]$ er følgeligt et egentligt polynomium med $\alpha+\beta$ som rod. Analogt for $\alpha\beta$, $-\alpha$ og α^{-1}. ∎

Hvis $K \subsetneq L_1 (\subsetneq L)$, siges L_1 at være <u>algebraisk</u> over K (eller en <u>algebraisk udvidelse</u> af K), hvis ethvert element i L_1 er algebraisk over K, og vi skriver da også "<u>L_1/K er algebraisk</u>"

Korollar. <u>Hvis α er algebraisk af grad n over K, da er $K(\alpha)/K$ algebraisk.</u>

Opgave. L/K er algebraisk, hvis og kun hvis enhver ring R mellem K og L er et legeme.

Et legeme $L_1 \supsetneq K$ kaldes en <u>endelig udvidelse</u> af K, hvis $[L_1:K]$ er endelig. Vi har set, at hvis $\alpha \in L$ er algebraisk over K, da er $K(\alpha)/K$ en endelig udvidelse.

Sætning. <u>En endelig udvidelse, L/K, er algebraisk</u>.
Bevis. Antag, at $[L:K] = n < \infty$, og lad $\alpha \in L$. Da $1,\alpha,\ldots,\alpha^n$ er lin.uafh. over K findes $a_0,\ldots,a_n \in K$, ikke alle 0, så at $a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0$, ɔ: α er rod i et egentligt polynomium $\in K[X]$. ∎

Heraf følger atter, at $K(\alpha) = K[\alpha]/K$ er algebraisk, hvis α er algebraisk.

Eks. Lad L_1 være mængden af reelle tal, der er algebraiske over $\dot{\mathbb{Q}}$, da er $[L_1:\dot{\mathbb{Q}}] = \infty$, thi for alle $n \in \dot{\mathbb{N}}$ er $1, \sqrt[n+1]{2}, (\sqrt[n+1]{2})^2, \ldots, (\sqrt[n+1]{2})^n$ lin.uafh. over $\dot{\mathbb{Q}}$, da $X^{n+1}-2$ er irreducibel over $\dot{\mathbb{Q}}$. ∎

En udvidelse L/K kaldes <u>simpel</u>, hvis der findes $\alpha \in L$ så at $L = K(\alpha)$.

Eks. En endelig udvidelse er ikke nødvendigvis simpel. Lad $k = GF(2)$, lad $L = k(X,Y)$ og $K = k(X^2,Y^2)$, da er $1,X,Y,XY$ en K-basis for L. For $f/g \in L$, har vi, da Kar = 2, at $f/g = gf/g^2 = g(X,Y)f(X,Y)/g(X^2,Y^2)$; det er altså nok at vise, at hvert $f(X,Y) \in k[X,Y]$ er lin.komb. $1,X,Y,XY$, samt at disse elementer er K-uafh. Det første følger let ved at betragte produkter X^iY^j, og for det sidste er det tilstrakkeligt at vise, at for $f,g,h,k \in k[X^2,Y^2]$ gælder $f(X^2,Y^2)XY + g(X^2,Y^2)Y + h(X^2,Y^2)X + k(X^2,Y^2) = 0 \Rightarrow f = g = h = k = 0$, men dette ses ved at betragte potenserne X^iY^j. L/K er følgelig endelig

af grad 4, men da vi for $\alpha \in L$ har $\alpha^2 \in K$, har en simpel udvidelse grad ≤ 2. L/K er således ikke simpel.

sætning. Lad $K \subseteq L \subseteq M$ være legemer, da er $[M:L][L:K] = [M:K]$
Bevis. Hvis $[L:K] = \infty$ eller $[M:L] = \infty$ er $[M:K] = \infty$. Lad nu $v_1,\ldots,v_m$ være en L-basis for M, og lad $u_1,\ldots,u_n$ være en K-basis for L, da ses det let, at $\{u_i v_j \mid 1 \leq i \leq n \wedge 1 \leq j \leq m\}$ er en K-basis for M ∎

Sætning. Er $K \subseteq L$, og $\alpha_1,\ldots,\alpha_m \in L$ algebraiske over K, da er $K(\alpha_1,\ldots,\alpha_m) = K[\alpha_1,\ldots,\alpha_m]$, og $K(\alpha_1,\ldots,\alpha_m)$ er en endelig udvidelse af K.
Bevis. Da α_1 er alg. over K, er $K(\alpha_1) = K[\alpha_1]$ og $[K(\alpha_1):K]$ er endelig. Da α_2 er alg. over K, er α_2 specielt alg. over $K(\alpha_1)$, så $K(\alpha_1)(\alpha_2) = K(\alpha_1)[\alpha_2]$ og dermed $K(\alpha_1,\alpha_2) = K(\alpha_1)(\alpha_2) = K(\alpha_1)[\alpha_2]$ $= K[\alpha_1][\alpha_2] = K[\alpha_1,\alpha_2]$, og da $[K(\alpha_1,\alpha_2):K(\alpha_1)]$ er endelig, er også $[K(\alpha_1,\alpha_2):K]$ endelig iflg den forrige sætning o.s.v. ∎

Korollar. Hvis $K \subseteq L \subseteq M$, så M/L og L/K er algebraiske, da er også M/K algebraisk.
Bevis. Et $\beta \in M$ er algebraisk over L, så der findes $\alpha_0,\ldots,\alpha_{n-1} \in L$ så at β er rod i $\alpha_0+\alpha_1 X+\ldots+\alpha_{n-1}X^{n-1}+X^n \in L[X]$. Nu er $\alpha_0,\ldots,\alpha_{n-1}$ algebraiske over K, så $K(\alpha_0,\ldots,\alpha_{n-1})$ er endelig over K. Da β er algebraisk over $K(\alpha_0,\ldots,\alpha_{n-1})$ er $K(\alpha_0,\ldots,\alpha_{n-1})[\beta] = K(\alpha_0,\ldots,\alpha_{n-1},\beta)$ endelig over $K(\alpha_0,\ldots,\alpha_{n-1})$, og derfor endelig over K. Specielt er β algebraisk over K, da en endelig udvidelse er algebraisk. ∎

Lad $K \subseteq L$. Vi har tidligere vist, at mængden $\tilde{K}$ af elementer i L, algebraiske over K, er et dellegeme af L. Det kaldes K's algebraisk afsluttede hylster i L, Det foregående korollar viser nu, at $\tilde{\tilde{K}} = \tilde{K}$.

Eks. Lad $K \subseteq L$, og lad $\alpha \in L$ være transcendent over K, og lad $\tilde{K}$ være K's alg. afsluttede hylster i $K(\alpha)$, da er $\tilde{K} = K$. Lad nemlig $\beta \in \tilde{K}$, altså $\beta = f(\alpha)/g(\alpha) \in K(\alpha)$ alg. over K, og $K(\beta)/K$ algebraisk. Hvis $\beta \notin K$, er $f(X) - \beta g(X) \in K(\beta)[X]$ ikke nulpolynomiet, og da det har α som rod, er α alg. over $K(\beta)$, og dermed også over K, hvilket er en modstrid. □

Lad K være et legeme, og $f(X) \in K[X]$ af grad(f) ≥ 1, da findes

en simpel algebraisk udvidelse af K indenfor hvilken f(X) har en rod, idet der gælder

Sætning. Er $f(X) = X^n+a_1X^{n-1}+\ldots+a_n \in K[X]$ irreducibel, da findes et (og på nær isomorfi kun ét) legeme L^*, med dellegeme K^* isomorft med K (ved $K \xrightarrow{\varphi} K^*$), og et element $\alpha^* \in L^*$, algebraisk over K^*, så at $L^* = K^*(\alpha^*)$ og $\mathrm{Irr}(\alpha^*,K^*) = X^n+\varphi(a_1)X^{n-1}+\ldots+\varphi(a_n) = \varphi f$.

Bevis. Eksistens: $L^* = K[X]/(f(X))$ er et legeme, og elementerne i L^* er af formen $\overline{b_0+b_1X+\ldots+b_{n-1}X^{n-1}} = \overline{b_0} + \overline{b_1}\,\overline{X} + \ldots + \overline{b_{n-1}}\,\overline{X}^{n-1}$. Sæt $\varphi(a) = \overline{a} \in L^*$ for $a \in K$, da er φ en isomorfi af K på et dellegeme $K^* \subseteq L$. Sæt $\alpha^* = \overline{X} \in L^*$, da er α^* rod i $\varphi f \in K^*[X]$, thi $\varphi f(\alpha^*) = \varphi f(\overline{X}) = \overline{X}^n + \overline{a_1}\,\overline{X}^{n-1}+\ldots+\overline{a_n} = \overline{X^n+\ldots+a_n} = \overline{0}$, så α^* er algebraisk over K^*. Da f er irreducibel over K og $\varphi: K \to K^*$ er en isomorfi, er φf irreducibel over K^*, d: $\varphi f = \mathrm{Irr}(\alpha^*,K^*)$, og vi har øjensynlig $L^* = K^*(\alpha^*)$.

Entydighed: vil følge af

Lemma. Lad $L \supseteq K$, $L^* \supseteq K^*$ og φ: K på K^* en isomorfi. Hvis $L = K(\alpha)$, hvor $\alpha \in L$ er algebraisk over K, hvis $L^* = K^*(\alpha^*)$, hvor $\alpha^* \in L^*$ er algebraisk over K^* og hvis $\varphi(\mathrm{Irr}(\alpha,K)) = \mathrm{Irr}(\alpha^*,K^*)$, da kan φ entydigt fortsættes til en isomorfi $\bar{\varphi}: L$ på L, så at $\bar{\varphi}(\alpha) = \alpha^*$.

Bevis. Ethvert element $\beta \in L$ kan skrives $\beta = b_0+b_1\alpha+\ldots$, så den eneste mulighed for at definere $\bar{\varphi}$ er $\bar{\varphi}(\beta) = \bar{\varphi}(b_0+b_1\alpha+\ldots) = \varphi(b_0)+\varphi(b_1)\alpha^*+\ldots$. Da $\varphi(\mathrm{Irr}(\alpha,K)) = \mathrm{Irr}(\alpha^*,K^*)$ er dette virkelig en definition, og det ses let, at $\bar{\varphi}$ opfylder de stillede krav. ∎

Det herved entydigt bestemte legeme siges at fremgå af K ved adjunktion af en rod i f(X); vi vil ofte identificere K og K^*.

Sætning. Lad $f(X) \in K[X]$ være af $\mathrm{grad}(f) = n \geq 1$, da findes en (og på isomorfi nær) kun én endelig udvidelse L/K, så at f(X) spaltes til bunds i førstegradsfaktorer i L[X], og som er minimal (d: intet ægte dellegeme af L har denne egenskab)

Bevis. Eksistens: Lad $f(X) = p_1(X)\ldots p_\nu(X)$, hvor $p_\iota(X) \in K[X]$ er irreducibel. Hvis alle p_ι har grad 1 er vi færdige. Ellers kan vi antage at $\mathrm{grad}(p_1) > 1$. Nu adjungeres en rod α_1 i $p_1(X)$ til K, så $K \subset K(\alpha_1)$. Lad f(X)'s opspaltning i irreducible faktorer i $K(\alpha_1)[X]$ være $f(X) = (X-\alpha_1)p_1'(X)\ldots p_\nu'(X)$. Hvis alle p_ι' er af grad 1 er vi færdige. Ellers kan vi antage, at $\mathrm{grad}(p_1') > 1$. Adjungeres en rod α_2 i $p_1'(X)$ til $K(\alpha_1)$, er $K \subset K(\alpha_1) \subset K(\alpha_1)(\alpha_2) = K(\alpha_1,\alpha_2)$ o.s.v. Dette må imidlertid stoppe, da f(X) højst har n rødder, så $K \subset K(\alpha_1) \subset \ldots \subset K(\alpha_1,\ldots,\alpha_\mu) = L$, hvor $\mu \leq n$. $L = K(\alpha_1,\ldots,\alpha_\mu)$ er en endelig udvidelse af K, og den er klart minimal.

Entydighed: vil følge af

Lemma. Lad $L \supseteq K$, $L^* \supseteq K^*$ og φ: K på K^* være en isomorfi. Hvis L er en minimal udvidelse af K, så $f(X) \in K[X]$ spaltes til bunds i 1.gradsfaktorer, og hvis det samme gælder for L^* og K^* med $\varphi f \in K^*[X]$, da kan φ fortsættes (ikke entydigt) til en isomorfi Φ: L på L^*.

Bevis. Induktion efter grad(f) = n. Klart, hvis n = 1, da vi så har $L = K \cong K^* = L^*$. Antag sætningen for polynomier af grad $\leq n-1$, og lad $f(X) = p_1(X)\ldots p_\nu(X) \in K[X]$ være af grad n med $p_\iota(X) \in K[X]$ irreducibel. Nu er $\varphi f(X) = \varphi p_1(X)\ldots\varphi p_\nu(X)$, og da φ er en isomorfi er $\varphi p_\nu(X) \in K^*[X]$ irreducibel. Lad $\alpha \in L$ så at $p_1(\alpha) = 0$, og lad $\alpha^* \in L^*$, så $\varphi p_1(\alpha^*) = 0$. Iflg. forrige lemma kan φ (entydigt) fortsættes til en isomorfi $\varphi_1 : K(\alpha)$ på $K^*(\alpha^*)$ med $\varphi_1(\alpha) = \alpha^*$. M Vi har $p_1(X) = (X-\alpha)q(X)$ i $K(\alpha)$ og $\varphi p_1(X) = (X-\alpha^*)\varphi_1 q(X)$ i $K^*(\alpha^*)$. Nu er L det mindste legeme, der indeholder $K(\alpha)$, så at $f(X) \in K(\alpha)[X]$ spaltes til bunds, og L^* har samme egenskaber med $\varphi_1 f(X)$ og $K^*(\alpha^*)$. Da $f(X) = (X-\alpha)q(X)p_2(X)\ldots p_\nu(X)$ og $\varphi_1 f(X) = (X-\alpha^*)\varphi_1 q(X)\varphi p_2(X)\ldots \varphi p_\nu(X)$, ses det, at L er den mindste udvidelse af $K(\alpha)$, så at $q(X)p_2(X)\ldots p_\nu(X) \in K(\alpha)[X]$ spaltes til bunds, og at L^* har samme egenskab med $K^*(\alpha^*)$ og $\varphi_1(q(X)p_2(X)\ldots p_\nu(X)) = \varphi_1 q(X)\varphi p_2(X)\ldots\varphi p_\nu(X) \in K^*(\alpha^*)[X]$. Af induktionsantagelsen følger nu, at L og L^* er isomorfe. ∎

Dette (på isomorfi nær) entydigt bestemte legeme $L \supseteq K$, i hvilket $f(X) \in K[X]$ spaltes til bunds, kaldes f(X)'s spaltningslegeme over K (eller rodlegeme)

EKSEMPLER PA ANVENDELSE AF SPALTNINGSLEGEME:

1) Bevis for algebraens fundamentalsætning. Vi skal vise, at hvert $f(X) \in \grave{C}[X]$ har mindst en rod i $\grave{C}$. Det er tilstrækkeligt at vise dette for polynomier $\in \grave{R}[X]$, thi $f(X)\bar{f}(X) \in \grave{R}[X]$, og hvis $f(\alpha)\bar{f}(\alpha) = 0$ for et $\alpha \in \grave{C}$, er $f(\alpha) = 0$ eller $f(\bar{\alpha}) = 0$. Sæt grad(f) $= n = 2^\ell u$, hvor u er ulige. Induktion efter ℓ. For $\ell = 0$ er dette et velkendt resultat (Weierstrass). Antag sætningen for $\ell-1$. $f(X) \in \grave{R}[X] \subset \grave{C}[X]$. f(X)'s spaltningslegeme over $\grave{C}$ kaldes L. Vi har da $f(X) = X^n + a_1X^{n-1} + \ldots + a_n = (X-\alpha_1)\ldots(X-\alpha_n)$, $\alpha_i \in L$ hvor $a_1, \ldots, a_n \in \grave{R}$.

Vi sætter for $c \in \grave{R}$: $g_c(X) = \prod_{i<j}(X-(\alpha_i+\alpha_j+c\alpha_i\alpha_j))$ og finder $\operatorname{grad}(g_c) = n' = \binom{n}{2} = \frac{1}{2}n(n-1) = 2^{\ell-1}u(2^\ell u-1) = 2^{\ell-1}u'$. Vi har

$$g_c(X) = X^{n'} + h_1(\alpha_1,\ldots,\alpha_n)X^{n'-1} + \ldots + h_{n'}(\alpha_1,\ldots,\alpha_n)$$

hvor h_i'erne er polynomier i $\alpha_1,\ldots,\alpha_n$ med reelle koefficienter

Endvidere er h_i'erne øjensynlig symmetriske polynomier, og kan derfor skrives som reelle polynomier i de elementarsymmetriske polynomier $-a_1,\ldots,(-1)^n a_n$, som er reelle; følgelig er $h_i(\alpha_1,\ldots,\alpha_n) \in \grave{R}$, d: $g_c(X) \in R[X]$. Iflg. induktionsantagelsen har $g_c(X)$ en rod i $\grave{C}$, d.v.s. der findes $i < j$, så at $\alpha_i+\alpha_j+c\alpha_i\alpha_j \in \grave{C}$. Til hvert $c \in \grave{R}$ svarer et par: $i < j$ så at $\alpha_i+\alpha_j+c\alpha_i\alpha_j \in \grave{C}$. Betragtes $\binom{n}{2}+1$ forskellige c'er, må mindst to, c,c' svare til samme par $i < j$, altså $\alpha_i+\alpha_j+c\alpha_i\alpha_j \in \grave{C}$ og $\alpha_i+\alpha_j+c'\alpha_i\alpha_j \in \grave{C}$. Heraf fås $(c-c')\alpha_i\alpha_j \in \grave{C}$, men så er $\alpha_i\alpha_j \in \grave{C}$, og dermed også $\alpha_i+\alpha_j \in \grave{C}$. Da fundamentalsætningen som bekendt gælder for polynomier af grad 2, slutter vi endelig at $\alpha_i,\alpha_j \in \grave{C}$. ∎

2) <u>$X^p-X-1 \in \grave{Q}[X]$ er irreducibel for et primtal p.</u>

Bevis. Idet vi har den kann. hom. $\varkappa : \grave{Z} \to \grave{Z}/p\grave{Z} = k$ er det øjensynligt nok at vise, at $f(X) = X^p-X-1$ er irreducibel over k. f(X)'s spaltningslegeme over k kaldes L. f(X) har ingen rødder i k, da $a^p-a-1 = -1$ for alle $a \in k$. Lad nu $\alpha \in L$ være rod i f(X). Da L/k er endelig, er $c \to c^p$, $c \in L$ en automorfi i L, og dermed $(\alpha+1)^p-(\alpha+1)-1 = \alpha^p+1-(\alpha+1)-1 = \alpha^p-\alpha-1 = 0$. Vi kan således finde p rødder: $\alpha,\alpha+1,\ldots,\alpha+p-1$, og har

$$f(X) = (X-\alpha)(x-(\alpha+1))\ldots(X-(\alpha+p-1)).$$

En ægte divisor $g(X) \in k[X]$ af f(X) måtte være af formen $g(X) = \prod_{i=1}^{\nu}(X-\alpha-a_i)$, med $a_i \in k$, hvor $1 \leq \nu = \operatorname{grad}(g) < p$. Koefficienten til $X^{\nu-1}$ er $-\nu\alpha-\sum_{i=1}^{\nu}a_i \in k$, og da $\nu \in k$, $\nu \neq 0$, ville dette medføre, at $\alpha \in k$. ∎

3) <u>$f(X) = X^p-t$ er irreducibel over $\grave{F}_p(t)$.</u> ($\grave{F}_p = \grave{Z}/\grave{Z}p$)

Bevis. Elementerne i $\grave{F}(t)$ er af formen $h(t)/k(t)$, hvor $h,k \in \grave{F}[t]$, og for disse gælder $(h(t)/k(t))^p = h(t^p)/k(t^p) \neq t$. Lad L være spaltningslegemet for X^p-t over $\grave{F}(t)$. Er $\beta \in L$ en rod i f(X), er $\beta^p = t$, så $\beta \notin \grave{F}(t)$. Da $X^p-t = X^p-\beta^p = (X-\beta)^p$ er β en p-dobbelt rod i f(X). Hvis $f(X) \in \grave{F}(t)[X]$ havde en ægte divisor $g(X) \in \grave{F}(t)[X]$, måtte $g(X) = \prod_{i=1}^{\nu}(X-\beta)$, hvor $1 \leq \nu = \operatorname{grad}(g) < p$, altså specielt $\beta^{\nu} \in \grave{F}(t)$. Da $(\nu,p) = 1$, findes a,b, så at $a\nu+bp = 1$, men så er $\beta = \beta^{a\nu+bp} = (\beta^{\nu})^a t^b \in \grave{F}(t)$, hvilket er en modstrid. ∎

For $f(X) = \sum_{m \geq 0} a_n X^n \in K[X]$, sættes $f'(X) = \sum_{m \geq 0} n a_n X^{n-1} \in K[X]$. Der gælder øjensynligt

$$(f+g)' = f'+g' \qquad (kf)' = kf' \qquad (fg)' = f'g+fg'.$$

Lad nu $f(X) \in K[X]$ være et irreducibelt polynomium, og lad $L \supset K$

være en udvidelse af K, der indeholder en multipel rod, α, i f(X). Af $f(X) = (X-\alpha)^2 g(X)$ fås $f'(X) = (X-\alpha)2g(X) + (X-\alpha)^2 g'(X)$, så $f'(\alpha) = 0$. Heraf følger $f \mid f'$, men da $\text{grad}(f') \leq \text{grad}(f)-1$, slutter vi $f'(X) = 0$. $= \sum n a_n X^{n-1}$, altså at $na_n = 0$. Hvis Kar(K) = p får vi $p \mid n$ eller $p \nmid n$ og $a_n = 0$, så $f(X) = a_0 + a_p X^p + a_{2p} X^{2p} + \ldots$. Hvis Kar(K) = 0 er dette en modstrid, så

Sætning. Hvis Kar(K) = 0, og $f(X) \in K[X]$ er irreducibel, da har f(X) simple rødder i enhver udvidelse af K i hvilken f(X) spaltes til bunds.

Et irreducibelt polynomium $f(X) \in K[X]$ kaldes separabelt, hvis f(X) kun har simple rødder i spaltningslegemet.

Sætning. Hvis Kar(K) = p, og $f(X) \in K[X]$ er irreducibel, da er f(X) inseparabel $\Leftrightarrow$ $f(X) = g(X^p)$ for et vist $g(X) \in K[X]$.

Bevis. "$\Rightarrow$" er vist. "$\Leftarrow$": Hvis $f(X) = g(X^p)$, og α er en rod i f(X), da er α^p rod i g(X), så $g(X) = (X-\alpha^p)q(X)$, og dermed $f(X) = (X^p-\alpha^p)q(X^p) = (X-\alpha)^p q(X^p)$ ∎

Et polynomium $f(X) \in K[X]$ kaldes separabelt, hvis alle dets irreducible faktorer er separable. Vi siger, at K er fuldkomment, hvis ethvert polynomium over K er separabelt. Vi har set:

Sætning. Hvis Kar(K) = 0, da er K fuldkomment.

Sætning. Hvis Kar(K) = p, da er K fuldkomment $\Leftrightarrow$ $a \longrightarrow a^p$, $a \in K$, er en automorfi.

Bevis. "$\Leftarrow$": Hvis $f(X) = a_0 + \ldots +$ er irreducibel og inseparabel, da var $f(X) = a_0 + a_1 X^p + \ldots + a_h X^{ph}$; nu er $a_i = b_i{}^p$, og dermed $f(X) = b_0{}^p + \ldots + b_h{}^p X^{ph} = (b_0 + \ldots + b_h X^h)^p$ i modstrid med at f(X) vær irreducibel

"$\Rightarrow$". Hvis $a \longrightarrow a^p$ ikke var en automorfi, findes $b \in K$, så at $f(X) = X^p - b$ ikke har rødder i K. Nu er f(X) irreducibel (jfr 3. p.6), men der findes kun én p-dobbelt rod i spaltningslegemet. ∎

Korollar. Ethvert endeligt legeme er fuldkomment.

Sætning (Steinitz, 1871-1928). Lad $L = K(\alpha, \beta, \ldots, \mu)$, hvor $\alpha, \beta, \ldots, \mu$ er algebraiske over K, og hvor $\beta, \gamma, \ldots, \mu$ er separable over K, da er L/K en simpel udvidelse.

Bevis. Det er nok at vise, at $K(\alpha, \beta)$ er simpel over K, da vi i så fald har $K(\alpha, \beta, \gamma) = K(\alpha, \beta)(\gamma) = K(\vartheta)(\gamma) = K(\vartheta, \gamma)$ og ϑ er algebraisk over K. Beviset føres i to tilfælde:

1)K er et uendeligt legeme: Sættes $f(X) = \mathrm{Irr}(\alpha,K)$ $m = \mathrm{grad}(f)$, er $f(\alpha) = 0$, og sættes $g(X) = \mathrm{Irr}(\beta,K)$, $n = \mathrm{grad}(g)$, er $g(\beta) = 0$. Vi udvider nu $L = K(\alpha,\beta)$ til et legeme M, hvor f(X) og g(X) spaltes til bunds. Her har f(X) rødderne $\alpha = \alpha_1, \ldots, \alpha_m$ (ens eller forskellige) og g(X) rødderne $\beta = \beta_1, \ldots, \beta_n$ (forskellige). Vi vælger $\vartheta = \alpha + c\beta$, hvor $c \in K$, så at $\alpha_i + c\beta_k \neq \alpha + c\beta$ for alle i og alle $k \neq 1$, hvilket er muligt. Nu er $K(\vartheta) = K(\alpha+c\beta) = K(\alpha,\beta)$, thi $K(\vartheta) \subseteq K(\alpha,\beta)$. Vi har $f(\vartheta - cX) \in K(\vartheta)[X]$, og $f(\vartheta - cX)$ har roden $\beta_1 = \beta$, og $f(\vartheta - c\beta_k) \neq 0$, da $\vartheta - c\beta_k \neq \alpha_i$, alle i, $k \neq 1$. $d(X) = (g(X), f(\vartheta - cX))$ har altså kun én rod, nemlig $\beta_1 = \beta$, og da $d(X) = X - \beta \in K(\vartheta)[X]$, er $\beta \in K(\vartheta)$, så at også $\alpha = \vartheta - c\beta \in K(\vartheta)$, og dermed $K(\alpha,\beta) \subseteq K(\vartheta)$ ∎

2) Ker et endeligt legeme. Da L er en endelig udvidelse af K, er også L et endeligt legeme, så påstanden følger af

Sætning. I et endeligt legeme, L, er den multiplikative gruppe, L^*, cyklisk.

et specialtilfælde af

Sætning. Enhver endelig undergruppe i et legemes multiplikative gruppe er cyklisk.

Bevis. I den endelige undergruppe, $\mathcal{G}$, har $X^p - 1$ højst p rødder, så påstanden følger af

Lemma. ER $\mathcal{G}$ en endelig abelsk gruppe, og har $\mathrm{Ann}(p) = \{x \in \mathcal{G} \mid x^p = 1\}$ højst p elementer for ethvert primtal, p, da er $\mathcal{G}$ cyklisk.

Bevis. Lad $\mathcal{G} = \dot{Z}/p_1^{a_1}\dot{Z} \oplus \ldots \oplus \dot{Z}/p_r^{a_r}\dot{Z}$, da er $\mathcal{G}$ cyklisk netop hvis $p_1, \ldots, p_r$ er indbyrdes forskellige. I $\dot{Z}/p^a\dot{Z}$ har Ann(p) mindst p elementer; er nemlig α en frembringer, vil $\alpha^{p^{a-1}}$ frembringe en undergruppe af orden p; o: p elementer fra Ann(p). Hvis også $\dot{Z}/p^b\dot{Z}$ forekom i det direkte produkt, ville Ann(p) altså have mindst 2p-1 elementer. ∎

Bemærk. Steinitz' sætning gælder ikke i et skævlegeme. (Betragt fx. gruppen af kvaternionenheder).

Korollar. En endelig separabel udvidelse er simpel.

Korollar. En endelig udvidelse af et fuldkomment legeme er simpel.

ENDELIGE LEGEMER

Et endeligt legeme af Kar(K) = p har p^n elementer, hvilket ses ved at betragte K som vektorrum over $\dot{F}_p$.

Sætning. Til hver primtalspotens, p^n, findes et, og på isomorfi nær kun ét, legeme K med p^n elementer.

Bevis. Eksistens: Lad K være spaltningslegemet for polynomiet $X^{p^n}-X$ over $\grave{F}_p$. Alle rødder i $X^{p^n}-X$ er forskellige, thi var $X^{p^n}-X = (X-\alpha)^2 g(X)$, ses ved afledning, at $0 = p^n\alpha^{p^n-1}-1 = -1$. De p^n rødder i $X^{p^n}-X$ udgør hele K, thi er α,β rødder, er $(\alpha\pm\beta)^{p^n} = \alpha^{p^n}\pm\beta^{p^n} = \alpha\pm\beta$, $(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta$ og $(\frac{1}{\alpha})^{p^n} = \frac{1}{\alpha}$, så at rødderne udgør et legeme.

Entydighed: Er K et legeme med p^n elementer, er $\mathrm{Kar}(K) = p$. Den multiplikative gruppes orden er p^n-1, så for $\alpha \neq 0$ er $\alpha^{p^n-1} = 1$, så at alle elementer i K er rødder i $X^{p^n}-X$. K er nu spaltningslegemet for $X^{p^n}-X$ over $\grave{F}_p$, thi i $L \subset K$, kan $X^{p^n}-X$ ikke spaltes til bunds, da L har for få elementer. ∎

Det entydigt bestemte legeme kaldes Galoisfeltet med p^n elementer, og betegnes $GF(p^n)$ eller $\grave{F}_{p^n}$. Vi har set (p.8)

Sætning. Den multiplikative gruppe, $GF(p^n)^*$, er cyklisk.

Opg. $GF(p^m) \subseteq GF(p^n) \Leftrightarrow m|n$. "$\Rightarrow$" ses ved at betragte $GF(p^n)$ som vektorrum over $GF(p^m)$. "$\Leftarrow$" Hvis $m|n$ er $p^m-1 \mid p^n-1$ og dermed $X^{p^m-1}-1 \mid X^{p^n-1}-1$. Følgelig er $GF(p^n)$ = spaltningslegemet for $X^{p^n-1}-1$ over $\grave{F}_p \supseteq$ spaltningslegemet for $X^{p^m-1}-1$ over $\grave{F}_p = GF(p^m)$.

Opg. Over $\grave{F}_p$ findes irreducible polynomier af enhver grad, thi $GF(p^n) = \grave{F}_p(\vartheta)$, og dermed $\mathrm{grad}(\mathrm{Irr}(\vartheta;\grave{F}_p)) = n$. Lad $\pi(n)$ betegne antallet af irreducible polynomier af grad n over $\grave{F}_p$. Er p(X) et sådant, vil $p(X) \mid X^{p^n}-X$, thi er α en rod i p(X), vil $F_p(\alpha)$ have grad n, altså $F_p(\alpha) = GF(p^n)$, så α er rod i $X^{p^n}-X$. Er p(X) irreducibel af grad $d|n$, er $p(X) \mid X^{p^d}-X \mid X^{p^n}-X$. Er omvendt p(X) irr. og $p(X) \mid X^{p^n}-X$, kan vi betragte spaltningslegemet, L, for p(X) over $\grave{F}_p$. Da L er simpel, $L = F_p(\vartheta)$, er $[L:F_p] = \mathrm{grad}(p) = d$, så L har p^d elementer, og da $L \subseteq GF(p^n)$ må $d|n$. Det er nu klart, at $X^{p^n}-X = \prod\{p(X) \mid p \text{ er irr. og } \mathrm{grad}(p)|n\}$, hvoraf $p^n = \sum_{d|n} d\pi(d)$. Af omvendingsformlen følger nu: $n\pi(n) = \sum_{d|n} p^{n/d}\mu(d)$ eller $\pi(n) = \frac{1}{n}\sum_{d|n} p^{n/d}\mu(d) = \frac{1}{n}\sum_{d|n} p^d\mu(\frac{n}{d})$.

ENHEDSRØDDER=

Rødderne i X^n-1 over $\dot{C}$ kaldes de n-te enhedsrødder, og udgør en multiplikativ gruppe $\cong (\dot{Z}/n\dot{Z},+)$. De er alle af formen $\xi = e^{\frac{2\pi i a}{n}}$ $a \in \dot{Z}$. En n-te enhedsrod ξ for hvilken $\{\xi^a \mid a \in \dot{Z}\} = \{e^{\frac{2\pi i a}{n}} \mid a \in \dot{Z}\}$ kaldes en primitiv n-te enhedsrod. Det er klart, at $\xi = e^{\frac{2\pi i a}{n}}$, $a \in \dot{Z}$ er en primitiv n-te E.R. $\Leftrightarrow (a,n) = 1$. Polynomiet

$$F_n(X) = \prod_{(a,n)=1}(X - e^{\frac{2\pi i a}{n}})$$

kaldes det n-te cirkeldelingspolynomium; Vi har $\operatorname{grad}(F_n) = \varphi(n)$.

Sætning. $F_n(X) \in Z[X]$, $X^n-1 = \prod_{d|n} F_d(X)$ og $F_n(X) = \prod_{d|n}(X^{\frac{n}{d}}-1)^{\mu(d)}$

Bevis. $\prod_{d|n} F_d(X) = \prod_{d|n}\prod_{(a,d)=1}(X - e^{\frac{2\pi i a}{d}}) = \prod_{d|n}\prod_{(a,\frac{n}{d})=1}(X - e^{\frac{2\pi i ad}{n}}) = \prod_{d|n}\prod_{(ad,n)=d}(X - e^{\frac{2\pi i ad}{n}}) = X^n-1$, hvilket er den anden påstand. Heraf følger den tredie påstand af omvendingsformlen. Den første påstand bevises nu ved fuldstændig induktion. Sæt $H(X) = \prod_{d<n, d|n} F_d(X) \in Z[X]$, Af $X^n-1 = H(X)F_n(X)$ følger først, at $F_n(X) \in Q[X]$, og dernæst, da $H(X)$ er normeret, at $F_n(X) \in Z[X]$ (korollar til Gauss' lemma) ∎

Sætning. $F_n(X)$ er irreducibel over $Q[X]$.

Bevis. For $\xi = e$ sættes $f(X) = \operatorname{Irr}(\xi, Z)$ (som skal betegne det med $\operatorname{Irr}(\xi, Q)$ proportionale primitive polynomium $Z X$). For ethvert primtal p og n er ξ^p ligeledes en primitiv n-te enhedsrod; Vi sætter $g(X) = \operatorname{Irr}(\xi^p, Z)$. Antag at $f \neq g$, altså at f og g ikke er associerede i $Z X$.

For en E.R. ξ er $\operatorname{Irr}(\xi, \dot{Q}) \in Z[X]$, iflg. korollar til Gauss' lemma. For en primitiv n-te E.R., ξ, og et primtal $p \nmid n$ er ξ^p ligeledes en primitiv n-te ER. Vi sætter $f(X) = \operatorname{Irr}(\xi, \dot{Q})$, $g(X) = \operatorname{Irr}(\xi^p, \dot{Q})$. Antag $f \neq g$. $f(X)$ og $g(X)$ er da ikke associerede primelementer i $Z[X]$, og af $f(X) \mid X^n-1$ og $g(X) \mid X^n-1$ følger $f(X)g(X) \mid X^n-1$, altså $X^n-1 = f(X)g(X)h(X)$, hvor $h(X) \in Z[X]$. $g(X^p)$ har ξ som rod, så $g(X^p) = f(X)q(X)$, hvor $q(X) \in Z[X]$. Vi betragter nu den kannoniske afbildning, $f(X) \to f^*(X)$ af $\dot{Z}[X] \to \dot{F}_p[X]$, og får $(g^*(X))^p = g^*(X^p) = f^*(X)q^*(X)$. Nu vil en irreducibel faktor, $b^*(X)$ i $f^*(X)$ gå op i $g^*(X)$. Af $X^n-1 = f^*(X)g^*(X)h^*(X)$ fås da $X^n-1 = (b^*(X))^2 c^*(X)$, og ved afledning: $nX^{n-1} = 2b^*(X)c^*(X) + (b^*(X))^2 c^{*\prime}(X)$, altså $b^*(X) \mid X^{n-1}$; da $b^*(X)$ var irreducibel, må $b^*(X) = X$, og dermed $X^n-1 = X^2 c^*(X)$, hvilket ikke kan være tilfældet. Følgelig er ξ^p rod i $\operatorname{Irr}(\xi, \dot{Q})$, og vi kan successivt vise, at ξ^a med $(a,n) = 1$ er rod i $\operatorname{Irr}(\xi, Q)$, altså $\operatorname{Irr}(\xi, Q) = F_n$ ∎

Lemma. Hvis $d \mid n$, $d < n$, vil $F_n(X) \mid \frac{X^n-1}{X^d-1}$ (indenfor $\dot{Z}[X]$)

Bevis. Klart.

Sætning. (J.H.M.Wedderburn 1905). Ethvert endeligt skævlegeme er kommutativt.

Bevis. Lad $\mathfrak{K}$ være et endeligt skævlegeme, og sæt $\mathfrak{Z} = \{z \in \mathfrak{K} \mid \forall x \in \mathfrak{K}: xz = zx\}$. $\mathfrak{Z}$ er et kommutativt dellegeme af $\mathfrak{K}$. Hvis $\mathfrak{Z}$ har q elementer, kan vi betragte $\mathfrak{K}$ som vektorrum over $\mathfrak{Z}$, og ser, at $\mathfrak{K}$ må have q^n elementer. $\mathfrak{Z}^* = \mathfrak{Z} \setminus \{0\}$ er centrum i $\mathfrak{K}^* = \mathfrak{K} \setminus \{0\}$. (da 1 og $0 \in \mathfrak{Z}$ er $q > 1$).

Sæt, for $\alpha \in \mathfrak{K}$, $\mathfrak{N}_\alpha = \{x \in \mathfrak{K} \mid \alpha x = x\alpha\}$. Det ses, at $\mathfrak{N}_\alpha$ er et delskævlegeme i $\mathfrak{K}$. $\mathfrak{N}_\alpha \setminus \{0\}$ er normalisatoren N_α for α i $\mathfrak{K}^*$. $\mathfrak{Z} \subseteq \mathfrak{N}_\alpha \subseteq \mathfrak{K}$ så hvis $(\mathfrak{N}_\alpha : \mathfrak{Z}) = d$, er der q^d elementer i $\mathfrak{N}_\alpha$. $\operatorname{card}(\mathfrak{N}_\alpha \setminus \{0\}) \mid \operatorname{card}(\mathfrak{K}^*)$, så $q^d - 1 \mid q^n - 1$, hvoraf $d \mid n$, hvilket let eftervises(er $n = dh+r$, $0 \leq r < d$, er $q^d \equiv 1 \pmod{q^d-1}$ og $q^n - 1 \equiv 0 \pmod{q^d-1}$, så $0 \equiv q^n - 1 = q^{dh+r} - 1 = (q^d)^h q^r - 1 \equiv q^r - 1 \pmod{q^d-1}$, hvoraf $r = 0$.)

Vi betragter nu klasserne af konjugerede elementer i $(\mathfrak{K}^*, \cdot)$. Antallet af elementer i $kl(\alpha)$ er $(\mathfrak{K}^* : N_\alpha) = \frac{q^n-1}{q^d-1}$. Vi får derfor, idet vi tager elementerne i centrum, $\mathfrak{Z}^*$, først at

$$q^n - 1 = q - 1 + \sum_{\text{visse } d < n,\ d \mid n} \frac{q^n-1}{q^d-1}$$

Men $F_n(q) \mid \frac{q^n-1}{q^d-1}$ og $F_n(q) \mid q^n - 1$, hvoraf $F_n(q) \mid q-1$. For $n > 1$ er $|F_n(q)| = \prod_{(n,a)=1} |q - e^{\frac{2\pi i a}{n}}| > (q-1)^{\varphi(n)} \geq q-1$. Følgelig er $n = 1$, så at $\mathfrak{K} = \mathfrak{Z}$ er kommutativt. ∎

KAPITEL IV GALOISTEORI

Lad der være givet et legeme L. For en automorfi, σ, i L udgør fixpunkterne et dellegeme, fixpunktlegemet for σ. Er $\mathcal{S}$ en mængde af automorfier i L, da udgør de fælles fixpunkter et legeme, fixpunktlegemet for $\mathcal{S}$.

Er $K \subseteq L$ et dellegeme, og er $\mathcal{G}$ mængden af automorfier i L, hvis res. til K er ident., da er $\mathcal{G}$ en gruppe, og fixpunktlegemet, $\hat{K}$, for $\mathcal{G}$ vil indeholde K.

Eks.1. $L = \grave{R}, K = \grave{Q}$. For $a > 0$ er $\sigma(a) = \sigma(\sqrt{a})^2 > 0$. σ er altså ordenstro, og dermed identiteten, d.v.s. $\mathcal{G} = (i$ og $\hat{K} = \grave{R}$.

Eks.2. $L = \grave{C}$, $K = \grave{R}$. For $\sigma \in \mathcal{G}$ og $a \in R$, er $\sigma(a) = a$, så $\sigma(a+ib) = \sigma(a)+\sigma(ib) = a+\sigma(i)b$. Nu er $\sigma(i)^2 = \sigma(-1) = -1$, så $\sigma(i) = \pm i$. Da ident. og konj. virkelig er automorfier, er $\mathcal{G} = \{$ident.,konj.$\}$ og $\hat{K} = \grave{R}$

Eks.3. $L = \grave{C}$, $K = \grave{Q}$. Det viser sig, at $\mathcal{G}$ er uendelig, og $\hat{K} = \grave{Q}$.

Eks.4. $L = GF(p^n)$, $K = \grave{F}_p$. $\grave{F}_p$ er primlegeme i L, og derfor invariant over for enhver automorfi i L, o: $\mathcal{G}$ består af samtlige automorfier i $GF(p^n)$. Nu er $GF(p^n)$ = $= F_p(\zeta)$, hvor $Irr(\zeta, F_p) = p(X) \in F_p[X]$, grad(p) = n, og da $p(X) \mid X^{p^n}-X$ har p(X) n forskellige rødder i L. Er nu σ en automorfi i $GF(p^n)$, og $a = a_0+\ldots+a_{n-1}\zeta^{n-1}$, da er $\sigma(a) = a_0+a_1\sigma(\zeta)+\ldots+a_{n-1}\sigma(\zeta)^{n-1}$, d.v.s. σ er helt bestemt ved sine værdi på ζ. Endvidere er det klart, at $\sigma(\zeta)$ er rod i p(X), så der er højst n forskellige automorfier i $GF(p^n)$. På den anden side defineres ved $a \to a^p$ en automorfi, σ, i $GF(p^n)$, og automorfierne $\sigma_0 = e$, $\sigma_1 = \sigma, \ldots, \sigma_{n-1} = \sigma^{(n-1)}$ er alle forskellige, thi $\sigma_i = \sigma_j$ $\Rightarrow a^{p^j}-a^{p^i} = 0$ for alle $a \in GF(p^n)$, altså alle a er rod i $X^{p^j}-X^{p^i}$, hvoraf J = i. Fixelementerne for σ er rødder i X^p-X, så der er højst p; på den anden side er alle elementer i $\grave{F}_p$ fixpunkter, så $K = \grave{F}_p$. $\mathcal{G} = (\sigma)$.

5) $L = \grave{Q}(\sqrt[3]{2})$, $K = \grave{Q}$. $L = \{a_0+a_1\sqrt[3]{2}+a_2(\sqrt[3]{2})^2 \mid a_0, a_1, a_2 \in Q$ σ er bestemt ved $\sigma(\sqrt[3]{2})$, og da $(\sigma(\sqrt[3]{2}))^3 = \sigma(2) = 2$, og $\sigma(\sqrt[3]{2}) \in L = Q(\sqrt[3]{2})$, er $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$, o: $\sigma = id_L$ altså $\hat{K} = L$

Sætning. Lad L være spaltningslegemet for et separabelt polynomium $f(X) \in K[X]$. Hvis $\mathcal{G}$ betegner gruppen af automorfier, σ, i L med $\sigma_{|K} = id_K$, da er K fixpunktlegemet for $\mathcal{G}$.

Bevis. Lad $\alpha, \beta, \ldots$ være rødder i f(X), successivt adjungeret så at $K = K_0 \subset K(\alpha) = K_1 \subset K(\alpha,\beta) = K_2 \subset \ldots \subset K_\nu = L$. Vi skal vise, at der til $c \in L \setminus K$ findes en automorfi $\sigma \in \mathcal{G}$, med $\sigma(c) \neq c$. Lad $c \in K_{i+1} \setminus K_i = K_i(\mu) \setminus K_i$. Er $\operatorname{grad}(\operatorname{Irr}(\mu,K_i)) = m$, da er $K_{i+1} = \{a_0+a_1\mu+\ldots+a_{m-1}\mu^{m-1} \mid a_0,\ldots,a_{m-1} \in K_i\}$. Da $\operatorname{Irr}(\mu,K_i) \mid \operatorname{Irr}(\mu,K)$, og $\operatorname{Irr}(\mu,K)$ er separabel, er også $\operatorname{Irr}(\mu,K_i)$ separabel. Antag, at $\operatorname{Irr}(\mu,K_i)$ har rødderne $\mu = \mu_1,\ldots,\mu_m$, som altså er forskellige. Nu er $c = b_0+b_1\mu+\ldots+b_{m-1}\mu^{m-1}$, $b_0,\ldots,b_{m-1} \in K_i$; elementerne $c_j = b_0+b_1\mu_j+\ldots+b_{m-1}\mu_j^{m-1}$ er da ikke alle $= c$, thi da havde polynomiet $(b_0-c)+b_1X+\ldots+b_{m-1}X^{m-1} \in K_{i+1}[X]$ de m forskellige rødder $\mu_1,\ldots,\mu_m$ og det måtte følgelig være 0-polynomiet, hvoraf $c = b_0 \in K_i$, i modstrid med at $c \in K_{i+1} \setminus K_i$. Lad fx. $c_2 \neq c = c_1$. Vi betragter nu $K_i(\mu)$ og $K_i(\mu_2)$. Da $\operatorname{Irr}(\mu,K_i) = \operatorname{Irr}(\mu_2,K_i)$, findes en isomorfi $\Phi : K_i(\mu)$ på $K_i(\mu_2)$, så at $\Phi_{|K_i} = id_{K_i}$ og $\Phi(\mu) = \mu_2$. Da f(X) er spaltningslegemet for f(X) over K, og dermed over $K_i(\mu)$ og $K_i(\mu_2)$, kan Φ fortsættes til en isomorfi σ : L på L, så $\sigma_{|K} = \Phi_{|K} = (id_{K_i})_{|K} = id_K$ og $\sigma(c) = \Phi(c) = c_2 \neq c$. ∎

En udvidelse $L \supseteq K$ kaldes ~~maximal~~ Galoisk, hvis K er fixpunktlegeme for en gruppe af automorfier i L (og dermed for gruppen af automorfier i L med res. til K = ident. for K). Vi har vist:

Sætning. Spaltningslegemet, L, for et separabelt polynomium over K er en endelig Galoisk udvidelse.

Eks. Lad L være spaltningslegemet for X^p-t over $K = \mathbb{F}_p(t)$. $f(X) = X^p-t$ er ikke separabel, thi er $\beta \in L$ en rod i f(X), så er β p-dobbelt rod (III,6), og altså $L = K(\beta)$. Er $\sigma \in \operatorname{Gr}(L/K)$, da er $\sigma(\beta)^p = \sigma(\beta^p) = \sigma(t) = t$, så $\sigma(\beta)$ er rod i f(X), altså $\sigma(\beta) = \beta$, men så er $\sigma = id_L$, og fixpunktlegemet for Gr(L/K) er L. L/K er således ikke Galoisk.

Eks. Lad Λ være et legeme, og sæt $L = \Lambda(X_1,\ldots,X_n)$. Betegner $s_1,\ldots,s_n$ de elementarsymmetriske polynomier, og sættes $K = \Lambda(s_1,\ldots,s_n)$, er $L \supseteq K$. Betragt polynomiet $f(X) = (Z-X_1)\ldots(Z-X_n) = Z^n-s_1Z^{n-1}+\ldots+(-1)^n s_n \in K[Z]$. Det ses, at L er spaltningslegemet for f(Z) over K, og da f(Z) er separabel, kan sætningen anvendes. Lad σ væ-

re en automorfi i Gr(L/K), da er σ bestemt ved $\sigma(X_1)$, ...,$\sigma(X_m)$. Da X_i er rod i f(Z), er også $\sigma(X_i)$ rod i f(Z), altså = et X_j. σ giver således anordning til en permutation $\sigma \in S_n$. Er omvendt $\sigma \in S_n$, vi$ $\sigma(X_i) = X_{\sigma(i)}$ bestemme en automorfi σ under hvilken K er invariant, altså $\sigma \in$ Gr(L/K). En symmetrisk brudden rational fkt. i $\Lambda(X_1,\ldots,X_m)$ vil være invariant over for alle disse automorfier, altså element i $\Lambda(s_1,\ldots,s_m)$. Vi har således vist, at enhver symmetrisk brudden rational fkt. kan skrives som brudden rational fkt. i $s_1,\ldots,s_m$.

Eks. $L = \Lambda(t) \supseteq K = \Lambda(t+\frac{1}{t})$. L er spaltningslegeme for $f(X) = (X-t)(X-\frac{1}{t}) = X^2-(t+\frac{1}{t}) + 1 \in K[X]$, som er separabel. Et element $\sigma \in$ Gr(L/K) er bestemt ved $\sigma(t)$, osm er rod i f(X), altså $\sigma(t) = t$ eller $= \frac{1}{t}$. Det ses nu, at Gr(L/K) består af ident. og $t \to \frac{1}{t}$. Iflg. sætningen vil altså enhver brudden rational funktion i $\Lambda(t)$*) kunne skrives som brudden rational funktion i $t+\frac{1}{t}$.

Lemma. <u>Endelig mange automorfier i et legeme L, $\sigma_1,\ldots,\sigma_n$ er uafhængige</u> (d: hvis $a_1,\ldots,a_n \in L$ og $a_1\sigma_1(c) + \ldots + a_n\sigma_n(c) = 0$ for alle $c \in L$, da er $a_1 = \ldots = a_n = 0$)
Induktion efter n. n = 1: Der findes $c \in L$, så at $\sigma_1(c) \neq 0$, men så vil $a_1\sigma_1(c) = 0$ medføre, at $a_1 = 0$. Antag sætningen for n-1, og antag, at $a_1\sigma_1(c)+\ldots+a_n\sigma_n(c) = 0$ for alle c. For alle b er
$a_1\sigma_1(b)\sigma_1(c)+\ldots+a_n\sigma_n(b)\sigma_n(c) = a_1\sigma_1(bc)+\ldots+a_n\sigma_n(bc) = 0$ og
$a_1\sigma_n(b)\sigma_1(c)+\ldots+a_n\sigma_n(b)\sigma_n(c) = 0$, hvoraf
$a_1[\sigma_1(b)-\sigma_n(b)]\sigma_1(c) + \ldots + a_{n-1}[\sigma_{n-1}(b)-\sigma_n(b)]\sigma_{n-1}(c) = 0.$
Vælges $b \in L$ så at $\sigma_1(b) \neq \sigma_n(b)$, vil (iflg. induktionsantagelsen) $a_1 = 0$, men så er (iflg. induktionsantagelsen) også $a_2 = \ldots = a_n = 0$ ∎

Sætning (Artin) <u>Lad L være et legeme, og G en gruppe af automorfier i L, og K fixpunktlegemet for G, da er ord(G) = [L:K].</u>
Bevis. 1) <u>[L:K] ≥ ord(G).</u> Beviset er klart, hvis $[L:K] = \infty$, og hvis $[L:K] = n < \infty$, viser vi, at G ikke kan indeholde n+1 forskellige automorfier. Indirekter: Er $\sigma_1,\ldots,\sigma_{n+1} \in G$ forskellige automorfier, og er $\omega_1,\ldots,\omega_n$ en K-basis for L, da er $\sum_{j=1}^{n+1} a_j\sigma_j(\omega_i) = 0$, i = 1,...,n et homogent linært ligningssystm. med n ligninger og de n+1 ubekendte $a_1,\ldots,a_{n+1}$ Det har følgelig en ikke triviel løsning $(a_1,\ldots,a_{n+1})$. For $c \in L$ har vi $c = b_1\omega_1+\ldots+b_n\omega_n$, $b_i \in K$ men så er $a_1\sigma_1(c)+\ldots+a_{n+1}\sigma_{n+1}(c) = \sum_j\sum_i b_i a_j\sigma_j(\omega_i) = \sum_i\sum_j b_i a_j\sigma_j(\omega_i) = 0.$

*), der er invariant over for $t \to \frac{1}{t}$,

2) $[L:K] \leq \mathrm{ord}(G)$. Dette er klart, hvis $\mathrm{ord}(G) = \infty$, og er $\mathrm{ord}(G) = r < \infty$, $G = \{\sigma_1,\ldots,\sigma_r\}$, viser vi, at vilkårlig r+1 elementer $\omega_1,\ldots,\omega_{r+1} \in L$ er afhængige over K. Det lineære ligningssystem $\sum_{i=1}^{r+1} a_i \sigma_j^{-1}(\omega_i) = 0$, $j = 1,\ldots,r$ ses (som før) at have en ikke triviel løsning $(a_1,\ldots,a_{r+1})$. Nu er $0 = \sum_{j=1}^{r} \sigma_j \sum_{i=1}^{r+1} a_i \sigma_j^{-1}(\omega_i) = \sum_i \sum_j \sigma_j(a_i)\omega_i$, altså

$$\not\in \quad S(a_1)\omega_1+\ldots+S(a_{r+1})\omega_{r+1} = 0,$$

hvor $S(a) = \sum_{\sigma \in G} \sigma(a)$. Da G er en gruppe, er $\sigma(S(a)) = S(a)$, og dermed $S(a) \in K$. Da $(a_1,\ldots,a_{r+1}) \neq (0,\ldots,0)$, kan vi fx. antage, at $a_1 \neq 0$, men så kan vi også antage, at $S(a_1) \neq 0$ (og $\not\in$ er da en egentlig K-relation mellem $\omega_1,\ldots,\omega_{r+1}$), thi da $\sigma_1,\ldots,\sigma_r$ er forskellige, findes c så at $\sigma_1(c)+\ldots+\sigma_r(c) \neq 0$, altså $S(c) \neq 0$, men så er $c \neq 0$, og det ønskede ville være opfyldt for $c = a_1 \cdot \frac{c}{a_1}$, $a_2\frac{c}{a_1}$, $\ldots, a_{r+1}\frac{c}{a_1}$. ∎

Korollar. Er L et legeme, og G en endelig automorfigruppe i L, og K fixpunktlegemet for G, da er $G = \mathrm{Gr}(L/K)$.

Bevis. Vi har $\mathrm{Gr}(L/K) \supseteq G$, og $\mathrm{Gr}(L/K)$'s fixpunktlegeme er K. Af $\mathrm{ord}(\mathrm{Gr}(L/K)) = [L:K] = \mathrm{ord}(G)$ følger nu, at $\mathrm{Gr}(L/K) = G$. ∎

Korollar. I legemet L har forskellige endelige automorfigrupper i L forskellige fixpunktlegemer.

er klart!

Eks. $L = \grave{C}(t)$. Ved $\{t \to t+a \mid a \in \grave{Z}\}$ bestemmes en (uendelig) automorfigruppe, G, for hvilken fixpunktlegemet er $K = \grave{C}$. Vi har nemlig $\grave{C} \subsetneq K$, og hvis $f(t)/g(t) \in K \setminus \grave{C}$ er uforkortelig kan vi (evt. ved overgang til den inverse) antage, at $\mathrm{grad}(f) \geq 1$. Nu er $f(t)/g(t) = f(t+1)/g(t+1) = \ldots$; Hvis $f(\alpha) = 0$ er $g(\alpha) \neq 0$, så $f(\alpha+1) = 0$, $f(\alpha+2) = 0,\ldots$ i modstrid med at $\mathrm{grad}(f) \geq 1$.

Havde vi i stedet betragtet automorfigruppen bestemt ved $\{t \to t+2a \mid a \in \grave{Z}\}$ havde vi fundet samme fixpunktlegeme.

Sætning. Lad L/K være en endelig Galoisk udvidelse, og sæt $G = \mathrm{Gr}(L/K)$, da vil for ethvert $\alpha \in L$ rødderne i $\mathrm{Irr}(\alpha,K)$ alle tilhøre L, og være indbyrdes forskellige, nemlig lig de forskellige billeder af α ved automorfierne i G.

Specielt er L/K separabel.

Bevis. Lad $[L:K] = \mathrm{ord}(G) = n$, så $G = \{\sigma_1,\ldots,\sigma_n\}$, og lad $\alpha \in L$. Er $\sigma_1(\alpha),\ldots,\sigma_r(\alpha)$ de forskellige billeder af α ved automorfierne i G, og er $\sigma \in G$, da har vi $\{\sigma\sigma_1(\alpha),\ldots,\sigma\sigma_r(\alpha)\} = \{\sigma_1(\alpha),\ldots,\sigma_r(\alpha)\}$.

Sættes $f(X) = (X-\sigma_1(\alpha))\ldots(X-\sigma_n(\alpha)) \in L[X]$, hvor vi derfor $\sigma(f(X)) = f(X)$, og dermed $f(X) \in K[X]$. Da $f(\alpha) = 0$, er $\mathrm{Irr}(\alpha,K) \mid f(X)$. Det er på den anden side klart, at $\sigma(\alpha)$ er rod i $\mathrm{Irr}(\alpha,K)$ for alle $\sigma \in G$, så $f(X) \mid \mathrm{Irr}(\alpha,K)$, og da $f(X)$ er normeret må $f(X) = \mathrm{Irr}(\alpha,K)$. ∎

Korollar. <u>En endelig Galoisk udvidelse er simpel.</u>
thi en endelig separabel udvidelse er simpel. ∎

En algebraisk udvidelse, L/K, kaldes <u>normal</u>, hvis ethvert <u>irreducibelt</u> polynomium $f(X) \in K[X]$, med blot en rod i L har samtlige rødder i L. Vi har set, at en endelig Galois'sk udvidelse er normal.

Sætning. <u>En endelig udvidelse, L/K, er normal, hvis og kun hvis L er spaltningslegeme for et polynomium i K[X].</u>
Bevis. "kun hvis": Er $L = K(\alpha_1,\ldots,\alpha_m)/K$ en normal udvidelse, da er L øjensynlig spaltningslegeme over K for polynomiet $\mathrm{Irr}(\alpha_1,K)\ldots \mathrm{Irr}(\alpha_m,K) \in K[X]$.
"Hvis": Lad L være spaltningslegemet for polynomiet $f(X) \in K[X]$, og lad $\alpha \in L$, og sæt $g(X) = \mathrm{Irr}(\alpha,K) \in K[X]$, da skal vi vise, at $g(X)$ har samtlige rødder i L. Lad M være et spaltningslegeme for $g(X)$ over L. Er $\beta \in M$ en rod i $g(X)$, da findes en isomorfi $\varphi : K(\alpha)$ på $K(\beta)$, med $\varphi(\alpha) = \beta$. Nu er $\varphi f(X) = f(X)$, og da L er spaltningslegeme for $f(X)$ over $K(\alpha)$, og $L(\beta)$ er spaltningslegemet for $f(X)$ over $K(\beta)$, kan φ udvides til en isomorfi, $\Phi : L$ på $L(\beta)$. Her er både L og $L(\beta) \subseteq M$. Da Φ er en K-isomorfi, og $f(X) \in K[X]$, vil Φ afbilde mængden af rødder i $f(X)$ <u>på</u> sig selv, og da L frembringes af disse rødder, følger det, at Φ er en automorfi i L. Specielt er altså $\beta \in L$. ∎

Sætning. <u>En endelig udvidelse L/K er Galois'sk, hvis og kun hvis den er separabel og normal.</u>
Bevis. "kun hvis" er vist. "hvis" L/K er separabel og normal, er L spaltningslegeme for et polynomium i K[X], som nødvendigvis er separabelt. ∎

Korollar 1. <u>En endelig udvidelse, L/K, er Galois'sk, hvis og kun hvis L er spaltningslegeme for et separabelt polynomium i K[X].</u>
"Hvis" er vist. "kun hvis": iflg. ovenstående.

Korollar 2. <u>Hvis $K \subseteq L \subseteq M$, og M/K er en endelig normal (Galois'sk udvidelse, da er M/L endelig normal (Galois'sk).</u>
thi M er spaltningslegeme for et (separabelt) polynomium $f(X) \in K[X] \subseteq L[X]$. ∎

Korollar 3. Hvis L/K er en endelig (separabel) udvidelse, da finen og (på isomorfi nær) kun én mindste udvidelse M/L så at M/K er endelig normal (Galois'sk).
Bevis. Lad $L = K(\alpha_1,\ldots,\alpha_n)$, sæt $f(X) = \mathrm{Irr}(\alpha_1,K)\ldots\mathrm{Irr}(\alpha_n,K)$, og lad M være spaltningslegemet for f(X) over L. Det ses, at $M \supseteq L$ også er spaltningslegeme for f(X) over K, og M/K er følgelig endelig normal (Galois'sk).
Lad M'/K være endelig normal, med $M' \supseteq L$, da er $\alpha_1,\ldots,\alpha_n \in M'$, så M' endeholder et spaltningslegeme for f(X) over K, altså et dellegeme isomorft med M. (og det er klart, at intet ægte dellegeme af M kan have denne egenskab) ∎

Sætning. Lad $L \supseteq K$, da udgør mængden af elementer i L, separable over K, et dellegeme L_1 af L (kaldet det separable hylster af K i L)
Bevis. Det er nok at vise, at for $\alpha,\beta \in L_1$ er $K(\alpha,\beta)/K$ en separabel udvidelse. Sættes $f(X) = \mathrm{Irr}(\alpha,K)\ \mathrm{Irr}(\beta,K)$, og er M spaltningslegemet forf(X) over K, da er M/K specielt separabel, og da $M \supseteq K(\alpha,\beta)$ gælder det samme for $K(\alpha,\beta)/K$ ∎

For en gruppe, G, af automorfier i legemet L betegnes med L^G fixpunktlegemet for automorfierne i G.

Vi viser nu Galoisteoriens
Hovedsætning. Lad M/K være en endelig Galois'sk udvidelse, med Galoisgruppen $G = \mathrm{Gr}(M/K)$, da definerer $L \longrightarrow H = \mathrm{Gr}(M/L)$ en entydig antitro forbindelse mellem legemerne, L, mellem K og M og undergrupperne, H, I G, idet
1) $M^{\mathrm{Gr}(M/L)} = L$, $\mathrm{Gr}(M/M^H) = H$ og $L \subseteq L' \Leftrightarrow \mathrm{Gr}(M/L) \supseteq \mathrm{Gr}(M/L')$.
2) M/L er normal; specielt er $[M:L] = \mathrm{ord}(\mathrm{Gr}(M/L))$ og dermed $[L:K] = (G:\mathrm{Gr}(M/L))$.
3) L/K er Galois'sk $\Leftrightarrow$ Gr(M/L) er normaldeler i G, og i bekræftende fald er $\mathrm{Gr}(L/K) \cong G/\mathrm{Gr}(M/L)$.
Bevis. Vi har $\mathrm{Gr}(M/M^H) = H$ iflg. Korollar p.IV,4. Endvidere er M/L Galoisk iflg. Korollar 2, med det betyder netop, at $M^{\mathrm{Gr}(M/L)} = L$. Vi har $L \subseteq L' \Rightarrow \mathrm{Gr}(M/L) \supseteq \mathrm{Gr}(M/L')$ og $H \supseteq H' \Rightarrow M^H \subseteq M^{H'}$, hvormed 1) er vist. 2) er nu en umiddelbar følge. Beviset for 3) støtter sig til
Lemma. L/K er Galoisk $\Leftrightarrow \forall \sigma \in G: \sigma(L) = L$.
Bevis for lemma. "$\Rightarrow$" Lad $\sigma \in G$. For $\alpha \in L$ er $\sigma(\alpha)$ rod i $\mathrm{Irr}(\alpha,K)$, og dermed $\sigma(\alpha) \in L$, altså $\sigma(L) \subseteq L$. Da også $\sigma^{-1}(L) \subseteq L$, er $\sigma(L) = L$. "$\Leftarrow$": Lad $\alpha \in L$, og sæt $f(X) = \mathrm{Irr}(\alpha,K)$, da skal vi vise, at

f(X)'s rødder alle ligger i L, men da M/K er ~~xxx~~Galoisk, er disse rødder $\{\sigma(\alpha) \mid \sigma \in G\} \subseteq L$. ∎
Det ses endvidere let, at $Gr(M/\sigma(L)) = \sigma Gr(M/L)\sigma^{-1}$, thi for $\tau \in Gr(M/L)$ og $\alpha \in L$ er $\sigma\tau\sigma^{-1}(\sigma(\alpha)) = \sigma\tau(\alpha) = \sigma(\alpha)$, så $\sigma Gr(M/L)\sigma^{-1} \subseteq Gr(M/\sigma(L))$, og for $\rho \in Gr(M/\sigma(L))$ er $\rho\sigma(\alpha) = \sigma(\alpha)$ ⟹ $\sigma^{-1}\rho\sigma(\alpha) = \alpha$, så $\sigma^{-1}\rho\sigma \in Gr(M/L)$, og dermed $\rho \in \sigma Gr(M/L)\sigma^{-1}$.
Bevis for 3): L/K er Galois'sk $\iff \forall \sigma \in G: \sigma(L) = L \iff \forall \sigma \in G: Gr(M/L) = Gr(M/\sigma(L)) \iff \forall \sigma \in G: \sigma Gr(M/L)\sigma^{-1} = Gr(M/L) \iff Gr(M/L) \lhd G$.
Hvis L/K er Galois'sk, ~~x~~ og $\sigma \in G$, da $\sigma_{|L}$ en automorfi i L, altså $\sigma_{|L} \in Gr(L/K)$. Ved $\sigma \to \sigma_{|L}$ defineres altså en afbildning Res_L : $G \to G_{|L} \subseteq Gr(L/K)$, som øjensynlig er en homomorfi, og da $Ker(Res_L) = \{\sigma \in G \mid Res_L(\sigma) = id_L\} = Gr(M/L)$, er $G_{|L} \cong G/Gr(M/L)$. Da $G_{|L}$ og Gr(L/K) således har samme orden iflg 2) er $G_{|L} = Gr(L/K)$.
Hermed er beviset fuldført. ∎

Det er nu let at vise
Tilføjelse. <u>Hvis $K \subseteq L, L' \subseteq M$, da er $Gr(M/L \cap L') = Gr(M/L)Gr(M/L')$ (kompositet), og $Gr(M/LL') = Gr(M/L) \cap Gr(M/L')$.</u>

Korollar. <u>Hvis L/K og L'/K er Galois'ske, da er også $L \cap L'/K$ og LL'/K Galois'ske.</u>
thi analoge sætninger gælder for normaldelere.

EKSEMPLER

$\dot{Q}(\sqrt{2},\sqrt{3})/\dot{Q}$ er Galoisk, da $\dot{Q}(\sqrt{2},\sqrt{3})$ er spaltningslegeme for $f(X) = (X^2-2)(X^2-3)$ over $\dot{Q}$. Automorfierne i $G = Gr(\dot{Q}(\sqrt{2},\sqrt{3})/\dot{Q})$, er belt bestemt ved $\sigma(\sqrt{2})$ og $\sigma(\sqrt{3})$, og da disse er rødder i f(X), er der højst 4, nemlig $e = \begin{pmatrix} \sqrt{2} & \sqrt{3} \\ \sqrt{2} & \sqrt{3} \end{pmatrix}$, $\sigma = \begin{pmatrix} \sqrt{2} & \sqrt{3} \\ -\sqrt{2} & \sqrt{3} \end{pmatrix}$, $\tau = \begin{pmatrix} \sqrt{2} & \sqrt{3} \\ \sqrt{2} & -\sqrt{3} \end{pmatrix}$ og $\sigma\tau = \begin{pmatrix} \sqrt{2} & \sqrt{3} \\ -\sqrt{2} & -\sqrt{3} \end{pmatrix}$, og da $[\dot{Q}(\sqrt{2},\sqrt{3}):\dot{Q}] = [\dot{Q}(\sqrt{2},\sqrt{3}):\dot{Q}(\sqrt{2})] \cdot [\dot{Q}(\sqrt{2}):\dot{Q}] = 2 \cdot 2 = 4$, er altså $G = \{e, \sigma, \tau, \sigma\tau\}$. Vi finder $\sigma^2 = \tau^2 = (\sigma\tau)^2 = e$, så $G \cong V$ (Kleins Vier-gruppe). ~~X~~ sættes $M = \dot{Q}(\sqrt{2},\sqrt{3})$, da finder vi $M^{\{e,\sigma\}} = \dot{Q}(\sqrt{2})$, $M^{\{e,\tau\}} = \dot{Q}(3)$ og $M^{\{e,\sigma\tau\}} = \dot{Q}(\sqrt{6})$.

Er omvendt $M/\dot{Q}$ en normal udvidelse, for hvilken $Gr(M/\dot{Q}) = V$, da er $M^{\{e,\sigma\}} = L_1 \supseteq \dot{Q}$, hvor $[L_1:\dot{Q}] = 2$, så $L_1 = \dot{Q}(\sqrt{a})$ og altså også $M^{\{e,\tau\}} = \dot{Q}(\sqrt{b})$, og dermed $M = M^{\{e,\sigma\} \cap \{e,\tau\}} = M^{\{e,\sigma\}} M^{\{e,\tau\}} = \dot{Q}(\sqrt{a})\dot{Q}(\sqrt{b}) = \dot{Q}(\sqrt{a}, \sqrt{b})$.

Sætning. <u>Lad M være spaltningslegeme for et separabelt irreducibelt polynomium p(X) over K, med grad(p) = n (så $[M:K] \geq n$), da er Gr(M/K) isomorf med en transitiv undergruppe i gruppen, S_n, af permutationer af rødderne i p(X); specielt er $[M:K] \leq n!$.</u>
Bevis. Hvis $p(X) = (X-\alpha_1)\ldots(X-\alpha_m)$, er $M = K(\alpha_1, \ldots, \alpha_m)$. For

$\sigma \in Gr(M/K)$ er $\sigma(\alpha_i)$ en rod i $p(X)$ (ϑ: = et α_j), så $\sigma(\{\alpha_1,\ldots,\alpha_n\}) = \{\alpha_{\sigma(1)},\ldots,\alpha_{\sigma(n)}\}$. Det ses, at afbildningen $Gr(M/K) \longrightarrow S_n$ er injektiv og homomorf, og billedet bliver en transitiv undergruppe. ∎

Eksamensopgave: Antag $f(X) \in \mathbb{Q}[X]$ er irreducibel, og at grad(f) = n, samt at der for antallet, r, af reelle rødder gælder $0 < r < n$. Lad $K \subsetneq \mathbb{C}$ være spaltningslegemet for f(X) over $\mathbb{Q}$. 1) Vis, at $L = K \cap \mathbb{R}$ ikke er normal over $\mathbb{Q}$. Eftervis herved, at $[K:\mathbb{Q}] \geq 2n$. 2) $f(X) = X^4-2X^3-2X+1$ er irreducibel over $\mathbb{Q}$. 3) Angiv antallet af reelle rødder i f(X) 4) Bestem, idet K er f(X)'s spaltningslegeme orden og gruppetype af $Gr(K/\mathbb{Q})$ (Benyt, at $f(\alpha) = 0 \Rightarrow f(\frac{1}{\alpha}) = 0$.)
Løsning. 1) Da f(X) har en rod i L, men ikke samtlige rødder i L, er $L/\mathbb{Q}$ ikke normal. Er α en reel rod i f(X), da er $[K:\mathbb{Q}] = [K:\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha):\mathbb{Q}] \geq 2\cdot n$. 2) $f(X) = X^4-2X^3-2Z+1$ er irreducibel over $\mathbb{Q}$, thi $f(X+1) = X^4+2X^3-4X-2$ er irreducibel iflg. Schönemann-Eisenstein. 3) $f(X) = X^2(X^2-2X-2\frac{1}{X}+\frac{1}{X^2}) = X^2((X+\frac{1}{X})^2-2(X+\frac{1}{X})-2)$, hvoraf det ses, at f(X) har 2 reelle og to kaoplekse (konjugerede) rødder. 4) Er α en reel rod og β en komplex rod, er f(X)'s 4 forskellige rødder $\alpha,\alpha^{-1},\beta,\beta^{-1}$, så $K = \mathbb{Q}(\alpha,\beta)$, og dermed $[K:\mathbb{Q}] = [\mathbb{Q}(\alpha,\beta):\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha):\mathbb{Q}]$ Nu er $f(X) = (X-\alpha)(X-\alpha^{-1})f_1(X)$ i $\mathbb{Q}(\alpha)$, så $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}(\alpha)] \leq 2$, og da $[\mathbb{Q}(\alpha):\mathbb{Q}] = 4$ må $[K:\mathbb{Q}] \leq 8$. Iflg 1) er altså $[K:\mathbb{Q}] = 8$. og også ord $Gr(K/\mathbb{Q}) = 8$, og da $Gr(K/\mathbb{Q})$ iflg. 1) har en ikke normal undergruppe, er altså $Gr(K/Q) \cong D_4$.

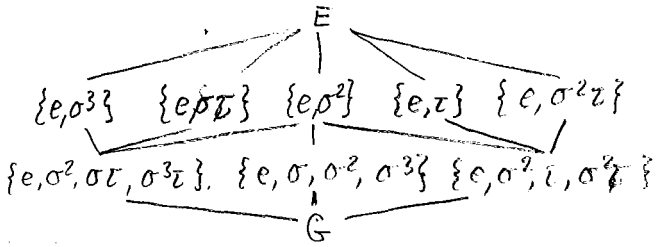
Eks. $f(X) = X^3-2$ er irreducibel over $\mathbb{Q}$ iflg. Schönemann-Eisenstein Spaltningslegemet K bliver $K = \mathbb{Q}(\alpha_0,\alpha_1,\alpha_2) = \mathbb{Q}(\sqrt[3]{2},\sqrt[3]{2}\,\varepsilon,\sqrt[3]{2}\,\varepsilon^2)$, hvor ε er en primitiv 3-die enhedsrod, altså $K = \mathbb{Q}(\sqrt[3]{2},\varepsilon)$, og $[K:\mathbb{Q}] = 6$ ses nu let, så $Gr(K/\mathbb{Q}) \cong S_3$ iflg. sætning. $Gr(K/\mathbb{Q})$ er bestemt ved e, $\sigma = (\alpha_0,\alpha_1,\alpha_2)$, $\sigma^2 = (\alpha_0,\alpha_2,\alpha_1)$, $\tau = (\alpha_1,\alpha_2)$, $\tau\sigma = (\alpha_2,\alpha_0)$ og $\tau\sigma^2 = (\alpha_0,\alpha_1)$. Vi har $\sigma^3 = e$, τ er komplex konjugering, $\tau^2 = e$ $\tau\sigma\tau = \sigma^{-1}$. Der er 4 undergrupper, 3 af orden 2 og 1 af orden 3: $\{e,\tau\}$, $\{e,\sigma\tau\sigma\}$, $\{e,\tau\sigma^2\}$, og $\{e,\sigma,\sigma^2\}$. svarende til mellemlegemerne: $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[3]{2}\varepsilon)$, $\mathbb{Q}(\sqrt[3]{2}\varepsilon^2)$, og $\mathbb{Q}(\varepsilon)$.

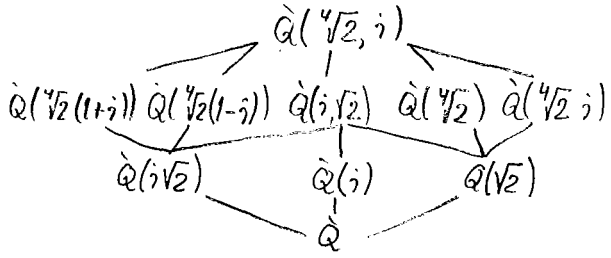
Eks. Er $f(X) = X^3+aX^2+bX+c \in \mathbb{Q}[X]$ irreducibelt med spaltningslegeme L og Galoisgruppe, G, og er α en rod, da er enten $L = \mathbb{Q}(\alpha)$ og dermed $G \cong A_3$, eller $(X-\alpha)^{-1}f(X) \in \mathbb{Q}(\alpha)[X]$ er irreducibel af grad 2, med en rod β, og da er $L = \mathbb{Q}(\alpha,\beta)$ og $L/\mathbb{Q} = 6$, så $G \cong S_3$

Eks. X^4-2 er irreducibel over $\mathbb{Q}[X]$ iflg Sch.-Eis., med spaltningslegemet $K = \mathbb{Q}(\sqrt[4]{2},\sqrt[4]{2}i,-\sqrt[4]{2},-i\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2},i)$ af grad 8 over $\mathbb{Q}$. Galoisgruppen er bestemt ved $\sigma(\sqrt[4]{2})$ og $\sigma(i)$, så
$e = \begin{pmatrix}\sqrt[4]{2} & i\\ \sqrt[4]{2} & i\end{pmatrix}$, $\sigma = \begin{pmatrix}\sqrt[4]{2} & i\\ i\sqrt[4]{2} & i\end{pmatrix}$, $\sigma^2 = \begin{pmatrix}\sqrt[4]{2} & i\\ -\sqrt[4]{2} & i\end{pmatrix}$, $\sigma^3 = \begin{pmatrix}\sqrt[4]{2} & i\\ -i\sqrt[4]{2} & i\end{pmatrix}$,

$\tau = \begin{pmatrix} \sqrt[4]{2} & i \\ \sqrt[4]{2} & -i \end{pmatrix}$, $\sigma\tau = \begin{pmatrix} \sqrt[4]{2} & i \\ i\sqrt[4]{2} & -i \end{pmatrix}$, $\sigma^2\tau = \begin{pmatrix} \sqrt[4]{2} & i \\ -\sqrt[4]{2} & -i \end{pmatrix}$, $\sigma^3\tau = \begin{pmatrix} \sqrt[4]{2} & i \\ -i\sqrt[4]{2} & -i \end{pmatrix}$.

Da $\dot{Q}(\sqrt[4]{2})$ indeholder en, men ikke alle rødder, er $\dot{Q}(\sqrt[4]{2})$ ikke normal, så $Gr(K/\dot{Q})$ er en gruppe af orden 8 med ikke normale undergrupper, altså $Gr(K/\dot{Q}) \cong D_4$. Man kan vise, at undergrupperni i G svarer til følgende diagram. (Her er foruden de trivielle også $\{e,\sigma^2\}$ normaldeler, og derfor $\dot{Q}(i,\sqrt{2})$ normal over $\dot{Q}$.





Eks. Er ζ en primitiv n-te enhedsrod, da er $\dot{Q}(\zeta)$ øjensynlig spaltningslegemet for polynomiet $F_n(X) = \prod_{(a,n)=1}(X-\zeta^a)$ over $\dot{Q}$. $\dot{Q}(\zeta)$ kaldes det n-te cirkeldelingslegeme; $[\dot{Q}(\zeta):\dot{Q}] = \text{grad}(F_n) = \varphi(n)$ Ved $\zeta \to \zeta^a$, $(a,n) = 1$ defineres således de $\varphi(n)$ automorfier i $Gr(\dot{Q}(\zeta)/\dot{Q})$. Nu er $Gr(\dot{Q}(\zeta)/\dot{Q})$ øjensynlig isomorf med gruppen, G(n), af primiske restklasser mod.n, altså specielt abelsk. Omvendt gælder følgende dybere liggende

Sætning (Weber - Kronecker). <u>En endelig abelsk udvidelse K/Q er altid indeholdt i et cirkeldelingslegeme.</u>

Vi beviser et specialtilfælde

Sætning. <u>En kvadratisk udvidelse $Q(\sqrt{d})$ er indeholdt i et cirkeldelingslegeme</u>.

Bevis. For d = 2 er $\sqrt{2} \in \dot{Q}(e^{\frac{2\pi i}{8}})$. Vi viser nu

Lemma. <u>For et primtal $p \neq 2$ er $\sqrt{(-1)^{\frac{p-1}{2}}\, p} \in \dot{Q}(e^{\frac{2\pi i}{p}})$.</u> Dette legemes Galoisgruppe er $G(p) = \dot{F}_p^*$, som er cyklisk af orden p-1. Da $\frac{p-1}{2} \mid p-1$ findes netop én undergruppe i G(p) af orden $\frac{p-1}{2}$; er ρ en frembringer for G(p), er ρ^2 en frembringer for denne undergruppe, som kaldes gruppen af kvadratiske rester mod.p. Det ses, at a er kv. rest $\Leftrightarrow a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Denføres Legendresymbolet $(\frac{a}{p}) = 1$ hvis a er kv. rest, $= -1$ hvis a er kv.ikkerest og $= 0$, hvis $p \mid a$, så er $a^{\frac{p-1}{2}} \equiv (\frac{a}{p}) \pmod{p}$, thi $(a^{\frac{p-1}{2}}+1)(a^{\frac{p-1}{2}}-1) = a^{p-1}-1 \equiv 0 \pmod{p}$. Heraf ses, at $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$. Sæt $\zeta = e^{\frac{2\pi i}{p}}$ og betragt $T = \sum_{a \neq 0}(\frac{a}{p})\zeta^a \in \dot{Q}(\zeta)$. Vi finder (idet $\sum(\frac{b}{p}) = 0$), at

$$T^2 = \sum_{a \neq 0}\sum_{b \neq 0}(\frac{a}{p})(\frac{b}{p})\zeta^a\zeta^b = \sum_{a \neq 0}\sum_{b \neq 0}(\frac{a}{p})(\frac{ab}{p})\zeta^a\zeta^{ab}$$

$$= \sum_{a \neq 0}\sum_{b \neq 0}(\frac{b}{p})\zeta^{a(1+b)} = \sum_b (\frac{b}{p})\sum_{a \neq 0}\zeta^{a(1+b)}$$

$$=$$

$$= \sum_b \left(\frac{b}{p}\right) \sum_a \zeta^{a(1+b)} = \left(\frac{-1}{p}\right) p + \sum_{b \neq -1} \left(\frac{b}{p}\right) \sum_a \zeta^{a(1+b)}$$

$$= \left(\frac{-1}{p}\right) p = (-1)^{\frac{p-1}{2}}\, p,$$

hvoraf

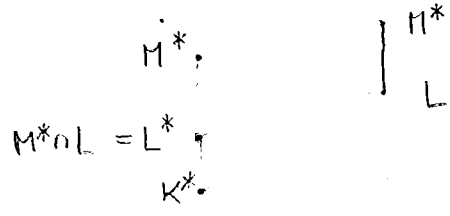
$$\sqrt{(-1)^{\frac{p-1}{2}}\, p} = \pm T \in \dot{Q}(\zeta) \text{ som påstået.} \blacksquare$$

Af lemmaet følger, at $\sqrt{p}$ eller $i\sqrt{p}$ ligger i $\dot{Q}(e^{\frac{2\pi i}{p}})$, og da $i \in Q(e^{\frac{2\pi i}{4p}})$ har vi altså i alle tilfælde $\sqrt{p} \in \dot{Q}(e^{\frac{2\pi i}{4p}})$. Og dermed: For $d = p_1 \cdots p_n$ kvadratfri, er $\sqrt{d} \in \dot{Q}(e^{\frac{2\pi i}{4p_1 \cdots p_n}})$. $\blacksquare$

Lad M/K være en endelig Galoisk udvidelse, og lad L/K være en vilkårlig udvidelse. M er spaltningslegeme for et separabelt polynomium $f(X) \in K[X]$. Er $\alpha_1, \ldots, \alpha_m$ rødderne i f(X), er $M = K(\alpha_1, \ldots, \alpha_m)$ f(X) er også separabelt over L. Lad ML betegne spaltningslegemet for f(X) over L. $ML = L(\alpha_1, \ldots, \alpha_m)$ og $ML \supseteq \begin{cases} M \\ L \end{cases}$, og intet ægte dellegeme af ML har denne egenskab. ML kaldes <u>kompositet</u> af M og L

Translationssætningen 1. <u>Lad M^*/K^* være en endelig Galois'sk udvidelse, og L/K en vilkårlig udvidelse, da er M^*L/L en endelig Galois'sk udvidelse, og $Gr(M^*L/L) \cong Gr(M^*/M^* \cap L)$. Specielt er $[M^*L:L] = [M^*:M^* \cap L]$.</u>

Bevis. Sæt $G^* = Gr(M^*/K^*)$. M^*L/L er endelig Galois'sk iflg. konstruktionen; sæt $H = Gr(M^*L/L)$, og lad $\sigma \in H$. Er $M^* = K^*(\alpha_1, \ldots, \alpha_m)$, er $\sigma(\{\alpha_1, \ldots, \alpha_m\}) = \{\sigma(\alpha_1), \ldots, \sigma(\alpha_m)\} = \{\alpha_1, \ldots, \alpha_m\}$: $\sigma(M^*) = M^*$. $\sigma|_{M^*}$ er derfor en automorfi i M^*. Ved $\sigma \to \sigma|_{M^*}$ defineres således en afbildning $Res : H \to G^*$, som er homomorf og injektiv, idet $M^*L = L(\alpha_1, \ldots, \alpha_m)$. Vi har altså $H \cong H|_{M^*} \subseteq G^*$. Nu er $M^{*H}|_{M^*} = \{a \in M^* \mid \forall \sigma|_{M^*} \in H|_{M^*} : \sigma(a) = a\} = \{a \in M^* \mid \forall \sigma \in H : \sigma(a) = a\} = M^* \cap (M^*L)^H = M^* \cap L$, så $Gr(M^*L/L) = H \cong H|_{M^*} = Gr(M^*/M^* \cap L)$



Bemærk, at hvis både M^* og L er indeholdt i en endelig Galois'sk udvidelse af K^*, da følger påstanden af Noethers 1.isomorfisætning.

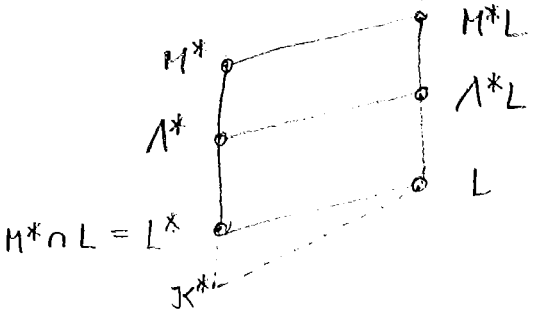
Lemma 1. <u>En L^*-basis $(\omega_1^*, \ldots, \omega_m^*)$ for M^* er en L-basis for M^*L.</u>

Bevis. Da $M^* = L^*(\omega_1^*, \ldots, \omega_m^*)$, er $M^*L = L(\omega_1^*, \ldots, \omega_m^*) = L[\omega_1^*, \ldots, \omega_m^*]$. For $a \in M^*L$ er $a = \sum_{\gamma_1, \ldots, \gamma_m} b_{\gamma_1, \ldots, \gamma_m} (\omega_1^*)^{\gamma_1} \ldots (\omega_m^*)^{\gamma_m}$ hvor $b_{\gamma_1, \ldots, \gamma_m} \in L$, og $(\omega_1^*)^{\gamma_1} \ldots (\omega_m^*)^{\gamma_m}$ er L^*- (og dermed L-) linearkombinationer af $\omega_1, \ldots, \omega_m$, så vektorrummet M^*L over L frembringes af $\omega_1^*, \ldots, \omega_m^*$. Da de to vektorrum har samme dimmension:

$[M^*L:L] = [M^*:L^*]$ er $\omega_1^*,\ldots,\omega_m^*$ uafhængige over L. ∎

Lemma 2. <u>Er $L^* \subseteq \Lambda^* \subseteq M^*$, er $[\Lambda^*:L^*] = [\Lambda^*L:L]$.</u>

Bevis. En L^*-basis $(\omega_1^*,\ldots,\omega_n^*)$ for Λ^* kan suppleres til en L^*-basis $(\omega_1^*,\ldots,\omega_m^*)$ for M^*. Iflg. lemma 1 er $\omega_1^*,\ldots,\omega_m^*$ og dermed også $\omega_1^*,\ldots\omega_n^*$ uafhængige over L. Da $\Lambda^* = L^*(\omega_1^*,\ldots,\omega_n^*)$, er $\Lambda^*L = L(\omega_1^*,\ldots,\omega_n^*) = L[\omega_1^*,\ldots,\omega_n^*]$ = vektorrummet over L frembragt af de lin.uafh. elementer $\omega_1^*,\ldots,\omega_n^*$. ∎

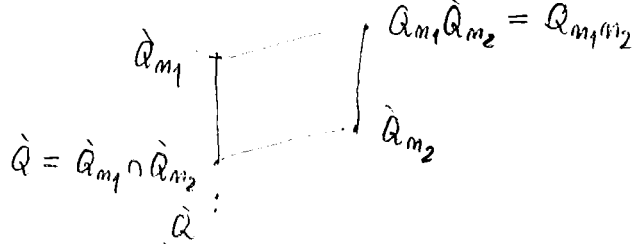


Sætning. <u>Afbildningen $\Lambda^* \to \Lambda^*L = \Lambda$ er en enentydig forbindelse mellem legemerne Λ^* mellem L^* og M^* og legemerne, Λ, mellem L og M^*L, idet $(\Lambda^*L)\cap M^* = \Lambda^*$ og $(M^*\cap\Lambda)L = \Lambda$ og $Gr(M^*/\Lambda^*) \cong Gr(M^*L/\Lambda^*L)$.</u>

Bevis. $\Lambda^*L \cap M^* \supseteq \Lambda^*$, og = gælder iflg. translationssætning 1, thi $[M^*:\Lambda^*L\cap M^*] = [M^*L:\Lambda^*L] = [M^*:\Lambda^*]$.

$(M^*\cap\Lambda)L \subseteq \Lambda$, og = gælder iflg. lemma, thi $[\Lambda:L] = [\Lambda\cap M^*:L^*] = [(M^*\cap\Lambda)L:L]$. ∎

Eks. $K^* = \dot{Q}$, $M^* = \dot{Q}(e^{\frac{2\pi i}{n_1}}) = \dot{Q}_{n_1}$, $L = \dot{Q}(e^{\frac{2\pi i}{n_2}}) = \dot{Q}_{n_2}$, hvor n_1 og n_2 er indb.primiske.



Nu findes $a,b\in\dot{Z}$, så $an_1+bn_2 = 1$, altså $\frac{1}{n_1n_2} = \frac{a}{n_1} + \frac{b}{n_2}$, hvoraf $e^{\frac{2\pi i}{n_1n_2}} = (e^{\frac{2\pi i}{n_1}})^b(e^{\frac{2\pi i}{n_2}})^a \in \dot{Q}_{n_1}\dot{Q}_{n_2}$, så $\dot{Q}_{n_1n_2} = \dot{Q}(e^{\frac{2\pi i}{n_1n_2}}) \subseteq \dot{Q}_{n_1}\dot{Q}_{n_2}$. Da den omvendte inklusion er tirviel er $\dot{Q}_{n_1}\dot{Q}_{n_2} = \dot{Q}_{n_1n_2}$. Nu er $[\dot{Q}_{n_1n_2}:\dot{Q}_{n_2}] = [\dot{Q}_{n_1n_2}:\dot{Q}]/[\dot{Q}_{n_2}:\dot{Q}] = \varphi(n_1n_2)/\varphi(n_2) = \varphi(n_1) = [\dot{Q}_{n_1}:\dot{Q}]$. Følgelig er $\dot{Q}_{n_1}\cap\dot{Q}_{n_2} = \dot{Q}$.

Alment gælder: $\dot{Q}_{n_1}\dot{Q}_{n_2} = \dot{Q}_{\{n_1,n_2\}}$ og $\dot{Q}_{n_1}\cap\dot{Q}_{n_2} = \dot{Q}_{(n_1,n_2)}$

Sætning om normalbasis. <u>Lad L/K være en endelig Galoisk udvidelse, hvor K har uendelig mange elementer, og sæt $G = Gr(L/K)$, $ord(G) = [L:K] = n$, da findes en normalbasis for L over K</u>): der findes $\vartheta\in L$

så at $\sigma_1(\vartheta),\ldots,\sigma_m(\vartheta)$, $\sigma_i \in G$, er en K-basis for L.
Bemærk, at da har $\mathrm{Irr}(\vartheta,K)$ rødderne $\sigma_1(\vartheta),\ldots,\sigma_m(\vartheta)$, der er indb. forskellige, så $\mathrm{grad}(\mathrm{Irr}(\vartheta,K)) = n$ d: $K(\vartheta) = L$.
Bevis. Hvis $\sigma_1(\vartheta),\ldots,\sigma_m(\vartheta)$ er lin. afh. og $a_1\sigma_1(\vartheta)+\ldots+a_m\sigma_m(\vartheta) = 0$ er ikke triviel, da har ligningssystemet $\sum_{i=1}^{n} a_i \sigma_j\sigma_i(\vartheta) = 0$, $j = 1,\ldots,n$ en ikke triviel løsning, så det er nok at vise, at der findes $\vartheta \in L$ med $\det(\sigma_i\sigma_j(\vartheta)) \neq 0$.
Lad $\alpha \in L$ være et primitivt element d: $L = K(\alpha)$, og sæt $f(X) = \mathrm{Irr}(\alpha,K)$, da har $f(X)$ de indbyrdes forskellige rødder $\sigma_1(\alpha),\ldots,\sigma_m(\alpha)$, hvoraf én er $= \alpha$. Nu er $f(X) = (X-\alpha)G(X)$, hvor $G(X) \in L[X]$, og $G(\alpha) \neq 0$, og dermed $f'(X) = (X-\alpha)G'(X)+G(X)$, så $f'(\alpha) = G(\alpha) \neq 0$. Sættes $g(X) = (f'(\alpha))^{-1}G(X)$, er $g(X) \in L[X]$, $\mathrm{grad}(g) = n-1$ og $g(\alpha) = 1$, $g(\sigma(\alpha)) = 0$ for $\sigma(\alpha) \neq \alpha$. Endvidere er $f(X) = (X-\alpha)f'(\alpha)g(X)$. Nu er $f(X) = \sigma_i f(X) = (X-\sigma_i(\alpha))f'(\sigma_i(\alpha))\sigma_i g(X)$, så vi har $\sigma_i g(\sigma_j(\ )) = \delta_{ij}$. For $i \neq j$ har $\sigma_i g(X)\sigma_j g(X)$ rødderne $\sigma_1(\alpha),\ldots,\sigma_m(\alpha)$, så $\sigma_i g(X)\sigma_j g(X) \equiv 0 \pmod{f(X)}$ i $L[X]$. $\sum_i \sigma_i g(X) - 1$ har ligeledes de n (forsk) rødder $\sigma_1(\alpha),\ldots,\sigma_m(\alpha)$, og da dets grad er $\leq n-1$, er $\sum_i \sigma_i g(X) = 1$. Nu er $\sigma_i g(X) = \sigma_i g(X)(\sum_j \sigma_j g(X)) \equiv (\sigma_i g(X))^2 \pmod{f(X)}$ i $L\,X$.
Sæt $D(X) = \det(\sigma_i\sigma_j g(X))$, da er $D(X)^2 = \det_{k,l}(\sum_i \sigma_k\sigma_i g(X)\sigma_l\sigma_i g(X))$. For $k \neq l$ er $\sigma_k\sigma_i \neq \sigma_l\sigma_i$, så $\sigma_k\sigma_i g(X)\sigma_l\sigma_i g(X) \equiv 0 \pmod{f(X)}$, og for $k = l$ er $\sum_i \sigma_k\sigma_i g(X)\sigma_l\sigma_i g(X) = \sum_i (\sigma_k\sigma_i g(X))^2 \equiv \sum_i \sigma_k\sigma_i g(X) = 1 \pmod{f(X)}$. Heraf følger, at $D(X)^2 \equiv 1 \pmod{f(X)}$ i $L[X]$, men da $D(X)$ så ikke er identisk 0, og da K indeholdt uendelig mange elementer, findes $a \in K$, så at $D(a) \neq 0$. Nu sættes $\vartheta = g(a) \in L$, da er $\sigma(g(a)) = \sigma g(a)$, så $\det(\sigma_i\sigma_j(\vartheta)) = \det(\sigma_i\sigma_j(g(a))) = \det(\sigma_i\sigma_j g(a)) = D(a) \neq 0$. ∎

Bks. Betragt $\dot{Q}(e^{\frac{2\pi i}{p}})/\dot{Q}$, hvor p er et primtal, og sæt $\zeta = e^{\frac{2\pi i}{p}}$. $F_p(X) = X^{p-1}+\ldots+X+1$, så graden er $p-1$ d: $1,\zeta,\ldots,\zeta^{p-2}$ er en basis for $\dot{Q}(\zeta)$. Da $1 = -\zeta-\ldots-\zeta^{p-2} - \zeta^{p-1}$ er også $(\zeta,\zeta^2,\ldots,\zeta^{p-1})$ en basis, og dette er en normalbasis.

Lad K være et legeme af Kar.=0, og lad M være spaltningslegemet for X^n-1 over K. Rødderne i X^n-1 udgør en multiplikativ undergruppe af orden n i M^*, og denne undergruppe er altså cyklisk. Er ζ en frembringer, da er altså $\zeta,\zeta^2,\ldots,\zeta^n = 1$ samtlige rødder. Da $M \supseteq \dot{Q}$, vil spaltningslegemet over K indeholde spaltningslegemet over Q, så M indeholder det n'te cirkeldelingslegeme $Q(\zeta)$, $\zeta^n = 1$; $M \supseteq K(\zeta) \supseteq \dot{Q}(\zeta)$. Da $\dot{Q}(\zeta)/\dot{Q}$ er endelig normal med abelsk faktorgrup-

pe, G(n), er M/K normal og (iflg. translationssætningen) $Gr(M/K) \cong Gr(\dot{Q}(\zeta)/\dot{Q}(\zeta) \cap K)$ som er en undergruppe i G(n); specielt er M/K abelsk.

Sætning. Er K et legeme af Kar(K) = 0, som indeholder de n'te enhedsrødder, og er $a \in K$, da har spaltningslegemet for X^n-a over K cyklisk Galoisgruppe, hvis orden er divisor i n.

Bevis. Er $\sqrt[n]{a}$ en vilkårlig rod i X^n-a, og $\zeta \in K$ en primitiv n'te enhedsrod, da er spaltningslegemet øjensynlig $K(\sqrt[n]{a})$. $\sigma \in Gr(K(\sqrt[n]{a})/K)$ er bestemt ved $\sigma(\sqrt[n]{a}) = \sqrt[n]{a}\,\zeta^{\nu}$, og afbildningen $\sigma \to \zeta^{\nu}$ definerer en injektiv homomorfi $G \to$ Gruppen af n'te enhedsrødder, d: G er isomorf med en undergruppe i $\dot{Z}/n\dot{Z}$. ∎

Sætning. Er K et legme af Kar(K) = 0, $a \in K$ og p et primtal, da er $X^p-a \in K[X]$ enten irreducibelt, eller har en rod i K.

Bevis. Spaltningslegemet for X^p-a er $K(\sqrt[p]{a},\zeta)$, hvor ζ er en primitiv p'te enhedsrod. Nu er $(X-\sqrt[p]{a})(X-\sqrt[p]{a}\,\zeta)\ldots(X-\sqrt[p]{a}\,\zeta^{p-1}) = X^p-a$, så hvis X^p-a var ~~x~~reducibel måtte et produkt af ovenstående faktorer ligge i K[X]. Konstantleddet i et sådant er $b = (\sqrt[p]{a})^{\nu}\zeta^{i}$, hvor $1 < \nu < p$. NU findes $h,k \in \dot{Z}$, så $\nu h+kp = 1$, og da $a^{\nu} = b^p$ er $a = a^{kp}a^{h\nu} = (a^k b^h)^p$, så X^p-a har en rod $a^k b^h$ i K. ∎

Korollar. Er K et legeme af Kar(K) = 0, $a \in K$ og p et primtal, så X^p-a ikke har rødder i K, da er $Gr(K(\sqrt[p]{a})/K) \cong \dot{Z}/p\dot{Z}$.

Eks. Betragt $\dot{Q}(e^{\frac{2\pi i}{7}})/\dot{Q}$, sæt $\zeta = e^{\frac{2\pi i}{7}}$, da er $Gr(\dot{Q}(\zeta)/\dot{Q}) \cong \dot{Z}/6\dot{Z}$. Idet τ betegner komplex konjugerein, har $\{e,\tau\}$ orden 2, så $\dot{Q}(\zeta)^{\{e,\tau\}}$ har orden 3, og er derfor cyklisk. Vi finder $\dot{Q}(\zeta)^{\{e,\tau\}} = \dot{Q}(e^{\frac{2\pi i}{7}}+e^{-\frac{2\pi i}{7}}) = \dot{Q}(\cos\frac{2\pi}{7})$.

Lemma. Er L et legeme, og G en endelig automorfigruppe i L, da er $H^1(G,L^*) = (1)$.

Bevis. Lad $\sigma \to a_\sigma$ være en krydset homomorfi. Lflg lemma p.IV,3 findes $x \in L$ så at $\sum_{\tau \in G} a_\tau x^\tau = \frac{1}{\alpha} \neq 0$. Nu er $a_\sigma{}^{\sigma}(\frac{1}{\alpha})^{\sigma} = a_\sigma \sum_{\tau \in G} a_\tau{}^{\sigma} x^{\sigma\tau} = \sum_{\tau \in G}(a_\sigma a_\tau{}^{\sigma})x^{\sigma\tau} = \sum_{\tau \in G} a_{\sigma\tau}x^{\sigma\tau} = \frac{1}{\alpha}$ eller $a_\sigma = \frac{\alpha^\sigma}{\alpha}$. ∎

Sætning. Er K et legeme af Kar(K) = 0, som indeholder de n'te enhehedsrødder, og er L/K en normal udvidelse med cyklisk Galoisgruppe af orden n, da er L/K simpel, og $L = K(\alpha)$, hvor $\alpha^n \in K$.

Bevis. K indeholder de n'te enhedsrødder, $\zeta,\ldots,\zeta^{n-1}$. Lad $G_{\sigma^\nu} = Gr(L/K) = \{\sigma,\ldots,\sigma^{n-1},\sigma^n = e\}$, og sæt $a_{\sigma^\nu} = \zeta^{\nu}$, da er $a_{\sigma^\nu}a_{\sigma^\mu} = \zeta^{\nu}\sigma^{\nu}(\zeta^{\mu}) = \zeta^{\nu}\zeta^{\mu} = \zeta^{\nu+\mu} = a_{\sigma^{\nu+\mu}} = a_{\sigma^\nu\sigma^\mu}$, så $\sigma^\nu \to a_{\sigma^\nu} = \zeta^{\nu}$ er en krydset homomorfi, og derfor principal, d.v.s. der findes $\alpha \in L^*$,

så $a_{\sigma^\nu} = \zeta^\nu = \frac{\alpha^{\sigma^\nu}}{\alpha}$; specielt er $a_\sigma = \zeta = \frac{\alpha^\sigma}{\alpha}$, altså $\sigma(\alpha) = \alpha\zeta$, men så er $\sigma^2(\alpha) = \alpha\zeta^2, \ldots, \sigma^{n-1}(\alpha) = \alpha\zeta^{n-1}$, $\sigma^n(\alpha) = \alpha\zeta^n = \alpha$. Da α's billeder ved automorfierne i G er indb. forskellige, er Grad(Irr $(\alpha,K)) = n$ ↯: $L = K(\alpha)$, og da $\sigma(\alpha^n) = \sigma(\alpha)^n = \alpha^n\zeta^n = \alpha^n$, er $\alpha^n \in L^G = K$. ∎

Sætning. <u>Er K et legeme af Kar(K) = p ≠ 0, og er a ∈K, da er X^p-X-a enten irreducibel over K, eller har en rod i K.</u>

Bevis. Er α en rod i X^p-X-a, da er spaltningslegemet K(α), thi rødderne er da $\alpha, \alpha+1, \ldots, \alpha+(p-1)$. ∎

Korollar. <u>Er K et legeme af Kar(K) = p, a∈K, så X^p-X-a ikke har rødder i K, da er spaltningslegemet Galoisk med cyklisk Galoisgruppe af orden p.</u>

Lemma. <u>Er L et legeme, og G en endelig automorfigruppe i L, da er $H^1(G,L^+) = (0)$.</u>

Bevis. Lad $\sigma \to a_\sigma$ være en krydset homomorfi. Iflg lemma p.IV,3 findes $x \in L$, så at $\sum_{\tau\in G} x^\tau \neq 0$. Sæt $-\alpha = (\sum_\tau a_\tau x^\tau)/(\sum_\tau x^\tau) = (\sum_\tau a_{\sigma\tau}x^{\sigma\tau})/(\sum_\tau x^{\sigma\tau})$, da er $\alpha^\sigma - \alpha = (\sum_\tau (-a_\tau^\sigma + a_{\sigma\tau})x^{\sigma\tau})/(\sum_\tau x^{\sigma\tau}) = a_\sigma$. ∎

Sætning. <u>Er K et legeme af Kar(K) = p, og er L/K en Galoisk udvidelse med cyklisk Galoisgruppe af orden p, da er L = K(α), hvor $\alpha^p - \alpha \in K$.</u>

Bevis. Vi har $K \supseteq \hat{F}_p = \{e, 2e, \ldots, (p-1)e, pe = 0\}$. Lad G_{σ^ν} = Gr(L/K) $= \{\sigma, \sigma^2, \ldots, \sigma^{p-1}, \sigma^p = e\}$ og sæt $a_{\sigma^\nu} = \nu e$, da er $a_{\sigma^\nu} + a_{\sigma^\mu} = \nu e + \sigma^\nu(\mu e)$ $\nu e + \mu e = (\nu+\mu)e = a_{\sigma^{\nu+\mu}} = a_{\sigma^\nu\sigma^\mu}$, så $\sigma^\nu \longrightarrow a_{\sigma^\nu} = \nu e$ er krydset og derfor principal, ↯: der findes $\alpha \in L$, så at $a_{\sigma^\nu} = \nu e = \alpha^{\sigma^\nu} - \alpha$; specielt er $a_\sigma = e = \sigma(\alpha) - \alpha$, eller $\sigma(\alpha) = \alpha + 1e$, men så er $\sigma^2(\alpha) = \alpha+2e, \ldots, \sigma^{p-1}(\alpha) = \alpha+(p-1)e$, $\sigma^p(\alpha) = \alpha$. Da α's billeder ved automorfierne i G er indb.forsk. er L = K(α), og da $\sigma(\alpha^p - \alpha) = \sigma(\alpha)^p - \sigma(\alpha) = (\alpha+1e)^p - (\alpha+1e) = \alpha^p - \alpha$, er $\alpha^p - \alpha \in L^G = K$. ∎

Eks. Er Kar(K) = p, og L/K Galoisk med $[L:K] = p^m$, da har G = Gr(L/K) en normalrække $G \triangleright G_1 \triangleright \cdots \triangleright G_m = E$, hvor $(G_i : G_{i+1}) = p$, og hertil svarer $K \subset K_1 \subset \ldots \subset L$, hvor K_i/K_{i-1} er Galoisk med cyklisk Galoisgruppe af orden p.

Sætning. For et legeme, L, er følgende betingelser ækvivalente:
1) L har ingen algebraisk undidelse
2) Ethvert irreducibelt polynomium i L[X] har grad 1.
3) Ethvert polynomium i L[X] af grad ≥ 1 er produkt af 1.grads-polynomier
4) Ethvert polynomium i L[X] af grad ≥ 1 har en rod i L
klart! og et legeme, der opfylder en af disse betingelser, kaldes algebraisk afsluttet.
Et legeme $L \supseteq K$ kaldes et algebraisk hylster af K, hvis L/K er algebraisk, og L er algebraisk afsluttet.

Sætning. Hvis K er dellegeme af et algebraisk afsluttet legeme, L, da er den algebraiske afslutning af K i L et algebraisk hylster af K.
Bevis. Et polynomium $f(X) \in \tilde{K}[X]$ har en rod α, i L. Da α således er algebraisk over $\tilde{K}$, og $\tilde{K}/K$ er algebraisk, er α algebraisk over K, altså $\alpha \in \tilde{K}$. ∎

Sætning. Hvis L/K er algebraisk, og hvis ethvert polynomium i K[X] spaltes i 1.gradsfaktorer i L[X], da er L et algebraisk hylster af K.
Bevis. Hvis L'/L er algebraisk, da er L'/K algebraisk. For $\alpha \in L'$ er $\mathrm{Irr}(\alpha,K) \in K[X]$, o: $\mathrm{Irr}(\alpha,K) = (X-\beta_1)\ldots(X-\beta_m)$, hvor $\beta_j \in L$, og da α = et β_j, er $\alpha \in L$. ∎

Eks. $\dot{C}$ er algebraisk afsluttet, og $\dot{Q}$'s algebraiske hylster i $\dot{C}$ er et algebraisk hylster af $\dot{Q}$.

Sætning. Til ethvert legeme, K, findes et og (på isomorfi nær) kun ét algebraisk hylster af L af K.
Bevis. Eksistens (efter Zariski): Sæt $\mathfrak{M} = K[X]^* \times \dot{Z} = \{(f(X),n) \mid f \neq 0 \wedge n \in \dot{Z}\}$. Afbildningen $a \longrightarrow (X-a,0)$ er bijektiv : K på $K' \subseteq \mathfrak{M}$ og organiserer K' til et legeme isomorft med K. Vi identificerer K og K'. Lad $\mathfrak{L}$ betegne mængden af delmængder $\mathfrak{Z} \subseteq \mathfrak{M}$ forsynet med kompositioner $\oplus$ og $\odot$ så at 1) $(\mathfrak{Z},\oplus,\odot)$ er et legeme 2) $\mathfrak{Z}$ har K som dellegeme og 3) Hvis $z = (f(X),n) \in \mathfrak{Z}$, da er $f(z) = 0$. (d.v.s. for $f(X) = a_0+a_1X+\ldots \in K[X]$ og $(f(X),n) \in \mathfrak{Z}$ gælder $f(z) = (X-a_0,0) \oplus (X-a_1,0) \odot (f(X),n) + \ldots = (X-0,0)$). $\mathfrak{L} \neq \emptyset$, idet $(K,+,\cdot) \in \mathfrak{L}$; 1) og 2) er trivielle, og er $z=(X-a,0) \in K$, da er $z-a = (X-a,0) - (X-a,0) = (X-0,0)$. |
Ved $(\mathfrak{Z},\oplus,\odot) \prec (\mathfrak{Z}',\oplus',\odot')$, når det første er dellegeme af det andet, defineres en induktiv ordning af $\mathfrak{L}$. Ifølge Zorns lemma har $\mathfrak{L}$ da et maximalt element $(L,\oplus,\odot)$. På grund af 3) er L/K en algebraisk

udvidelse.

Antag, at L ikke er algebraisk afsluttet, da fandtes $M \supset L$, så at M/L er algebraisk (og dermed M/K algebraisk). Vi konstruerer nu en afbildning $\phi: M \to \mathfrak{M}$ så $\phi|_L = id_L$. Sæt $\phi(a) = a$ for $a \in L$. For $\alpha \in M \setminus L$, er α rod i $f(X) = Irr(\alpha, K) \in K[X]$. Lad $f(X)$ have rødderne $\beta_1, \ldots, \beta_h \in L$ $(h \geq 0)$ og rødderne $\alpha = \alpha_1, \ldots, \alpha_g \in M \setminus L$ $(g \geq 1)$. Vi vælger nu g indbyrdes forskellige hele tal $n_1, \ldots, n_g$ så at $(f(X), n_1), \ldots, (f(X), n_g)$ er forskellige fra $\beta_1, \ldots, \beta_h$, og sætter $\phi(\alpha_1) = (f(X), n_1), \ldots, \phi(\alpha_g) = (f(X), n_g)$. $\phi(\alpha) = \phi(\alpha_1) \notin L$, thi var $\phi(\alpha) \in L$, da var $\phi(\alpha) = (f(X), n_1)$ rod i $f(X)$, altså $\phi(\alpha) =$ et β_j, hvilket ikke kan være tilfældet. Endvidere er ϕ klart injektiv. M's legemsstruktur kan nu "plantes over" i $\phi(M) \subseteq \mathfrak{M}$, så at ϕ bliver en isomorfi, og $L = \phi(L)$ bliver herved et dellegeme af $\phi(M)$. $\phi(M) \in \mathcal{S}$, thi 1) er opfyldt, 2) følger af $\phi(M) \supseteq \phi(L) = L \supseteq K$, og er $\phi(\alpha) \in \phi(M)$, $\phi(\alpha) \notin L$, da er $\phi(\alpha) = (f(X), n)$, hvor $f(X) = Irr(\alpha, K)$, men så er $f(\phi(\alpha)) = a_0 \oplus a_1 \circ \phi(\alpha) \oplus a_2 \circ \phi(\ )^2 \oplus \ldots = \phi(a_0 + a_1\alpha + a_2\alpha^2 + \ldots) = \phi(f(\alpha)) = \phi(0) = 0$, hvilket viser 3). Da $L \prec \phi(M)$, er dette en modstrid. ∎

<u>Entydighed:</u> Vi viser først

Lemma. <u>Hvis L/K er en algebraisk udvidelse, og $\hat{L}$ er algebraisk afsluttet, da kan enhver monomorfi $\varphi: K \to \hat{L}$ fortsættes til en monomorfi $\phi: L \to \hat{L}$.</u>

som medfører entydigheden, thi er $\varphi: K \to K^*$ en isomorfi, L/K og L^*/K^* algebraiske udvidelser, så at L, L^* er algebraisk afsluttede, da kan φ fortsættes til $\phi: L \to L^*$. Da L^*/K^* er algebraisk, og $L^* \supseteq \phi(L) \supseteq \varphi(K) = K^*$, er $L^*/\phi(L)$ algebraisk, og da L er algebraisk afsluttet, er også $\phi(L)$ algebraisk afsluttet, og dermed $\phi(L) = L^*$. ∎

Bevis for lemma. Sæt $\mathcal{S} = \{(K', \varphi') \mid K \subseteq K' \subseteq L$ og $\varphi': K' \to \hat{L}$ er en monomorfi, der udvider $\varphi\}$. $\mathcal{S} \neq \emptyset$ er ikke tom og kan ordnes partielt ved $(K', \varphi') \prec (K'', \varphi'')$, når $K' \subseteq K''$ og φ'' er en udvidelse af φ'. $\mathcal{S}$ er induktivt ordnet, og indeholder derfor et maximalt element iflg. Zorn. Lad $(\bar{K}, \bar{\varphi})$ være et sådant, da er $K \subseteq \bar{K} \subseteq L$ og $\bar{\varphi}|_K = \varphi$, da viser vi indirekte, at $\bar{K} = L$. Antag altså at $\bar{K} \subset L$. Da L/K er algebraisk, er $L/\bar{K}$ algebraisk. Lad $a \in L \setminus \bar{K}$, og sæt $f(X) = Irr(a, \bar{K})$. Nu er $\bar{\varphi}f \in \bar{\varphi}\bar{K}[X]$, og $\bar{\varphi}f$ er irreducibel i $\bar{\varphi}\bar{K}[X]$. Vi vælger $b \in \hat{L}$, så at $\bar{\varphi}f(b) = 0$, og har altså $\bar{\varphi}(Irr(a, \bar{K})) = \bar{\varphi}f = Irr(b, \bar{\varphi}\bar{K})$, så iflg. en tidligere lemma kan $\bar{\varphi}$ fortsættes til en isomrfi $\tilde{\varphi}: \bar{K}(a)$ på $\bar{\varphi}\bar{K}(b)$. Da $(\bar{K}, \bar{\varphi}) \prec (\bar{K}(a), \tilde{\varphi})$ er dette en modstrid. ∎

Eks. <u>$\dot{C}/\dot{Q}$ er en (uendelig) normal udvidelse</u>. Vi skal for $\alpha \in \dot{C} \setminus \dot{Q}$ bestemme en automorfi $\phi: \dot{C} \to \dot{C}$ så $\phi(\alpha) \neq \alpha$.

Hvis α er algebraisk over $\dot{Q}$, da findes $K \supseteq Q(\alpha)$, så $K/\dot{Q}$ er normal, og så findes en automorfi $\varphi: K \to K$, for hvilken $\varphi(\alpha) \neq \alpha$. Og hvis α er transcendent over $\dot{Q}$ er $Q(\alpha) \cong \dot{Q}(X)$, og da $X \to X+1$ bestemmer en automorfi i $\dot{Q}(X)$, findes en automorfi $\varphi: \dot{Q}(\alpha) \to \dot{Q}(\alpha)$ for hvilken $\varphi(\alpha) = \alpha+1 \neq \alpha$. Vi viser nu, at automorfien $\varphi: K \to K$ kan udvides til en automorfi $\bar{\phi}: \dot{C} \to \dot{C}$. $\mathfrak{M} = \{(K', \varphi') \mid K \subseteq K' \subseteq \dot{C}\}$ og φ' er en automorfi i K', som udvider $\varphi\}$ er induktivt ordnet; lad $(\hat{K}, \hat{\varphi})$ være maximalt element i $\mathfrak{M}$. Antag $\hat{K} \subset \dot{C}$. Hvis $\dot{C}/\hat{K}$ er algebraisk, kan $\hat{\varphi}$ iflg. entydighedssætningen udvides til en automorfi ϕ i $\dot{C}$, og ellers findes $\beta \in \dot{C}$, β transcendent over $\hat{K}$, og ved $\hat{\varphi}(\beta) = \beta$ kunne $\hat{\varphi}$ da udvides til en automorfi i $\hat{K}(\beta)$, i modstrid med maximaliteten af $(\hat{K}, \hat{\varphi})$.

KONSTRUKTION MED PASSER OG LINEAL

De tilladte operationer er
1) Konstruktion af linie gennem to givne eller konstruerede punkter. 2) Konstruktion af cirkel med givet eller konstrueret centrum, og et givet eller konstrueret liniestykke som radius.
3) At opsøge skæringspunkter mellem to linier, en linie og en cirkel eller to cirkler.

Mængden af punkter i den komplekse plan $\dot{C}$, der kan konstrueres udfra punkterne 0 og 1 kaldes de konstruerbare tal, og betegnes $\dot{K}$. Punkterne i K kan opskrives i en følge $x_0 = 0$, $x_1 = 1, x_2, x_3, \ldots$
Ved induktion vises
Sætning. Der findes en følge af reelle tallegemer $\dot{Q} = L_1 \subseteq L_2 \subseteq \ldots$ så at koordinaterne til x_n ligger i L_n, og således at hvert L_{n+1}, $n \geq 1$, enten er $= L_n$, eller $= L_n(\sqrt{a_n})$, hvor a_n er et positivt tal i L_n for hvilket $\sqrt{a_n} \notin L_n$.

Legemerne $L_n(i)$ indeholder nu punkterne $x_0, \ldots, x_n$, og hvert $L_n(\sqrt{-1})$ fås udfra $\dot{Q}$ ved successiv adjunktion af kvadratrødder.
Man kan nu vise:
Sætning. $\dot{K}$ er det mindste over for kvadratrod afsluttede tallegeme. Der findes en følge af tallegemer $\dot{Q} = K_0 \subseteq K_1 \subseteq \ldots$ hvor hvert K_{n+1} er af formen $K_{n+1} = K_n(\sqrt{a_n})$, hvor $a_n \in K_n$, $\sqrt{a_n} \notin K_n$ så at $\dot{K} = \bigcup K_n$. Specielt er hvert konstruerbart tal algebraisk af grad = potens af 2.

Den regulære n-kant er konstruerbar, hvis og kun hvis $e^{\frac{2\pi i}{n}}$ er konstruerbar.

Gauss' sætning. Den regulære n-kant er konstruerbar, hvis og kun $n = 2^\nu p_1 \dots p_r$, $\nu \geq 0, r \geq 0$ og $p_1, \dots, p_r$ er indb.forskellige primtal af formen 2^s+1, $s \geq 1$. (og et sådant primtal er endda af formen $2^{2^t}+1$).

Bevis. "$\Rightarrow$" Antag $e^{\frac{2\pi i}{n}}$ er konstruerbar, hvor $n = 2^\nu p_1^{\alpha_1} \dots p_R^{\alpha_R}$. Her er $\alpha_1 = \dots = \alpha_R = 1$, thi for ulige primtal er p^2-kanten ikke konstruerbar, da $e^{\frac{2\pi i}{p^2}}$'s grad, $\varphi(p^2) = p(p-1)$, ikke er en potens af 2. På samme måde ses, at hvis p-kanten er konstruerbar, da er $e^{\frac{2\pi i}{p}}$, grad, $\varphi(p) = p-1$, en potens af 2, altså $p = 2^s+1$.
"$\Leftarrow$" Hvis k- og m-kanten er konstruerbare, $(k,m) = 1$, da er km-kanten også konstruerbar, thi der findes $a,b \in \dot{Z}$, så $1 = ak+bm$, men så er $e^{\frac{2\pi i}{km}} = (e^{\frac{2\pi i}{m}})^a (e^{\frac{2\pi i}{k}})^b$ konstruerbar. Vi skal altså blot vise, at for $p = 2^s+1$, primtal, er p-kanten konstruerbar. Nu er $G = Gr(\dot{Q}(e^{\frac{2\pi i}{p}})/\dot{Q})$ cyklisk af orden $p-1 = 2^s$, så vi kan finde en normalrække for G med alle faktorer $= \dot{Z}/2\dot{Z}$. Den tilsvarende række af legemsudvidelser fås da ved adjunktion af kvadratrødder. ∎

POLYNOMIERS OPLØSELIGHED MED RODTEGN.

I det følgende betegner K et legeme med $Kar(k) = 0$. En udvidelse F/K kaldes radikal, hvis der findes endelig mange legemer $K = K_0 \subset K_1 \subset \dots \subset K_s = F$, så $K_i = K_{i-1}(\alpha_i)$, hvor $\alpha_i^{m_i} \in K_{i-1}$.

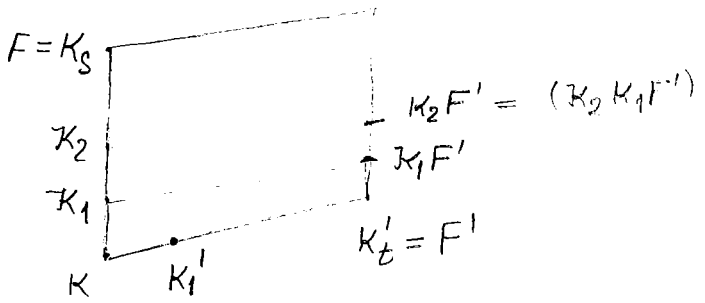
En udvidelse F/K kaldes metaabelsk, hvis der findes legemer $K = K_0 \subset K_1 \subset \dots \subset K_s = F$, så at K_i/K_{i-1} er en endelig abelsk udvidelse.

Lemma 1. Enhver radikal udvidelse er indeholdt i en metaabelsk udvidelse.

Bevis. Sæt $m = m_1 \dots m_s$. Er ζ en primitiv m-te enhedsrod, da er $K(\zeta)/K$ endelig abelsk, og $K_1(\zeta) = K(\zeta)(\alpha_1)$, så $K_1(\zeta)$ er abelsk (endda cyklisk jfr. p.IV,13) over $K(\zeta)$. Nu har vi $K \subset K(\zeta) \subset K_1(\zeta) \subset \dots \subset K_s(\zeta) = F(\zeta)$, så $F(\zeta)/K$ er metaabelsk, og $F \subseteq F(\zeta)$. ∎

Lemma 2. Kompositet FF' af metaabelske udvidelser $F, R'/K$ er igen metaabelsk.

Bvis. Vi har $K \subset K_1 \subset \dots \subset K_s = R$, og $K \subset K'_1 \subset \dots \subset K'_t = F'$. Iflg. translationssætningen er K_1F'/F' abelsk, K_2F'/K_1F' abelsk etc, altså $K \subset K'_1 \subset \dots \subset K_t' = F' \subset K_1F' \subset K_2F' \subset \dots \subset K_sF' = FF'$.



lemma 3. Enhver metaabelsk udvidelse er indeholdt i en normal metaabelsk xxudvidelse.

Bevis. Er F/K metaabelsk, findes $N \supseteq F$, så at N/K er endelig normal. Sæt $G = Gr(N/K) = \{\sigma_1,\ldots,\sigma_m\}$. For $\sigma \in G$ er σF metaabelsk over $\sigma K = K$ og $\sigma F \subseteq N$, altså er $\sigma_1 F,\ldots,\sigma_m F \subseteq N$ metaabelske over K, så at også $\tilde{F} = \sigma_1 F \sigma_2 F \ldots \sigma_m F$ er metaabelsk over K(lemma 2), og for $\sigma \in G$ er $\sigma\tilde{F} = \sigma\sigma_1 F \ldots \sigma\sigma_m F = \sigma_1 F \ldots \sigma_m F = \tilde{F}$, så $\tilde{F}/K$ er normal. ∎

Et irreducibelt polynomium $f(X) \in K[X]$ kaldes opløseligt med rodtegn, hvis der findes en radikal udvidelse af K, hvori f(X) har en rod.

Sætning. Er $f(X) \in K[X]$ irreducibel med spaltningslegemet L over K, da er f(X) opløseligt med rodtegn, hvis og kun hvis $G = Gr(L/K)$ er opløselig.

Bevis. "⇒" Lemma 1 og 3 viser, at den findes en normal metaabelsk udvidelse F/K, hvori f(X) har en rod. Af normaliteten følger, at $F \supseteq L$. Sæt $\tilde{G} = Gr(F/K)$. Da F er metaabelsk, findes $K \subset K_1 \subset \ldots \subset F$, med K_i/K_{i-1} abelsk. Til K_1 svarer $\tilde{G}_1 = Gr(F/K_1) \lhd \tilde{G}$, med $\tilde{G}/\tilde{G}_1$ abelsk. Det samme kan siges om K_1 og $\tilde{G}_1$ osv, atlså er $\tilde{G}$ opløselig, og da $L \subseteq F$, er $G = Gr(L/K) = Gr(F/K)/Gr(F/L)$ som homomorft billede af $\tilde{G}$ ligeledes opløselig.

"⇐" Sæt $n = ord(G)$, og lad ζ være en primitiv n'te enhedsrod, da er $Gr(L(\zeta)/K(\zeta))$ isomorf med en undergruppe i G, og derfor opløselig. Følgelig findes en kompositionsrække $G \rhd G_1 \rhd \cdots \rhd G_t = E$ med cykliske faktorer G_i/G_{i+1} af orden n_i $(n_i | n)$. Nu er den hertil hørende række af legemsudvidelser radikal (IV,13): $K(\zeta) \subset K_1(\zeta) \subset \cdots \subset L(\zeta)$, men så er også $L(\zeta)/K$ radikal, og $L \subseteq L(\zeta)$. ∎

Er f(X) et irreducibelt polynomium af grad n, da er Galoisgruppen for spaltningslegemet isomorf med en transitiv undergruppe i S_n.(p.IV,7). Da S_n er opløselig for $n \leq 4$, følger det, at polynomier af grad ≤ 4 er opløselige med rodtegn.

Eks. $K(X_1,\ldots,X_m)$ er spaltningslegemet for $Z^m - s_1 Z^{n-1} + \ldots + (-1)^n s_n$ over $K(s_1,\ldots,s_m)$. Galoisgruppen herfor

bliver oplagt isomorf med S_n.

Lemma. <u>En transitiv undergruppe, P, i S_p (p primtal), der indeholder blot én transposition er $= S_p$.</u>
Bevis. Lad S_p permutere $\{a_1,\ldots,a_p\}$ og sæt $a \sim b \Leftrightarrow a = b \vee (a,b) \in P$. Af $(a,b)(b,c)(a,b) = (a,c)$ ses let, at $\sim$ er en ækvivalensrelation. Er $a \sim b$ og $\sigma \in P$, da er $\sigma(a) \sim \sigma(b)$, thi $(\sigma(a), \sigma(b)) = \sigma(a,b)\sigma^{-1} \in P$. Ækvivalensklasser afbildes derfor i ækvivalensklasser ved premutaitonerne i P. Er ⓐ og ⓑ ækvivalensklasser, findes $\sigma \in P$, så at $\sigma(a) = b$ og dermed $\sigma(\text{ⓐ}) = \text{ⓑ}$, hvilket viser, at alle ækvivalensklasser har samme elementantal, som derfor må gå op i p. Da det iflg. foruds. er mindst 2, må det være p ɔ: alle elementer er ækvivalente, så alle transpositioner $\in P$, og dermed $P = S_p$. ∎

Sætning. <u>Er K et reelt tallegeme, og $f(X) \in K[X]$ irreducibelt af grad p (p primtal), da er Galoisgruppen for spaltningslegemet for f(X) over K isomorf med S_p, hvis f(X) har netop 2 ikke reelle rødder</u>.
Bevis. Galoisgruppen er isomorf med en transitiv undergruppe i S_p, og den indeholder kompleks konjugering, som må være en transposition af de to ikke reelle rødder; iflg. lemma er Galoisgruppen derfor isomorf med S_p. ∎

Eks. $f(X) = X^5 - 2qX + q$, hvor q primtal, er irreducibel over $\dot{Q}$ iflg. Sch.-Eisw. Det ses let, at f(X) har 3 reelle og 2 ikke reelle rødder. Følgelig er $G \cong S_5$, og <u>f(X) er derfor ikke opløselig med rodtegn over $\dot{Q}$.</u>

KAPITEL V IDEALTEORI I KOMMUTATIVE RINGE=

I det følgende betegner R en kommutativ ring med 1-element. $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \ldots$ betegner idealer i R. Vi sætter

$\mathfrak{a} \cap \mathfrak{b} = \{r \in R \mid r \in \mathfrak{a} \wedge r \in \mathfrak{b}\}$

$\mathfrak{a}\mathfrak{b} = \{\sum_i a_i b_i \mid a_i \in \mathfrak{a} \wedge b_i \in \mathfrak{b}\}$

$\mathfrak{a} + \mathfrak{b} = \{a+b \mid a \in \mathfrak{a} \wedge b \in \mathfrak{b}\}$

$\mathfrak{a} : \mathfrak{b} = \{r \mid r\mathfrak{b} \subseteq \mathfrak{a}\}$

Der gælder nu

1) $\mathfrak{a}+\mathfrak{b} = \mathfrak{b}+\mathfrak{a}$; $\mathfrak{a} + (\mathfrak{b}+\mathfrak{c}) = (\mathfrak{a}+\mathfrak{b}) + \mathfrak{c}$.
2) $\mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a}$; $\mathfrak{a}(\mathfrak{b}\mathfrak{c}) = (\mathfrak{a}\mathfrak{b})\mathfrak{c}$; $\mathfrak{a}(\mathfrak{b}+\mathfrak{c}) = \mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c}$.
3) $\mathfrak{a} \subseteq \mathfrak{a}+\mathfrak{b}$; $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$
4) $(\mathfrak{a}:\mathfrak{b})\mathfrak{b} \subseteq \mathfrak{a}$; $\mathfrak{a} \subseteq \mathfrak{a}:\mathfrak{b}$.
5) $(\bigcap_\iota \mathfrak{a}_\iota) : \mathfrak{b} = \bigcap_\iota (\mathfrak{a}_\iota : \mathfrak{b})$
6) $(\mathfrak{a}:\mathfrak{b}):\mathfrak{c} = \mathfrak{a}:(\mathfrak{b}\mathfrak{c})$
7) $\mathfrak{a}:(\mathfrak{b}+\mathfrak{c}) = (\mathfrak{a}:\mathfrak{b}) \cap (\mathfrak{a}:\mathfrak{c})$
8) $\mathfrak{a}:\mathfrak{b} = \mathfrak{a}:(\mathfrak{a}+\mathfrak{b})$.

$\mathfrak{p}$ kaldes et primideal, hvis $ab \in \mathfrak{p} \wedge a \notin \mathfrak{p} \Rightarrow b \in \mathfrak{p}$.

Sætning. $\mathfrak{p}$ er primideal $\Leftrightarrow$ R/$\mathfrak{p}$ er integritetsområde $\Leftrightarrow$ $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p} \wedge \mathfrak{a} \not\subseteq \mathfrak{p} \Rightarrow \mathfrak{b} \subseteq \mathfrak{p}$.

Sætning. $\mathfrak{a}_1 \ldots \mathfrak{a}_n \subseteq \mathfrak{p} \Rightarrow \mathfrak{a}_i \subseteq \mathfrak{p}$ for et vist i.

Sætning. $\mathfrak{a} \subseteq \mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_n \Rightarrow \mathfrak{a} \subseteq \mathfrak{p}_i$ for et vist i.

Bevis. Vi kan antage, at $\mathfrak{p}_j \not\subseteq \mathfrak{p}_i$ for $j \neq i$. Sæt $\mathfrak{b}_i = \mathfrak{a} \cap \bigcap_{j \neq i} \mathfrak{p}_j$ Hvis $\mathfrak{b}_i \not\subseteq \mathfrak{p}_i$, i = 1,...,n, findes $a_i \in \mathfrak{b}_i \setminus \mathfrak{p}_i \subseteq \mathfrak{a}$, men så er $\sum_i a_i \in \mathfrak{a}$, i modstrid med at $\mathfrak{a} \subseteq \mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_n$. Følgelig findes i så at $\mathfrak{b}_i \subseteq \mathfrak{p}_i$, men så er $\mathfrak{a} \subseteq \mathfrak{p}_i$ iflg. det foregående. ∎

$\mathfrak{m}$ kaldes et maximalideal, hvis $\mathfrak{m} \subset R$, og $\mathfrak{m} \subset \mathfrak{a} \subseteq R \Rightarrow \mathfrak{a} = R$.

Sætning. $\mathfrak{m}$ er maximalideal $\Leftrightarrow$ R/$\mathfrak{m}$ er et legeme.

Korollar. Et maximalt ideal er et primideal.

Sætning. Ethvert ægte ideal er indeholdt i et maximalt ideal, bevises v.hj.a. Zorn's lemma og eksistens af 1-element.

For et ideal $\mathfrak{a}$ defineres radikalet af $\mathfrak{a}$ som $\mathrm{Rad}(\mathfrak{a}) = \{r \in R \mid \exists n \in \mathbb{N} : r^n \in \mathfrak{a}\}$.

*) og $\sum_i a_i \notin \mathfrak{p}_j$, $j = 1, \ldots, n$

$\mathrm{Rad}(\mathfrak{a})$ er et ideal $\supseteq \mathfrak{a}$, og $\mathrm{Rad}(\mathfrak{a}\cap\mathfrak{b}) = \mathrm{Rad}(\mathfrak{a}\mathfrak{b}) = \mathrm{Rad}\mathfrak{a} \cap \mathrm{Rad}\mathfrak{b}$ og $\mathrm{Rad}(\mathrm{rad}\,\mathfrak{a}) = \mathrm{Rad}\,\mathfrak{a}$.

$a \in R$ kaldes nuldivisor, hvis der findes $b \in R \setminus (0)$, så $ab = 0$. $a \in R$ kaldes nilpotent, hvis $a^n = 0$ for et $n \in \mathbb{N} \Leftrightarrow a \in \mathrm{Rad}(0)$.

$\mathfrak{q}$ kaldes et primært ideal, hvis $ab \in \mathfrak{q}$ og $a \notin \mathfrak{q} \Rightarrow b \in \mathrm{Rad}\,\mathfrak{q}$.

Sætning. *$\mathfrak{q}$ er et primært ideal $\Leftrightarrow$ $R/\mathfrak{q}$ har kun nilpotnte nuldivisorer.*

Theorem. *Hvis $\mathfrak{q}$ er primært, da er $\mathfrak{p} = \mathrm{Rad}\,\mathfrak{q}$ et primideal, og $\mathfrak{q} \subseteq \mathfrak{p}' \Rightarrow \mathfrak{p} \subseteq \mathfrak{p}'$.*

$\mathfrak{q}$ kaldes da også $\mathfrak{p}$-primært.

Eks. R er P.I.D. $\mathfrak{a} = (a)$, $a = \varepsilon \pi_1^{m_1} \dots \pi_n^{m_n}$. $\mathrm{Rad}\,\mathfrak{a} = (\pi_1 \dots \pi_n)$. De primære idealer er (π^m).

Eks. på primært ideal, der ikke er potens af et primideal: $R = \mathbb{Z}[X]$, $\mathfrak{a} = (4,X)$. $\mathrm{Rad}\,\mathfrak{a} = (2,X)$ ses let at være maximalt, og dermed $\mathfrak{a}$ primært (se nedenfor). Hvis $\mathfrak{a} = \mathfrak{p}^n$, da er $\mathrm{Rad}\,\mathfrak{a} = \mathrm{Rad}\,\mathfrak{p}^m = \mathfrak{p}$, så $\mathfrak{p} = (2,X)$, men allerede $\mathfrak{p}^2 = (2,X)^2 = (4,2X,X^2) \subset (4,X)$.

Eks. på primidealpotens, der ikke er primær: $R = \{a_0 + 2a_1X + a_2X^2 + \dots \mid a_i \in \mathbb{Z}\} \subsetneq \mathbb{Z}[X]$. $\mathfrak{a} = \{f \in R \mid f(0) = 0\} = (2X, X^2, X^3)$ er primideal, da $R/\mathfrak{a} \cong \mathbb{Z}$, men $\mathfrak{a}^2 = (4X^2, 2X^3, 2X^4, X^4, X^5, X^6)$ er ikke primært, thi $4X^2 \in \mathfrak{a}^2$, $4 \notin \mathrm{Rad}\,\mathfrak{a}^2 = \mathfrak{a}$, og $X^2 \notin \mathfrak{a}^2$.

Eks. på ikke-primært ideal, hvis radikal er et primideal: $R = K[X,Y]$, $\mathfrak{a} = (X^2, XY) = (X)(X,Y)$. $\mathrm{Rad}\,\mathfrak{a} = \mathrm{Rad}(X) \cap \mathrm{Rad}(X,Y) = (X) \cap (X,Y) = (X)$ er et primideal, og $XY \in \mathfrak{a}$, $Y \notin \mathrm{Rad}\,\mathfrak{a}$ og $X \notin \mathfrak{a}$.

Sætning. *Hvis $\mathrm{Rad}\,\mathfrak{a} = \mathfrak{m}$ er maximalt, da er $\mathfrak{a}$ $\mathfrak{m}$-primært.*

Bevis. Vi skal vise, at $\mathfrak{a}$ er primært. For $xy \in \mathfrak{a}$, $x \notin \mathrm{Rad}\,\mathfrak{a} = \mathfrak{m}$, er $(x) + \mathfrak{m} = R$ og dermed $1 = rx + m$, hvor $m \in \mathfrak{m}$ og dermed $m^n \in \mathfrak{a}$. Nu er $1 = (rx+m)^n = x(\dots) + m^n = xc + m^n$, så $y = yxc + ym^n \in \mathfrak{a}$. ∎

Lemma. *Hvis $\mathfrak{p}, \mathfrak{q}$ er idealer, så at $\mathfrak{q} \subseteq \mathfrak{p} \subseteq \mathrm{Rad}\,\mathfrak{q}$ og $ab \in \mathfrak{q} \wedge b \notin \mathfrak{q} \Rightarrow a \in \mathfrak{p}$, da er $\mathfrak{q}$ $\mathfrak{p}$-primært.*

Bevis. $\mathfrak{q}$ er primært, thi $ab \in \mathfrak{q}$ og $b \notin \mathfrak{q} \Rightarrow a \in \mathfrak{p} \subseteq \mathrm{Rad}\,\mathfrak{q}$.

For $x \in \mathrm{Rad}\mathfrak{q}$ lader vi i være den mindste exponent ≥ 1, for hvilken $x^i \in \mathfrak{q}$. Hivs $i = 1$ er $x \in \mathfrak{q} \subseteq \mathfrak{p}$, og hvis $i > 1$, ses af $xx^{i-1} \in \mathfrak{q}$, og $x^{i-1} \notin \mathfrak{q}$, at $x \in \mathfrak{p}$. Altså er $\mathrm{Rad}\mathfrak{q} \subseteq \mathfrak{p}$. ∎

Sætning. Hvis $\mathfrak{q}$ er $\mathfrak{p}$-primær, da vil $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{q} \wedge \mathfrak{a} \notin \mathfrak{q} \Rightarrow \mathfrak{b} \subseteq \mathfrak{p}$.

DEKOMPOSITION

Lemma 1. Hvis $\mathfrak{q}$ er $\mathfrak{p}$-primær og $\mathfrak{a} \notin \mathfrak{p}$, da er $\mathfrak{q} : \mathfrak{a} = \mathfrak{q}$.
Bevis. Vi har $\mathfrak{q} : \mathfrak{a} \supseteq \mathfrak{q}$. Vælg nu $a \in \mathfrak{a} \setminus \mathfrak{p}$. For $x \in \mathfrak{q} : \mathfrak{a}$ er $ax \in \mathfrak{q}$, og da $a \notin \mathfrak{p}$ må $x \in \mathfrak{q}$. ∎

Lemma 2. Hvis $\mathfrak{q}$ er $\mathfrak{p}$-primær og $\mathfrak{a} \notin \mathfrak{q}$, da er $\mathfrak{q} : \mathfrak{a}$ $\mathfrak{p}$-primær.
Bevis. Vælg $a \in \mathfrak{a} \setminus \mathfrak{q}$. For $x \in \mathfrak{q} : \mathfrak{a}$ er $ax \in \mathfrak{q}$, og dermed $x \in \mathfrak{p}$, og for $y \in \mathfrak{p}$ er $y^m \in \mathfrak{q} \subseteq \mathfrak{q} : \mathfrak{a}$, altså $\mathfrak{q} : \mathfrak{a} \subseteq \mathfrak{p} \subseteq \mathrm{Rad}(\mathfrak{q} : \mathfrak{a})$.
For $\alpha\beta \in \mathfrak{q} : \mathfrak{a}$ og $\beta \notin \mathfrak{q} : \mathfrak{a}$ er $\alpha\beta a \in \mathfrak{q}$ for et $a \in \mathfrak{a}$ med $\beta a \notin \mathfrak{q}$ og dermed $\alpha \in \mathfrak{p}$. ∎

Lemma 3. Gennemsnit af endelig mange $\mathfrak{p}$-primære idealer er igen $\mathfrak{p}$-primært.
Bevis. Oplagt.

$\mathfrak{a} = \bigcap_i \mathfrak{q}_i$ (endelig mange) kaldes en dekomposition eller fremstilling. Iflg. lemma 3 kan vi "slå $\mathfrak{q}_i$'er hørende til samme $\mathfrak{p}$ sammen", og dernæst "droppe" overflødige $\mathfrak{q}_i$'er, så at $\mathfrak{q}_i \not\supseteq \bigcap_{j \neq i} \mathfrak{q}_j$. Den herved opnåede fremstilling kaldes uforkortelig eller normal.

Eks. på ikke entydig fremstilling: $R = K[X,Y]$; $\mathfrak{a} = (X^2, XY) = (X) \cap (X^2, XY, Y^2) = (X) \cap (X^2, Y)$ ses at være uforkortelige fremstillinger.

Entydighedssætning. Hvis $\mathfrak{a} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_m = \mathfrak{q}_1' \cap \ldots \mathfrak{q}_n'$ er uforkortelige fremstillinger med $\mathfrak{q}_i$ $\mathfrak{p}_i$-primær, og $\mathfrak{q}_j'$ $\mathfrak{p}_j'$-primær, da er 1) $m = n$ og 2) efter premutation $\mathfrak{p}_i = \mathfrak{p}_i'$, $i = 1, \ldots, n$.
Bevis. Hvis $\mathfrak{a} = R$ er alt trivielt. Antag $\mathfrak{a} \neq R$. Blandt $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$, $\mathfrak{p}_1', \ldots, \mathfrak{p}_n'$ findes et maximal (m.h.t. $\subseteq$), fx $\mathfrak{p}_m$. Vi viser, at $\mathfrak{p}_m =$ et $\mathfrak{p}_j'$, og hertil er det nok, at $\mathfrak{p}_m \subseteq$ et $\mathfrak{p}_j'$. Indirekte: Hvis $\mathfrak{p}_m \not\subseteq \mathfrak{p}_j'$, $j = 1, \ldots, m$, da er $\mathfrak{q}_j' : \mathfrak{q}_m = \mathfrak{q}_j'$, thi $\mathfrak{q}_m \not\subseteq \mathfrak{p}_j'$, og påstanden følger af lemma 1. Endvidere er $\mathfrak{p}_m \not\subseteq \mathfrak{p}_i'$, $i = 1, \ldots, n-1$, og vi får derfor analogt $\mathfrak{q}_i : \mathfrak{q}_m = \mathfrak{q}_i$, $i = 1, \ldots, n-1$.
Nu er dels

$$(\mathfrak{a} : \mathfrak{q}_m) = (\bigcap_j \mathfrak{q}_j') : \mathfrak{q}_m = \bigcap_j (\mathfrak{q}_j' : \mathfrak{q}_m) = \bigcap_j \mathfrak{q}_j' = \mathfrak{a}$$

dels

$$(\mathfrak{a} : \mathfrak{q}_m) = (\bigcap_i \mathfrak{q}_i) : \mathfrak{q}_m = \bigcap_{i \neq m} (\mathfrak{q}_i : \mathfrak{q}_m) \cap (\mathfrak{q}_m : \mathfrak{q}_m) = \bigcap_{i \neq m} \mathfrak{q}_i,$$

altså $\mathfrak{a} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_{m-1}$ i strid med uforkorteligheden.
Vi kan antage, at $\mathfrak{p}_m = \mathfrak{p}_m'$; $\mathfrak{q} = \mathfrak{q}_m \cap \mathfrak{q}_m'$ er da $\mathfrak{p}_m$-primært. Vi har da $\mathfrak{a} : \mathfrak{q} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_{m-1}$, da $\mathfrak{q} \not\supseteq \mathfrak{p}_i$, $i = 1,\ldots,n-1$ og analogt $\mathfrak{a} : \mathfrak{q} = \mathfrak{q}_1' \cap \ldots \cap \mathfrak{q}_{m-1}'$ altså $\mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_{m-1} = \mathfrak{q}_1' \cap \ldots \cap \mathfrak{q}_{m-1}'$ o.s.v. ∎

I $\mathfrak{a} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_m$ kaldes $\mathfrak{q}_i$ en <u>minimalkomponent</u>, hvis $\mathfrak{p}_j \not\subseteq \mathfrak{p}_i$, $j \neq i$.

Tillæg til entydighedssætning. <u>De minimale komponenter er entydigt bestemt ved .</u>

Bevis. (for R integritetsområde):
Indskud: Lad R være et int. område og S et multiplikativt system i $R \setminus (0)$, da Sættes $\frac{R}{S} = \left\{ \frac{r}{s} \mid r \in R \wedge s \in S \right\} \subseteq$ kvotientlegemet for R. Det ses let, at $\mathfrak{a}\frac{R}{S} = \left\{ \frac{a}{s} \mid a \in \mathfrak{a} \wedge s \in S \right\}$. Der gælder

$$\underline{(\mathfrak{a} \cap \mathfrak{b})\tfrac{R}{S} = \mathfrak{a}\tfrac{R}{S} \cap \mathfrak{b}\tfrac{R}{S},}$$

thi "$\subseteq$" er trivielt, og for $\frac{r}{s} \in \mathfrak{a}\frac{R}{S} \cap \mathfrak{b}\frac{R}{S}$ er $\frac{r}{s} = \frac{a}{s_1} = \frac{b}{s_2} = \frac{as_2}{s_1 s_2} = \frac{bs_1}{s_1 s_2} \in (\mathfrak{a} \cap \mathfrak{b})\frac{R}{S}$. Endvidere

$$\underline{\mathfrak{a}\tfrac{R}{S} = \tfrac{R}{S},} \quad \text{hvis } S \cap \mathfrak{a} \neq \emptyset.$$

Lad nu $\mathfrak{a} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_m$ ≠ og antag, at $\mathfrak{q}_1$ er minimalkomponent. $S = R \setminus \mathfrak{p}_1 \subsetneq R \setminus (0)$ er et multiplikativt system, og $\mathfrak{a}\frac{R}{S} = \mathfrak{q}_1\frac{R}{S}$, thi minimaliteten af $\mathfrak{q}_1$ medfører $\mathfrak{q}_i \cap S \neq \emptyset$, og dermed $\mathfrak{q}_i\frac{R}{S} = \frac{R}{S}$, $i = 2,\ldots,n$. Nu er $\mathfrak{a}\frac{R}{S} \cap R = \mathfrak{q}_1$, thi "$\supseteq$" er oplagt, og for $r \in \mathfrak{q}_1\frac{R}{S} \cap R$ er $r = \frac{q}{s}$, altså $rs \in \mathfrak{q}_1$, og da $s \notin \mathfrak{p}_1$ er $r \in \mathfrak{q}$. Heraf følger påstanden. ∎

NOETHERSKE RINGE.

Man viser let, at følgende betingelser er ækvivalente:

1) Ethvert $\mathfrak{a} \subseteq R$ er endeligt frembragt ($\overset{def.}{\Longleftrightarrow}$ R er Noethersk)
2) a.c.c. (axcending chain condition)
3) Maximalbetingelsen gælder for idealerne i R.

Eks. a) Et P.I.D. er Noethersk. b) $R = \hat{Z}[\sqrt{-3}]$ er Noethersk, thi $(R,+)$ er fri abelsk gruppe af rang 2, så et ideal, $\mathfrak{a}$, er fri abelsk af rang ≤ 2, og specielt endeligt frembragt. 3) $R = \hat{C}_L[0,1]$ er ikke Noethersk. Betragt fx idealet af fkt., der er 0 i en omegn af 0
d) $R = \{ \text{pol. i } X^{\frac{1}{2m+1}},\ m=0,1,\ldots \}$ er ikke Noethersk. fx. er $(X) \subset (X^{\frac{1}{3}}) \subset (X^{\frac{1}{9}}) \subset (X^{\frac{1}{27}}) \subset \ldots$

Sætning. <u>R Noethersk ⇒ R/$\mathfrak{a}$ Noethersk er triviel</u>, og omvendt: hvis R/$\mathfrak{a}$ Noethersk for alle $\mathfrak{a} \neq (0)$, da er R Noethersk iflg. a.c.c.

Sætning. (Hilbert)= Hvis R er Noethersk, da er også R[X] Noethersk.

Bevis. For et ideal, $\mathcal{A}$, i R[X], sættes $\mathfrak{a}_n = \{r \in R \mid \exists\ r_0,\ldots,r_{n-1} \in R : rX^n + r_{n-1}X^{n-1} + \ldots + r_0 \in \mathcal{A}\}$. $\mathfrak{a}_n$ er et ideal i R, og $\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \ldots$

Lemma. Hvis $\mathcal{A} \subseteq \mathcal{B}$ og $\mathcal{A} \to (\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \ldots)$ og $\mathcal{B} \to (\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \ldots$ da er $\mathcal{A} = \mathcal{B}$.

Bevis. Lad $f(X) \in \mathcal{B}$, $f(X) = r_0 + \ldots + r_n X^n$, da er $r_n \in \mathfrak{b}_n = \mathfrak{a}_n$, så der findes $g_0 \in \mathcal{A}$, så at $\operatorname{grad}(f-g_0) \leq n-1$. Da $g_0 \in \mathcal{B}$, er $f-g_0 \in \mathcal{B}$, så der findes $g_1 \in \mathcal{A}$, så at $\operatorname{grad}(f-g_0-g_1) \leq n-2$. $f-g_0-g_1 \in \mathcal{B}$ o.s.v. Til sidst fås $\operatorname{graf}(f-g_0-\ldots-g_n) \leq n-(n+1) = -1$, altså $f = g_0+\ldots+g_n \in \mathcal{A}$. ∎

Betragt nu en stigende kæde $\mathcal{A}_0 \subseteq \mathcal{A}_1 \subseteq \ldots$ da har vi

$$\begin{array}{ccccccccc}
\mathcal{A}_0 & \longrightarrow & \mathfrak{a}_{00} & \subseteq & \mathfrak{a}_{01} & \subseteq & \mathfrak{a}_{02} & \subseteq & \cdots \\
\cap\!\!| & & \cap\!\!| & & \cap\!\!| & & \cap\!\!| & & \\
\mathcal{A}_1 & \longrightarrow & \mathfrak{a}_{10} & \subseteq & \mathfrak{a}_{11} & \subseteq & \mathfrak{a}_{12} & \subseteq & \cdots \\
\cap\!\!| & & \cap\!\!| & & \cap\!\!| & & \cap\!\!| & & \\
\mathcal{A}_2 & \longrightarrow & \mathfrak{a}_{20} & \subseteq & \mathfrak{a}_{21} & \subseteq & \mathfrak{a}_{22} & \subseteq & \cdots \\
\cap\!\!| & & \cap\!\!| & & \cap\!\!| & & \cap\!\!| & & \\
\vdots & & \vdots & & \vdots & & & & \\
j = M & & & & & & & & \mathfrak{a}_{NN} = \cdots \\
 & & & & & & & & \| \\
 & & & & & & & & \vdots
\end{array}$$

I følgen $\mathfrak{a}_{11} \subseteq \mathfrak{a}_{22} \subseteq \mathfrak{a}_{33} \subseteq \ldots$ har vi $\mathfrak{a}_{NN} = \mathfrak{a}_{N+1,N+1} = \ldots$ og dermed $\mathfrak{a}_{pq} = \mathfrak{a}_{NN}$ for $p \geq N$ og $q \geq N$. For $i = 0,1,\ldots,N-1$ gælder for et vist n, at $\mathfrak{a}_{n_i i} = \mathfrak{a}_{n_i+1,i} = \ldots$, så for $j \geq \max\{n_1,\ldots,n_{N-1},N\} = M$ har vi $\mathfrak{a}_{ji} = \mathfrak{a}_{j+1,i} = \mathfrak{a}_{j+2,i} = \ldots$, $i = 0,1,2,\ldots$ og dermed $\mathcal{A}_j = \mathcal{A}_{j+1} = \ldots$ iflg lemma. ∎

Eks. I $\mathbb{K}[X,Y]$ findes til hvert $n \in \mathbb{N}$ et $\mathfrak{a}$, der ikke kan frembringes af n elementer. $\mathfrak{M} = (X,Y)$, $\mathfrak{a} = \mathfrak{M}^n = (X^n, X^{n-1}Y, \ldots, Y^n)$ kan ikke frembringes af n elementer; lad nemlig V_n betegne vektorrummet over K af homogene n-tegradspolynomier. En basis for V_n er $X^n, X^{n-1}Y, \ldots, Y^n$, altså $\dim V_n = n+1$. Antog man, at $\mathfrak{a} = (f_1,\ldots,f_n)$, og var $f_j^{(n)}$ den homogene bestanddel af f_j af grad n, da ville $X^{n-i}Y^i$ være K-lin-komb. af $f_1^{(n)},\ldots,f_n^{(n)}$, modstrid.

Et ideal $\mathfrak{a}$ i ringen R kaldes irreducibelt, hvis $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ medfører $\mathfrak{a} = \mathfrak{b}$ eller $\mathfrak{a} = \mathfrak{c}$.

Eks. Et primideal er irreducibelt, thi er $\mathfrak{p} = \mathfrak{b} \cap \mathfrak{c}$, hvor $\mathfrak{p} \subset \mathfrak{b}$ og $\mathfrak{p} \subset \mathfrak{c}$, da findes $b \in \mathfrak{b} \setminus \mathfrak{p}$ og $c \in \mathfrak{c} \setminus \mathfrak{p}$, men $bc \in \mathfrak{b} \cap \mathfrak{c} = \mathfrak{p}$.

Sætning. I en Noethersk ring er ethvert ideal gennemsnit af primæridealer.

Bevises (Se Northcott) ved to lemmaer:

Lemma 1. I en Noethersk ring er hvert ideal gennemsnit af irreducible idealer.

Lemma 2. I en Noethersk ring er et irreducibelt ideal primært.

Bemærk. I en ikke Noethersk ring behøver et irreducibelt ideal ikka at være primært.

Eks. Selv om R er Noethrsk behøver et primært ideal ikke at være irreducibelt. I fx. $R = K[X,Y]$ er (X,Y) maksimalt, så $(X,Y)^2 = (X^2,XY,Y^2)$ er primært, men $(X^2,XY,Y^2) = (X^2,Y) \cap (X,Y^2)$.

Eks. Et ideal $\mathfrak{a}$ i en (vilk.) ring R, kaldes primalt, hvis nuldivisorerne i $R/\mathfrak{a}$ udgør et ideal. Et primært ideal er primalt, thi for et primært ideal, $\mathfrak{a}$, er nuldivisorerne i $R/\mathfrak{a}$ netop $\mathrm{Rad}_{R/\mathfrak{a}}(0)$, altså et ideal. Hvis $\mathfrak{a}$ er primalt, da er nuldivisorerne i $R/\mathfrak{a}$ endda et primideal (oplagt). Et irreducibelt ideal er primalt. Indirekte: Ved overgang til $R/\mathfrak{a}$ kan vi antage, at $\mathfrak{a} = (0)$. Nu findes nuldivisorer a,b i R så at $a+b$ ikke er nuldivisor, men så er $(0) \subset (0):(a)$, $(0) \subset (0):(b)$ og $(0) = (0):(a+b) = [(0):(a)] \cap [(0):(b)]$.

Idealer $\mathfrak{a},\mathfrak{b}$ kaldes komaximale, hvis $\mathfrak{a}+\mathfrak{b} = R$.

Sætning. Hvis $\mathfrak{a}$ og $\mathfrak{b}$ er komaximale, da er $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$.

Bevis. Alment gælder $(\mathfrak{a}+\mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) = \mathfrak{a}(\mathfrak{a} \cap \mathfrak{b}) + \mathfrak{b}(\mathfrak{a} \cap \mathfrak{b}) \subseteq \mathfrak{a}\mathfrak{b}$, og påstanden følger nu let. $\subseteq \mathfrak{a} \cap \mathfrak{b}$.

Sætning. Hvis $\mathfrak{a},\mathfrak{b}$ og $\mathfrak{a},\mathfrak{c}$ er komaximale, da er også $\mathfrak{a},\mathfrak{b}\mathfrak{c}$ komaximale.

Bevis. thi $R \supseteq \mathfrak{a}+(\mathfrak{b} \cap \mathfrak{c}) \supseteq \mathfrak{a}+\mathfrak{b}\mathfrak{c} \supseteq \mathfrak{a}^2+\mathfrak{a}\mathfrak{b}+\mathfrak{a}\mathfrak{c}+\mathfrak{b}\mathfrak{c} = (\mathfrak{a}+\mathfrak{b})(\mathfrak{a}+\mathfrak{c}) = R$.

Sætning. Hvis $\mathrm{Rad}\,\mathfrak{a}, \mathrm{Rad}\,\mathfrak{b}$ er komaximale, da er $\mathfrak{a},\mathfrak{b}$ komaximale.

Bevis. Da vi alment har $\mathrm{Rad}\,\mathfrak{a}+\mathrm{Rad}\,\mathfrak{b} \subseteq \mathrm{Rad}(\mathfrak{a}+\mathfrak{b})$, altså i dette tilfælde $\mathrm{Rad}(\mathfrak{a}+\mathfrak{b}) = R$, er $1^n \in \mathfrak{a}+\mathfrak{b}$ d: $1 \in \mathfrak{a}+\mathfrak{b}$ d: $\mathfrak{a}+\mathfrak{b} = R$.

Sætning. I et Noethersk integritetsområde, hvor ethvert ~~ægte~~ ikke-trivielt primideal er maximalt, kan hvert $\mathfrak{a} \neq (0)$ entydigt skrives $\mathfrak{a} = \prod_i \mathfrak{q}_i$, hvor $\mathfrak{q}_i$ er $\mathfrak{p}_i$-primært og $\mathfrak{p}_i \neq \mathfrak{p}_j$, $i \neq j$.

Bevis. Lad $\mathfrak{a} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n$ være en normal fremstilling. Da

$\mathcal{A} \neq (0)$ er $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ maximale, og da $\mathfrak{p}_i \neq \mathfrak{p}_j$, $i \neq j$, er $\mathfrak{p}_i + \mathfrak{p}_j = R$, og dermed $\mathcal{Q}_i + \mathcal{Q}_j = R$, men så er $\mathcal{Q}_i + \bigcap_{j \neq i} \mathcal{Q}_j = R$ og følgelig $\mathcal{A} = \mathcal{Q}_1 \cap \bigcap_{j \neq 1} \mathcal{Q}_j = \mathcal{Q}_1 \cdot \bigcap_{j \neq 1} \mathcal{Q}_j = \mathcal{Q}_1 \mathcal{Q}_2 \cdot \bigcap_{j > 2} \mathcal{Q}_j = \ldots = \mathcal{Q}_1 \mathcal{Q}_2 \cdots \mathcal{Q}_n$.

Er omvendt $\mathcal{A} = \mathcal{Q}_1 \cdots \mathcal{Q}_n$ og $\mathcal{Q}_i \neq \mathcal{Q}_j$, $i \neq j$, da finder vi $\mathcal{A} = \mathcal{Q}_1 \cap \ldots \cap \mathcal{Q}_n$, og denne fremstilling er uforkortelig, thi var fx. $\mathcal{Q}_1 \supseteq \mathcal{Q}_2 \cap \ldots \cap \mathcal{Q}_n$, da var $\mathfrak{p}_1 \supseteq \mathcal{Q}_2 \cap \ldots \cap \mathcal{Q}_n$, altså fx $\mathfrak{p}_1 \supseteq \mathcal{Q}_2$, og dermed $\mathfrak{p}_1 = \mathfrak{p}_2$. Da alle $\mathcal{Q}$erne er minimalkomponenter, følger entydigheden. ∎

Sætning. Den direkte sum af (endl.man.) P.I.R.'er er et P.I.R.

Bevis. Lad $\mathcal{A} \subsetneq R_1 \oplus R_2$, sæt $\mathcal{A}_1 = \{r_1 \in R_1 \mid (r_1, 0) \in \mathcal{A}\} \subsetneq R_1$ og $\mathcal{A}_2 = \{r_2 \in R_2 \mid (0, r_2) \in \mathcal{A}\}$, da er $\mathcal{A}_1$, $\mathcal{A}_2$ idealer i R_1 og R_2 resp., altså $\mathcal{A}_1 = (a_1)$, $a_1 \in R_1$, og $\mathcal{A}_2 = (a_2)$, $a_2 \in R_2$, og det er nu let af vise, at $\mathcal{A} = ((a_1, a_2))$.

Et P.I.R. kaldes en speciel P.I.R., hvis det indeholder netop ét ægte primideal.

Eks. $\mathbb{Z}/p^n\mathbb{Z}$ er et speciel P.I.R.

Sætning. (Krull). Enhver P.I.R. er direkte sum af P.I.D.'er og specielle P.I.R.'er.

Først et lemma. Lad R være P.I.R., $\mathfrak{p}$ et ægte primideal, og $\mathfrak{p}' \subset \mathfrak{p}$, da er 1) $\mathfrak{p}'$ det eneste primideal $\subset \mathfrak{p}$, 2) ethvert primærideal der er $\subsetneq \mathfrak{p}$, vil $\supseteq \mathfrak{p}'$ og 3) Hvis $\mathfrak{p}_1$ er et ægte primideal, da er enten $\mathfrak{p}, \mathfrak{p}_1$ komaximale, eller det ene er indeholdt i det andet.

Bevis. Sæt $\mathfrak{p} = (p)$, $\mathfrak{p}' = (p')$; endvidere $p' = rp \in \mathfrak{p}'$, og da $p \notin \mathfrak{p}'$, er $r \in \mathfrak{p}'$, så $r = sp'$. Nu er $p' = rp = sp'p$, altså

$$p'(1-ps) = 0, \text{ hvor } 1-ps \notin \mathfrak{p},$$

da $\mathfrak{p} \subset R$. 1) Hvis $\tilde{\mathfrak{p}} \subset \mathfrak{p}$, da er $1-ps \notin \tilde{\mathfrak{p}}$, hvoraf $p' \in \tilde{\mathfrak{p}}$, altså $\mathfrak{p}' \subseteq \tilde{\mathfrak{p}}$. Ombyttes rollerne fås $\tilde{\mathfrak{p}} \subseteq \mathfrak{p}'$. 2). Hvis $\mathcal{Q} \subsetneq \mathfrak{p}$ er primær, da er $\operatorname{Rad}\mathcal{Q} \subsetneq \mathfrak{p}$, og specielt $1-ps \notin \operatorname{Rad}\mathcal{Q}$, hvoraf $p' \in \mathcal{Q}$, altså $\mathfrak{p}' \subseteq \mathcal{Q}$. 3) Antag endelig $\mathfrak{p} \neq \mathfrak{p}_1$. Hvis $\mathfrak{p} + \mathfrak{p}_1 \subset R$, er $\mathfrak{p} + \mathfrak{p}_1 \subsetneq \mathfrak{M} \subset R$, hvor fx $\mathfrak{p} \subset \mathfrak{M}$. Hvis også $\mathfrak{p}_1 \subset \mathfrak{M}$, var $\mathfrak{p} = \mathfrak{p}_1$ iflg. 2), så vi slutter at $\mathfrak{p}_1 = \mathfrak{M} \supset \mathfrak{p}$.

Bevis for krulls sætning. Lad $(0) = \mathcal{Q}_1 \cap \ldots \cap \mathcal{Q}_m$ være uforkortelig, med $\mathcal{Q}_i$ $\mathfrak{p}_i$-primær. Antog man $\mathfrak{p}_i + \mathfrak{p}_j \subset R$ med et $i \neq j$, da var fx. $\mathfrak{p}_i \subset \mathfrak{p}_j$ flg. lemma 3). Da $\mathcal{Q}_i \subsetneq \mathfrak{p}_i \subset \mathfrak{p}_j$, er $\mathcal{Q}_i = \mathfrak{p}_i$ i flg. lemma 2), og da $\mathcal{Q}_j \subsetneq \mathfrak{p}_j$, vil $\mathcal{Q}_i \supseteq \mathfrak{p}_i = \mathcal{Q}_i$, i strid med uforkorteligheden. Altså er $\mathfrak{p}_i + \mathfrak{p}_j = R$ og dermed $\mathcal{Q}_i + \mathcal{Q}_j = R$ for

for $i \neq j$. Heraf følger imidlertid let, at $R = R/(o) \cong R/\mathfrak{q}_1 \oplus \ldots \oplus R/\mathfrak{q}_m$. Hvis $\mathfrak{p}_i$ er maximalt, da er $\mathfrak{p}_i$ det eneste primideal, der indeholder $\mathfrak{q}_i$; i restklasseringen $R/\mathfrak{q}_i$ er der følgelig kun et primideal, nemlig $\mathfrak{p}_i/\mathfrak{q}_i$, så $R/\mathfrak{q}_i$ er en speciel P.I.R. Og hvis $\mathfrak{p}_i$ ikke er maximalt, da er $\mathfrak{p}_i \subset \mathfrak{M}$, $\mathfrak{q}_i \subseteq \mathfrak{p}_i \subset \mathfrak{M}$ men så $\mathfrak{q}_i \supseteq \mathfrak{p}_i$ iflg lemma 2), altså $\mathfrak{q}_i = \mathfrak{p}_i$, så $R/\mathfrak{q}_i = R/\mathfrak{p}_i$ er et integritetsområde, d: en P.I.D. ∎

Sætning. <u>Lad $\mathfrak{a}, \mathfrak{b}$ være idealer i et Noethersk integritetsområde, så at $\mathfrak{a}\mathfrak{b} = \mathfrak{b}$, da er $\mathfrak{a} = R$ eller $\mathfrak{b} = (0)$.</u>

Bevis. Hvis $\mathfrak{b} \neq (0)$, er $\mathfrak{b} = (b_1, \ldots, b_n)$, $b_i \neq 0$. Nu er $\mathfrak{b} = \mathfrak{a}\mathfrak{b} = \{\sum_{i=1}^{n} a^{(i)} b_i \mid a^{(i)} \in \mathfrak{a}\}$, så der findes $\underline{\underline{A}}$, så at $\underline{\underline{b}}_1 = \underline{\underline{A}}\underline{\underline{b}}_1$ eller

$$(\underline{\underline{A}} - \underline{\underline{E}})\underline{\underline{b}}_1 = \underline{\underline{0}}_1$$

Opfattes dette som en matrixligning med elementer fra kvotientlegemet for R, fås $0 = \det(\underline{\underline{E}} - \underline{\underline{A}}) = 1 - a$, hvor $a \in \mathfrak{a}$, altså $1 \in \mathfrak{a}$ og dermed $\mathfrak{a} = R$. ∎

Eks. I $R = \dot{Z}/6\dot{Z}$ (som har nuldivisorer) har vi $\mathfrak{a} = \mathfrak{b} = (2)$, men $\mathfrak{a}\mathfrak{b} = (4) = (-2) = (2) = \mathfrak{b}$.

Bemærk. Sætningen er også forkert, hvis R er et ikke-Noethersk integritetsområde.

Korollar. <u>Hvis R er et Noethersk integritetsområde, og $\mathfrak{a} \neq R$, da er $\bigcap_{n=1}^{\infty} \mathfrak{a}^n = (0)$.</u>

Bevis. Sæt $\mathfrak{b} = \bigcap \mathfrak{a}^n$, da er det nok at vise, at $\mathfrak{a}\mathfrak{b} = \mathfrak{b}$, og $\subseteq$ er trivielt. Følgelig er det tilstrækkeligt at vise, at ethvert primært ideal, der indeholder $\mathfrak{a}\mathfrak{b}$, også indeholder $\mathfrak{b}$. Lad altså $\mathfrak{q} \supseteq \mathfrak{a}\mathfrak{b}$ være primært og sæt $\mathfrak{p} = \operatorname{Rad}\mathfrak{q}$, da er $\mathfrak{q} \supseteq \mathfrak{b}$ eller $\mathfrak{p} \supseteq \mathfrak{a}$. Hvis vi kan vise, at $\mathfrak{q} \supseteq \mathfrak{p}^\nu$ for et vist ν, er vi færdige, thi af $\mathfrak{p} \supseteq \mathfrak{a}$ følger da $\mathfrak{q} \supseteq \mathfrak{p}^\nu \supseteq \mathfrak{a}^\nu \supseteq \bigcap_n \mathfrak{a}^n = \mathfrak{b}$, altså i alle tilfælde $\mathfrak{q} \supseteq \mathfrak{b}$. Beviset kan altså afsluttes med

Lemma. <u>Er $\mathfrak{r}$ et ideal i en Noethersk ring, R, da er $\mathfrak{r} \supseteq (\operatorname{Rad}\mathfrak{r})^\nu$ for et passende ν.</u>

Bevis. Sæt $\operatorname{Rad}\mathfrak{r} = (d_1, \ldots, d_n)$, da er $d_i \in \operatorname{Rad}\mathfrak{r}$, altså $d_i^{m_i} \in \mathfrak{r}$ for passende m_i. Sæt $\nu = m_1 + \ldots + m_n$, da er det let at vise, at $(\operatorname{Rad}\mathfrak{r})^\nu \subseteq \mathfrak{r}$. ∎

Eks. I $\dot{Z}/6\dot{Z}$ er $(2) = (2)^2 = \ldots$ altså $\bigcap_n (2)^n = (2)$.

Eks. Et ideal $\mathfrak{q}$ i en (vilk.) ring, R, kaldes <u>quasiprimært</u>, hvis $ab \in \mathfrak{q} \Rightarrow a \in \operatorname{Rad}\mathfrak{q} \vee b \in \operatorname{Rad}\mathfrak{q}$. $\mathfrak{q}$ er quasiprimært $\Leftrightarrow$ $\operatorname{Rad}\mathfrak{q}$ er primt ideal, thi "$\Leftarrow$" er oplagt, og

og hvis $\mathfrak{Q}$ er quasiprimært, og $xy \in \mathrm{Rad}\,\mathfrak{Q}$ og $x \notin \mathrm{Rad}\,\mathfrak{Q}$, er $x^n y^n \in \mathfrak{Q}$ og $x^n \notin \mathrm{Rad}\,\mathfrak{Q}$, så $y^n \in \mathrm{Rad}\,\mathfrak{Q}$ og dermed $y \in \mathrm{Rad}\,\mathfrak{Q}$. I et Noethersk integritetsområde gælder: Ethvert quasiprimært ideal er primært $\Leftrightarrow$ Ethvert ikke-trivielt primideal er maximalt. "$\Leftarrow$" er trivielt, "$\Rightarrow$": Hvis $(0) \subset \mathfrak{P} \subset \mathfrak{M} \subset R$, da er $\mathfrak{P}\mathfrak{M}$ quaisprimært, da $\mathrm{Rad}(\mathfrak{P}\mathfrak{M}) = \mathfrak{P} \cap \mathfrak{M} = \mathfrak{P}$ men ikke primært, thi da $\mathfrak{P}\mathfrak{M} \subset \mathfrak{P}$ (p.V,8), findes $a \in \mathfrak{P} \setminus \mathfrak{P}\mathfrak{M}$ og $b \in \mathfrak{M} \setminus \mathfrak{P}$; $ab \in \mathfrak{P}\mathfrak{M}$, $b \notin \mathrm{Rad}(\mathfrak{P}\mathfrak{M}) = \mathfrak{P}$ og $a \notin \mathfrak{P}\mathfrak{M}$.

Sætning. <u>Hvis R er Noethersk, da er enhver undermodul af en endelig frembragt R-modul, M, selv endeligt frembragt.</u>

Bevis. $M = Rm_1 + \ldots + Rm_\mu$. Induktion efter n: n = 1. Lad $N \subseteq M = Rm_1$ være en undermodul. $\mathfrak{A} = \{a \in R \mid am_1 \in N\}$ er et ideal i R, så $\mathfrak{A} = (a_1, \ldots, a_\nu)$, men så er for $n \in N$: $n = (r_1 a_1 + \ldots + r_\nu a_\nu)m_1 = r_1 a_1 m_1 + \ldots + r_\nu a_\nu m_1$, altså $N = Ra_1 m_1 + \ldots + Ra_\nu m_1$. Antag sætningen for n-1, og lad $N \subseteq M = Rm_1 + \ldots + Rm_\mu$ være en undermodul. $M_1 = Rm_1$ er undermodul i M, og $M_1 \cap N$ er undermodul i M_1, altså $M_1 \cap N = Ra_1 + \ldots + Ra_\nu$. Nu er $M/M_1 = R\,\overline{m_2} + \ldots + R\,\overline{m_\mu}$, og da $N/M_1 \cap N \cong M_1 + N/M_1 \subseteq M/M_1$, er $N/M_1 \cap N$ endelig frembragt iflg. induktionsforudsætningen, altså $N/M_1 \cap N = R\,\overline{b_1} + \ldots + R\,\overline{b_\mu}$. Nu er $N = Ra_1 + \ldots + Ra_\nu + Rb_1 + \ldots + Rb_\mu$, thi for $n \in N$ er $\overline{n} = r_1\,\overline{b_1} + \ldots + r_\mu\,\overline{b_\mu}$, og $n - r_1 b_1 - \ldots - r_\mu b_\mu \in M_1 \cap N$ er altså $= r'_1 a_1 + \ldots + r'_\nu a_\nu$, og dermed $n = r_1 b_1 + \ldots + r_\mu b_\mu + r'_1 a_1 + \ldots + r'_\nu a_\nu$. ∎

Sætning (I.S.Cohen). <u>Hvis alle primidealer i en ring R er endeligt frembragte, da er R Noethersk.</u>

Bevis. Antag, at der fandtes et ikke e.f. ideal, da var mængden $\mathfrak{F}$ af ikke endeligt frembragte idealer ikke tom. $\mathfrak{F}$ ses let at være induktivt ordnet. Lad $\mathfrak{A}$ være et maximalt element i $\mathfrak{F}$; $\mathfrak{A}$ er da ikke primideal, så der findes $\mathfrak{b} \supset \mathfrak{A}$, $\mathfrak{c} \supset \mathfrak{A}$ med $\mathfrak{A} \supseteq \mathfrak{b}\mathfrak{c}$, og her må $\mathfrak{b}, \mathfrak{c}$ være e.f. $\mathfrak{A}/\mathfrak{b}\mathfrak{c} \subseteq \mathfrak{b}/\mathfrak{b}\mathfrak{c}$ kan på natrulig måde betragtes som $R/\mathfrak{c}$ -modul, og da alle idealer mellem R og $\mathfrak{c}$ er e.f., er $R/\mathfrak{c}$ Noethersk. Da $\mathfrak{b}/\mathfrak{b}\mathfrak{c}$ er endeligt frembragt, er derfor også $\mathfrak{A}/\mathfrak{b}\mathfrak{c}$ en e.f. $R/\mathfrak{c}$ -modul, og dermed en endelig frembragt R-modul. Da $\mathfrak{b}\mathfrak{c}$ er e.f. følger det, at $\mathfrak{A}$ er e.f., modstrid.

I en vilkårlig ring er følgende betingelser ækvivalente:

1) d.d.c. (descending chain condition)
2) minimalbetingelsen gælder for idealer. Klart.

Sætning. <u>Hvis d.c.c. gælder i et int.omr. R, da er R et legeme.</u>

Bevis. Er $b \neq 0$, fås $(b) \supseteq (b^2) \supseteq \ldots$, altså $(b^n) = (b^{n+1}) = \ldots$ og dermed $b^n = cb^{n+1}$ eller $bc = 1$. ∎

Korollar. Hvis d.c.c. gælder i R, da er hvert ægte primideal maximalt.

Bevis. Hvis $\mathfrak{p}$ er et primideal i R, da er $R/\mathfrak{p}$ er integritetsområde hvori d.c.c. gælder, altså et legeme. ∎

Sætning. (Akisuki). d.c.c. $\Leftrightarrow$ a.c.c. og ethvert ægte primideal er maximalt.

Lemma 1. Hvis $(0) = \mathfrak{M}_1 \ldots \mathfrak{M}_n$ er produkt af maximale idealer, da er a.c.c. $\Leftrightarrow$ d.c.c..

Bevis. Vi har $(0) = \mathfrak{M}_1 \ldots \mathfrak{M}_n \subseteq \ldots \subseteq \mathfrak{M}_1\mathfrak{M}_2 \subseteq \mathfrak{M}_1 \subseteq R$ $(*)$. $\mathfrak{M}_1 \ldots \mathfrak{M}_{i-1}/\mathfrak{M}_1 \ldots \mathfrak{M}_i$ er på naturlig måde en modul over legemet $R/\mathfrak{M}_i$, altså et vektoruum, og dette er endeligt dimensionalt iflg. a.c.c. (d.c.c.) idet underrum svarer til idealer mellem $\mathfrak{M}_1 \ldots \mathfrak{M}_i$ og $\mathfrak{M}_1 \ldots \mathfrak{M}_{i-1}$. Heraf ses, at der findes endelig mange idealer, $\mathfrak{a}_1, \ldots, \mathfrak{a}_\nu$ mellem $\mathfrak{M}_1 \ldots \mathfrak{M}_i$ og $\mathfrak{M}_1 \ldots \mathfrak{M}_{i-1}$, så at $\mathfrak{M}_1 \ldots \mathfrak{M}_i \subset \mathfrak{a}_1 \subset \ldots \subset \mathfrak{a}_\nu \subset \mathfrak{M}_1 \ldots \mathfrak{M}_{i-1}$ ikke kan forfines. Anvendes dette for hvert i, ses, at $(*)$ kan forfines til en kompositionsrække. Iflg. Schreiers forfiningssætning må d.c.c.(a.c.c.) nu gælde. ∎

Bevis for Akizuki. "$\Leftarrow$" vises ved

Lemma 2. I en Noethersk ring indeholder ethvert ideal et produkt af primidealer.

Bevis. Lad $S = \{$idealer, der ikke indeholder et produkt af primidealer$\}$, og lad $\mathfrak{a}$ være et maximalt element i S, da er $\mathfrak{a}$ ikke primideal, så der findes $\mathfrak{b} \supset \mathfrak{a}$, $\mathfrak{c} \supset \mathfrak{a}$, med $\mathfrak{bc} \subseteq \mathfrak{a}$. Nu er $\mathfrak{b}, \mathfrak{c} \notin S$, så $\mathfrak{b} \supseteq \prod \mathfrak{p}_i$ og $\mathfrak{c} \supseteq \prod \mathfrak{p}_j'$, men så vil $\mathfrak{a} \supseteq \prod \mathfrak{p}_i\mathfrak{p}_j'$ ↯: $\mathfrak{a} \notin S$. Følgelig er $S = \emptyset$. ∎

"$\Rightarrow$": Vi har allerede bemærket, at hvis d.c.c. gælder, da er hvert ægte primideal maximalt. Beviset kan derfor afsluttes med

Lemma 3. Hvis d.c.c. gælder, da er $(0) = \mathfrak{p}_1 \ldots \mathfrak{p}_n$ produkt af primidealer.

Bevis. Da d.c.c. gælder findes et minimalt element $\mathfrak{o}$ i mængden af idealer, der er produkt af primidealer. Vi skal vise, at $\mathfrak{o} = (0)$. Indirekte: $\mathfrak{a} = (0):\mathfrak{o} \neq R$, da $1 \notin \mathfrak{a}$. Lad $\mathfrak{b}$ være et minimalt element i mængden af idealer, der ~~indeholder~~ $\supset \mathfrak{a}$, da er $\mathfrak{b} \supset \mathfrak{a}$, og der findes intet ideal mellem $\mathfrak{a}$ og $\mathfrak{b}$. $\mathfrak{a}:\mathfrak{b} \neq R$, da $1 \notin \mathfrak{a}:\mathfrak{b}$, og $\mathfrak{a}:\mathfrak{b}$ er et primideal, thi er $x,y \notin \mathfrak{a}:\mathfrak{b}$, er $x\mathfrak{b} \not\subseteq \mathfrak{a}$ og $y\mathfrak{b} \not\subseteq \mathfrak{a}$, så $\mathfrak{b} \supseteq \mathfrak{a} + x\mathfrak{b} \supset \mathfrak{a}$ og $\mathfrak{b} \supseteq \mathfrak{a} + y\mathfrak{b} \supseteq \mathfrak{a}$, hvoraf $\mathfrak{b} = \mathfrak{a} + x\mathfrak{b}$ og $\mathfrak{b} = \mathfrak{a} + y\mathfrak{b}$; nu er $\mathfrak{a} + xy\mathfrak{b} = (\mathfrak{a} + x\mathfrak{b})y + \mathfrak{a} = \mathfrak{b}y + \mathfrak{a} = \mathfrak{b}$, hvoraf $xy\mathfrak{b} \not\subseteq \mathfrak{a}$ ↯: $xy \notin \mathfrak{b}:\mathfrak{a}$.

Sæt $\mathfrak{y} = \mathfrak{a}:\mathfrak{c}$; $\mathfrak{y}\mathfrak{b} \subseteq \mathfrak{a} = (0):\mathfrak{v}$ og dermed $\mathfrak{y}\mathfrak{b}\mathfrak{v} = (0)$, eller $\mathfrak{b} \subseteq (0):(\mathfrak{y}\mathfrak{v})$. Af $\mathfrak{a} \subset \mathfrak{b}$ følger nu $\mathfrak{y}\mathfrak{v} \subset \mathfrak{v}$, hvilket er i modstrid med definitionen af $\mathfrak{v}$. ∎

Eks. Hvis d.c.c. gælder i R, da findes kun endelig mange primidealer, thi er $\mathfrak{M}_1, \mathfrak{M}_2, \ldots$ primidealer i R, da er $\mathfrak{M}_1 \supseteq \mathfrak{M}_1\mathfrak{M}_2 \supseteq \ldots \supseteq \mathfrak{M}_1 \ldots \mathfrak{M}_i \supseteq \ldots$, og altså $\mathfrak{M}_1 \cdots \mathfrak{M}_\nu = \mathfrak{M}_1 \ldots \mathfrak{M}_{\nu+1} \subseteq \mathfrak{M}_\nu$, hvoraf et $\mathfrak{M}_j \subseteq \mathfrak{M}_{\nu+1}$ og dermed $\mathfrak{M}_{\nu+1} = \mathfrak{M}_j$.

Sætning. <u>I $R/\mathfrak{a}$ gælder d.c.c. for $\mathfrak{a} \neq (0) \Leftrightarrow$ I R gælder a.c.c. og ethvert ikketrivielt primideal er maximalt</u>.
Bevis. "$\Leftarrow$" er trivielt. "$\Rightarrow$": Af $R/\mathfrak{a}$ a.c.c for $\mathfrak{a} \neq (0)$ følger R a.c.c. og af $R/\mathfrak{y}$ d.c.c. for et ikketrivielt primideal følger $R/\mathfrak{y}$ er et legeme, altså $\mathfrak{y}$ maximalt. ∎

Eks. For et integritetsområde R får vi: $R/\mathfrak{a}$ d.c.c. for $\mathfrak{a} \neq (0) \Leftrightarrow$ R er a.c.c. og ethvert quasiprimært ideal er primært. (Eks.V,8-9)

HELT AFSLUTTEDE RINGE

Lad R være integritetsområde, og $R \subseteq T$. $t \in T$ kaldes <u>helt afsluttet over R,</u> hvis t er rod i et normeret polynomium i $R[X]$.
($T \supseteq R$ er en R-modul. Hvis $S \subseteq T$ er en delmængde, betegnes med $R\{S\}$ den mindste R-modul $\subseteq T$, der indeholder (R og) S.)

Sætning. <u>$t \in T$ er hel over $R \Leftrightarrow R\{1,t,t^2,\ldots\}$ er endel.frembragt</u>.
Bevis. "$\Rightarrow$" $1,t,\ldots,t^{n-1}$ er da frembringere for ovennævnte modul.
"$\Leftarrow$". Hvis $R\{1,t,\ldots\}$ er frembragt af $\alpha_1,\ldots,\alpha_M \in T$, da vil $t\alpha_i \in R\{1,t,\ldots\}$, $i = 1,\ldots,M$, altså være R-lin.komb. af $\alpha_1,\ldots,\alpha_M$. Følgelig findes en $M \times M$-matrix $\underline{\underline{A}}$ med elementer fra R, så at $t\cdot\underline{\alpha}_| = \underline{\underline{A}}\,\underline{\alpha}_|$ eller $(t\cdot\underline{\underline{E}} - \underline{\underline{A}})\,\underline{\alpha}_| = \underline{0}_|$, men så er $0 = \det(t\underline{\underline{E}}-\underline{\underline{A}}) = t^M + r_{M-1}t^{M-1} + \ldots + r_0$. ∎

Eks. v.d.Waerden definerer: $t \in T$ hel over $R \Leftrightarrow R\{1,t,\ldots\}$ er $\subseteq$ endeligt frembragt R-modul. Hvis R er Noethersk gælder: <u>t "v.d.W. hel over R" $\Leftrightarrow$ t hel over R. (V,9)</u>

$\{t \in T \mid t$ er hel over $R\}$ kaldes R's <u>helt afsluttede hylster</u> i T, og betegnes $\bar{R}$. Det er klart, at $R \subseteq \bar{R}$.
Sætning. <u>$\bar{R}$ er en delring af T.</u>
Bevis. Lad $t,t' \in \bar{R}$, så $t'^{n'} + r'_{n'-1}t'^{n'-1} + \ldots + r'_0 = 0$ og $t^n + r_{n-1}t^{n-1} + \ldots + r_0 = 0$. Ethvert t^ν er R-lin.-komb. af $1,t,\ldots,t^{n-1}$ og ethvert

$t'^{\nu'}$ er R-lin.komb. af $1,t',\ldots,t'^{m'-1}$, så ethvert $t^{\nu}t'^{\nu'}$ er R-lin.-komb. af $t^{a}t'^{a'}$, $0 \leq a < n-1$, $0 \leq a' < n'-1$. Betegner $\underline{\underline{\alpha}}_1$ søjlen $(nn' \times 1)$ med disse elementer, findes en $(nn' \times nn')$-matrix $\underline{\underline{A}}$ med elementer fra R, så at $(t+t')\,\underline{\underline{\alpha}}_1 = \underline{\underline{A}}\,\underline{\underline{\alpha}}_1$, hvoraf $0 = \det((t+t')\underline{\underline{E}} - \underline{\underline{A}}) = (t+t')^{nn'} + \ldots$. Analogt med $t-t'$ og tt'. ∎

Hvis $\overline{\overline{R}} = T$, kaldes T hel over R.

Transitivitetssætning. Hvis $R \subseteq S \subseteq T$, $t \in T$ er hel over S og S er hel over R, da er t hel over R.

Bevis. Lad $t^{n}+s_1t^{n-1}+\ldots\pm s_n = 0$, og $s_i^{m_i} + r_{i,1}s_i^{m_i-1} + \ldots + r_{i,m_i} = 0$, $i = 1,\ldots,n$. Enhver potens $s_i^{\nu_i}$ er R-lin.-komb. af $1,s_i,\ldots,s_i^{m_i-1}$, så $s_1^{\nu_1}\ldots s_n^{\nu_n}$ er R-lin.komb. af $s_1^{a_1}\ldots s_n^{a_n}$, $0 \leq a_i < n_i-1$, men så er $t^{\nu}s_1^{\nu_1}\ldots s_n^{\nu_n}$ en R-lin.-komb. af $t^{a}s_1^{a_1}\ldots s_n^{a_n}$, $0 \leq a < n-1$ $0 \leq a_i < n_i-1$. ~~Følgelig findes en (nn$_1$...n$_n$ --- nn$_1$...n$_n$) matrix~~ $\underline{\underline{A}}$ Betegner $\underline{\underline{\alpha}}_1$ søjlen med disse $nn_1\ldots n_n$ elementer, findes altså en $(nn_1\ldots n_n \times nn_1\ldots n_n)$-matrix $\underline{\underline{A}}$ med elementer fra R, så at $t\underline{\underline{\alpha}}_1 = \underline{\underline{A}}\underline{\underline{\alpha}}_1$ hvoraf $0 = \det(t\underline{\underline{E}}-\underline{\underline{A}}) = t^{nn_1\cdots n_n} + \ldots$ ∴ t er hel over R. ∎

Korollar. $\overline{\overline{R}} = \overline{R}$.

Et int.omr. R kaldes helt afsluttet (i sit kvot.leg. $K = \frac{R}{R\setminus(0)}$) hvis $\overline{R} = R$ i K.

Sætning. Et U.F.D. er helt afsluttet.

Bevis. Lad $\frac{a}{b} \in K$, $(a,b) = 1$, være hel over R, fx $(\frac{a}{b})^{n}+r_1(\frac{a}{b})^{n-1}+\ldots+r_n = 0$, da er $a^{n} = b(-r_1a^{n-1} - \ldots - r_nb^{n-1})$, altså $b \mid a^{n}$ hvoraf $b \mid a$ ∴ $\frac{a}{b} \in R$.

Eks. $R = \mathbb{Z}[\sqrt{-3}]$ $K = \mathbb{Q}(\sqrt{-3})$. ikke helt afsluttet; for $\rho = -\frac{1}{2}-\frac{1}{2}\sqrt{-3} \notin R$ har vi $\rho^3 - 1 = 0$

Eks. $R = \{f(X) \in L[X] \mid f'(0) = 0\}$. Kvotlegemet er $K = L(X)$. Nu er $X \notin R$, men $X \in K$ og X er rod i polynomiet $Z^2-X^2 \in R[Z]$.

I en kommutativ ring R med 1-element er følgende bet.ækv.:

1) Ikke-enhederne udgør et ideal
2) R har netop ét maximalt ideal, klart!

og en sådan ring kaldes lokal.

Eks. $R = K[[X]]$ er en lokal ring med maximalideal (X)

Eks. Lad R være et int.omr. og $\varphi \subsetneq R$ et primideal. $S = R\setminus\varphi$ er et multiplikativt system. Sættes $R_\varphi = \frac{R}{S}$, da er R_φ lokal med det maximale ideal φR_φ.

Eks. Eks. Et int.omr. R kaldes en valuationsring, hvis $a,b \in R \Rightarrow a \mid b$ eller $b \mid a$. En valutaionsring er lokal, thi a,b ikke-enheder, er fx, $b = ra$, så $a+b = (1+r)a$ er ikke-enhed. Et endeligt frembragt ideal i en væluationsring er et hovedideal, thi er $\mathcal{O} = (a_1, a_2)$ og fx $a_1 \mid a_2$ er $\mathcal{O} = (a_1, ra_1) = (a_1)$. Altså: En Noethersk valuationsring er et P.I.D. (kaldet en diskret val.ring.). I et P.I.D. er primidealerne maximale, så der findes kun ét primelement, p, $\mathcal{M} = (p)$, så $R \supset \mathcal{M} \supseteq \mathcal{M}^2 \supseteq \ldots \supseteq (0)$ er samtlige idealer.

Sætning. Lad R være et int.omr. og lad Ω betegne (spektret) mg. af maximalidealer i R, da er $\bigcap_{\mathcal{M} \in \Omega} R_{\mathcal{M}} = R$.

Bevis. "$\supseteq$" er oplagt. "$\subseteq$": $R_{\mathcal{M}}$ er en lokal ring med det maximale ideal $\mathcal{M}R_{\mathcal{M}}$. Lad nu $\frac{x}{y} \in \bigcap_{\mathcal{M}} R_{\mathcal{M}}$, $x,y \in R$. Det er nok at vise, at $(y):(x) = R$, thi da er $x = ry$ d: $\frac{x}{y} = r \in R$. Indirekte: $(y):(X) \subseteq \mathcal{M} \subset R$. Nu er $\frac{x}{y} \in R_{\mathcal{M}}$ d.v.s. $\frac{x}{y} = \frac{r}{s}$, hvor $s \notin \mathcal{M}$, og dermed $xs = ry \in (y)$, hvoraf $s \in (y):(x)$, modstrid. ∎

Korollar. Hvis R er et int.omr., da er R helt afsluttet $\Leftrightarrow$ $R_{\mathcal{M}}$ er helt afsluttet for alle $\mathcal{M} \in \Omega$.

Bevis. "$\Rightarrow$". Vi viser, at $\frac{R}{S}$ er helt afsluttet for ethvert multiplikativt system $S \subseteq R \setminus (0)$. Kvot.legemet for $\frac{R}{S}$ er R's kvot.legm. Lad $(\frac{x}{y})^n + \frac{r_1}{s_1}(\frac{x}{y})^{n-1} + \ldots + \frac{r_n}{s_n} = 0$. Vi kan antage, at $s_1 = \ldots = s_n = s$, men så er $(\frac{sx}{y})^n + r_1(\frac{sx}{y})^{n-1} + \ldots + s^{n-1}r_n = 0$,
og da R er helt afsluttet er $\frac{sx}{y} \in R$ d: $\frac{x}{y} = \frac{r}{s} \in \frac{R}{S}$.

"$\Leftarrow$" Hvis $\frac{x}{y} \in K$ er hel over R, da er $\frac{x}{y}$ hel over $R_{\mathcal{M}}$, , og dermed $\frac{x}{y} \in R_{\mathcal{M}}$, hvoraf $\frac{x}{y} \in \bigcap_{\mathcal{M}} R_{\mathcal{M}} = R$. ∎

Sætning. Er $\mathcal{O}$ et ideal i et int.omr. R, da er $\bigcap_{\mathcal{M} \in \Omega} (\mathcal{O}R_{\mathcal{M}} \cap R) = \mathcal{O}$.

Bevis. "$\supseteq$" er trivielt. "$\subseteq$": Lad $r \in \bigcap \mathcal{O} \cdot R_{\mathcal{M}} \cap R$. Det er nok at vise, at $\mathcal{O}:(r) = R$, og var $\mathcal{O}:(r) \subseteq \mathcal{M} \subset R$, ville $r \in \mathcal{O}R_{\mathcal{M}}$, $r = \frac{a}{s}$, hvor $s \notin \mathcal{M}$, og $rs = a \in \mathcal{O}$, så $s \in \mathcal{O}:(r)$, modstrid. ∎

Sætning. Et helt afsluttet, lokalt, Noethersk int.omr. hvori ethvert ikke-trivielt primideal er maximalt, er et P.I.D. [en diskret valuationsring.].

Bevis. Ifølge forudsætningerne findes netop ét ikketrivielt primideal φ i R, og ethvert ikketrivielt primideal i R må være φ-primært. Vælg et $\alpha \in \varphi \setminus (0)$, da er $(\alpha):\varphi \supseteq (\alpha)$. Her må ⊃

gælde, thi ellers var $(\alpha) = (\alpha):\mathfrak{p} = (\alpha):\mathfrak{p}^2 = \ldots$; da R er Noethersk, og (α) er $\mathfrak{p}$-primært, vil $(\alpha) \supseteq \mathfrak{p}^n$ for et vist n, men af ovenstående ville da følge, $(\alpha) = R$.
Nu vælges $\beta \in (\alpha):\mathfrak{p} \setminus (\alpha)$. For $\frac{\beta}{\alpha}$ i kvot.leg. er $\frac{\beta}{\alpha}\mathfrak{p}$ et ideal i R, da $\beta\mathfrak{p} \subseteq (\alpha)$. Det påstås, at $\frac{\beta}{\alpha}\mathfrak{p} = R$. Indirekte, da vær $\frac{\beta}{\alpha}\mathfrak{p} \subsetneq \mathfrak{p} \subset$ $\subset R$, og dermed $(\frac{\beta}{\alpha})^2\mathfrak{p} \subseteq \mathfrak{p}$, $(\frac{\beta}{\alpha})^3\mathfrak{p} \subseteq \mathfrak{p}$ o.s.v. Specielt er $(\frac{\beta}{\alpha})^n\mathfrak{p} \subseteq$ R. Vælges $p \in \mathfrak{p} \setminus (0)$, da er $(\frac{\beta}{\alpha})^n p \in R$, så $(\frac{\beta}{\alpha})^n \in R\{\frac{1}{p}\}$ og dermed $R\{1, \frac{\beta}{\alpha}, (\frac{\beta}{\alpha})^2, \ldots\} \subseteq R\{\frac{1}{p}\}$. Da denne sidste R-modul er endelig frembragt, er $\frac{\beta}{\alpha}$ v.d.W. hel, og da R er Noethersk $\frac{\beta}{\alpha}$ dermed hel over R, altså $\frac{\beta}{\alpha} \in R$, men så er $\beta \in (\alpha)$ i modstrid med valget af β.
Da $\frac{\beta}{\alpha}\mathfrak{p} = R$, findes $\pi \in \mathfrak{p}$, så at $\frac{\beta}{\alpha}\pi = 1$. For $p \in \mathfrak{p}$, er $\frac{\beta}{\alpha}p = r \in R$, og dermed $p = r\pi$, så vi slutter, at $\mathfrak{p} = (\pi)$.
Et vilkårligt $\mathfrak{a} \neq (0), \neq R$ er $\mathfrak{p}$-primært. Lad $\mathfrak{p}^\rho$ være den højeste potens, så $\mathfrak{p}^\rho \supseteq \mathfrak{a}$. (En så dan findes øjensynlig.) Altså $\mathfrak{p}^{\rho+1}$ $\not\supseteq \mathfrak{a}$. Da er $\mathfrak{a} \subseteq (\pi^\rho), \mathfrak{a} \not\subseteq (\pi^{\rho+1})$, så der findes $a \in \mathfrak{a}$, $a \notin (\pi^{\rho+1})$, men $a = r\pi^\rho$, hvor altså $r \notin (\pi)$, og dermed r enhed. Følgelig er $\pi^\rho = r^{-1}a \in \mathfrak{a}$;: altså $\mathfrak{a} = (\pi^\rho)$. ∎

Lemma. <u>Lad R være et integritetsområde, og $S \subseteq R$ (0) et multiplikativt system, da gælder 1) $(\mathfrak{a} \cap \mathfrak{b})\frac{R}{S} = \mathfrak{a}\frac{R}{S} \cap \mathfrak{b}\frac{R}{S}$ 2) $(\mathfrak{a}\mathfrak{b})\frac{R}{S}$ $= (\mathfrak{a}\frac{R}{S})(\mathfrak{b}\frac{R}{S})$ og 3) Hvis $\tilde{\mathfrak{p}} \supset \tilde{\mathfrak{p}}'$ er primidealer i $\frac{R}{S}$, da er $\tilde{\mathfrak{p}} \cap R \supset \tilde{\mathfrak{p}}' \cap R$ primidealer i R</u>æ
Bevis for 3). $\tilde{\mathfrak{p}} \cap R$ er klart et primideal i R, og vælges $\frac{r}{s} \in \tilde{\mathfrak{p}} \setminus \tilde{\mathfrak{p}}'$, er $r \in \tilde{\mathfrak{p}}$ og $r \in \tilde{\mathfrak{p}}'$, da elementerne i S er enheder i $\frac{R}{S}$. Altså er $r \in$ $(\tilde{\mathfrak{p}} \cap R) \setminus (\tilde{\mathfrak{p}}' \cap R)$. ∎

Sætning. <u>Lad R være et integritetsområde så at</u>
1) <u>R er Noethersk</u>
2) <u>Ethvert ikke-trivielt primideal er maximalt.</u>
3) <u>R er helt afsluttet,</u>
<u>da kan ethvert ideal $\mathfrak{a} \neq (0)$ på entydig måde skrives som produkt af primidealer,</u>
og R kaldes da en <u>Dedekindring</u>.
Bevis. Lad $\mathfrak{p} \neq (0)$ være et primideal, da er $R_\mathfrak{p}$ <u>lokal</u> (V,12,eks) <u>Noethersk</u> (ses let), <u>helt afsluttet</u> (V,13) og ethvert fra (0) forskelligt primideal i R er maximalt (V,14). Heraf følger, at $R_\mathfrak{p}$ er en P.I.D. med idealerne $(\mathfrak{p}R_\mathfrak{p})^n$. Det følger nu, at hvis $\hat{\mathfrak{q}}$ er $\hat{\mathfrak{p}}$ -primær, da er

$$\mathfrak{q}R_\mathfrak{p} = \begin{cases} R_\mathfrak{p} & \text{for } \mathfrak{p} \neq \hat{\mathfrak{p}} . \\ (\mathfrak{p}R_\mathfrak{p})^m & \text{for } \mathfrak{p} = \hat{\mathfrak{p}} . \end{cases}$$

Eksistens. Lad $\mathfrak{a} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n$ være uforkortelig, da er $\mathfrak{a}R_\mathfrak{p} =$ $\mathfrak{q}_1R_\mathfrak{p} \cap \ldots \cap \mathfrak{q}_nR_\mathfrak{p}$, og dermed

$$\mathfrak{a}R_{\mathfrak{p}} = \begin{cases} R_{\mathfrak{p}} & \text{for } \mathfrak{p} \neq \mathfrak{p}_i\ ,\ i = 1,\dots,n \\ (\mathfrak{p}_i R_{\mathfrak{p}_i})^{\nu_i} & \text{for } \mathfrak{p} = \mathfrak{p}_i \end{cases}$$

Sættes $\mathfrak{b} = \mathfrak{p}_1^{\nu_1} \dots \mathfrak{p}_m^{\nu_m}$, da er $\mathfrak{b}R_{\mathfrak{p}} = (\mathfrak{p}_1^{\nu_1} R_{\mathfrak{p}}) \dots (\mathfrak{p}_m^{\nu_m} R_{\mathfrak{p}})$, og altså

$$\mathfrak{b}R_{\mathfrak{p}} = \begin{cases} R_{\mathfrak{p}} & \text{for } \mathfrak{p} \neq \mathfrak{p}_i\ ,\ i = 1,\dots,n \\ (\mathfrak{p}_i R_{\mathfrak{p}_i})^{\nu_i} & \text{for } \mathfrak{p} = \mathfrak{p}_i\ . \end{cases}$$

Altså er $\mathfrak{a}R_{\mathfrak{p}} = \mathfrak{b}R_{\mathfrak{p}}$ for alle $\mathfrak{p}$, altså for alle maximale idealer, og dermed $\mathfrak{a} = \mathfrak{b} = \mathfrak{p}_1^{\nu_1} \dots \mathfrak{p}_m^{\nu_m}$.

Entydighed. Hvis $\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \dots \mathfrak{p}_m^{\nu_m}$, er $\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \cap \dots \cap \mathfrak{p}_m^{\nu_m}$ (jfr. V, 6-7), og denne fremstilling er normal, da $\mathfrak{p}_i$'erne er forskellige ($\mathfrak{p}_i^{\nu_i}$ er $\mathfrak{p}_i$-primært, da Rad $\mathfrak{p}_i^{\nu_i} = \mathfrak{p}_i$ er maximalt). Komponenterne $\mathfrak{p}_i^{\nu_i}$ er entydigt bestemt, da de er minimalkomponenter, og da $\mathfrak{p} \supset \mathfrak{p}^2 \supset \dots \supsetneqq (0)$ er også ν_i entydigt bestemt.

Eks.

KAPITEL VI ANVENDELSER PÅ ALGEBRAISK GEOMETRI.

INDSKUD OM TRANSCENDENSUDVIDELSER=

Lad $K \subseteq L$ være legemer. Et sæt $\gamma_1,\ldots,\gamma_n \in L$ kaldes algebraisk uafhængige over K, hvis det for alle $f \in K[X_1,\ldots,X_n]$ gælder, at $f(\gamma_1,\ldots,\gamma_n) = 0$ medfører at $f = 0$, altså hvis homomorfien $f(X_1,\ldots,X_n) \longrightarrow f(\gamma_1,\ldots,\gamma_n)$ af $K[X_1,\ldots,X_n] \to L$ er injektiv. Da billedet ved denne afbildning altid er $K[\gamma_1,\ldots,\gamma_n]$ har vi altså: Hvis $\gamma_1,\ldots,\gamma_n$ er alg.uafh. over K, er $K[\gamma_1,\ldots,\gamma_n] \cong K[X_1,\ldots,X_n]$ og dermed også $K(\gamma_1,\ldots,\gamma_n) \cong K(X_1,\ldots,X_n)$.
$\gamma_1,\ldots,\gamma_n \in L$ kaldes en transcendensbasis for L over K, hvis 1) $\gamma_1,\ldots,\gamma_n$ er alg.uafh. over K og 2) $L/K(\gamma_1,\ldots,\gamma_n)$ er algebraisk.

Eks. $X_1,\ldots,X_n$ er en tr.basis for $K(X_1,\ldots,X_n)$ over K.

Sætning. Hvis $(\gamma_1,\ldots,\gamma_n)$ er en tr.basis for L/K, da er vilkårlige r+1 elementer, $\alpha_1,\ldots,\alpha_{n+1} \in L$ altid algebraisk afhængige.

Bevis. Induktion efter r: $r = 0$, da er L/K algebraisk, og alt er trivielt. Antag sætningen for alle $r' < r$. α_1 er algebraisk over $K(\gamma_1,\ldots,\gamma_n)$; sæt $f(X) = \mathrm{Irr}(\alpha_1, K(\gamma_1,\ldots,\gamma_n))$, da er

$$f(X) = X^n + \frac{g_1(\gamma_1,\ldots,\gamma_n)}{h_1(\gamma_1,\ldots,\gamma_n)} X^{n-1} + \ldots + \frac{g_n(\gamma_1,\ldots,\gamma_n)}{h_n(\gamma_1,\ldots,\gamma_n)},$$

hvor vi, da $K[\gamma_1,\ldots,\gamma_n] \cong K[X_1,\ldots,X_n]$ er et U.F.D., kan antage, at g_i/h_i er uforkortelig. Hvis intet γ_i optræder i f(X), er $f(X) \in K[X]$, så α_1 er algebraisk over K, og dermed $\alpha_1,\ldots,\alpha_{n+1}$ alg.afh. Antag fx nu, at γ_1 effektivt optræder. Multipliceres f(X) med mindste fælles multiplum af $h_1,\ldots,h_n$ får vi

$$(*) \quad G_0(\gamma_1,\ldots,\gamma_n)X^n + G_1(\gamma_1,\ldots,\gamma_n)X^{n-1} + \ldots + G_n(\gamma_1,\ldots,\gamma_n)$$

Ethvert andet pol. i $K[\gamma_1,\ldots,\gamma_n][X]$ med α_1 som rod, er enten af grad $\geq n+1$, eller fås ud fra (*) ved multiplikation med et element i $K[\gamma_1,\ldots,\gamma_n]$. Omordnes (*) efter potenser af γ_1 får vi

$$(**) \quad F_0(X)\gamma_1^N + F_1(X)\gamma_1^{N-1} + \ldots + F_N(X)$$

hvor $F_i(X) \in K[\gamma_2,\ldots,\gamma_n][X]$. Nu er α_1 rod i (**), og da grad $F_0(X) \leq n$, og da F_0 ikke er multiplum af (*), er $F_0(\alpha_1) \neq 0$, og (**) viser nu, at γ_1 er algebraisk over $K(\alpha_1,\gamma_2,\ldots,\gamma_n)$, og altså $K(\gamma_1,\ldots,\gamma_n)/K(\alpha_1,\gamma_2,\ldots,\gamma_n)$ algebraisk. Da også $L/K(\gamma_1,\ldots,\gamma_n)$ er algebraisk, slutter vi, at $L/K(\alpha_1,\gamma_2,\ldots,\gamma_n)$ er algebraisk.
Vi vælger nu et maximalt system af algebraisk uafhængige blandt $\gamma_2,\ldots,\gamma_n$ over $K(\alpha_1)$, fx. $\gamma_2,\ldots,\gamma_s$ $(s \leq r)$. Af maximaliteten følger let, at L er algebraisk over $K(\alpha_1)(\gamma_2,\ldots,\gamma_s) = K(\alpha_1,\gamma_2,\ldots,\gamma_s)$ d.v.s. $(\gamma_2,\ldots,\gamma_s)$ er tr.basis for L over $K(\alpha_1)$. Iflg induktionsantagelsen er $\alpha_2,\ldots,\alpha_{n+1}$ algebraisk afhængige over $K(\alpha_1)$, hvor-

af det let følger, at $\alpha_1, \alpha_2, \ldots, \alpha_{n+1}$ er algebraisk afhængige over K. ∎

Korollar. Hvis L/K har en endelig tr.basis, da er alle tr.baser endelige og med samme elementantal.

Dette elementantal kaldes L's transcendensgrad over K og betegnes trgr.L/K eller $\mathrm{trgr}_K L$.

Korollar. Hvis trgr.L/K = $t < \infty$, og $\alpha_1, \ldots, \alpha_t \in L$ er alg.uafh. over K, da er $\alpha_1, \ldots, \alpha_t$ en transcendensbasis for L/K.

Sætning. Antag at $K \subseteq M \subseteq L$, at $(\beta_1, \ldots \beta_s)$ er en tr.basis for L/M og at $(\alpha_1, \ldots, \alpha_n)$ er en tr.basis for M/K, da er $(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_s)$ en tr.basis for L/K.
Specielt er trgrL/K = trgr.L/M + trgr.M/K.
Bevis. 1) $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_s$ er algebraisk uafh. over K, thi hvis $\sum a_{\ldots,\ldots} \alpha_1^{\nu_1} \ldots \alpha_n^{\nu_n} \beta_1^{\mu_1} \ldots \beta_s^{\mu_s} = 0$, da er $\sum_{\nu} a_{\ldots,\ldots} \alpha_1^{\nu_1} \ldots \alpha_n^{\nu_n} \in M$, og altså = 0, da $\beta_1, \ldots, \beta_s$ er alg.uafh. over M, men heraf følger $a_{\ldots,\ldots} = 0$, da $\alpha_1, \ldots, \alpha_n$ er alg. uafh. over K.
2) $L/K(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_s)$ er algebraisk, thi $L/M(\beta_1, \ldots, \beta_s)$ er algebraisk, og $M/K(\alpha_1, \ldots, \alpha_n)$ er algebraisk, og dermed også $M(\beta_1, \ldots, \beta_s)/K(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_s)$ algebraisk. ∎

$L \supseteq K$ kaldes endeligt frembragt over K, hvis der findes $\alpha_1, \ldots, \alpha_m \in L$, så at $L = K(\alpha_1, \ldots, \alpha_m)$.

Sætning. Hvis $L = K(\alpha_1, \ldots, \alpha_m)$ er e.f. over K, da er trgr.L/K $\leq n$, og der findes en tr.basis for L/K med elementer blandt $\alpha_1, \ldots, \alpha_m$.
Bevis. Hvis alle α'er er alg. over K, er trgrL/K = 0, intet at bevise.
Antag fx at α_1 er transcendent over K. Hvis alle $\alpha_2, \ldots, \alpha_m$ er alg. over $K(\alpha_1)$, er $L/K(\alpha_1)$ alg., så α_1 er tr.basis for L/K. I modsat fald kan vi antage, at fx α_1, α_2 er alg. uafh. over K. Hvis alle $\alpha_3, \ldots, \alpha_m$ er alg. over $K(\alpha_1, \alpha_2)$, er $L/K(\alpha_1, \alpha_2)$ alg., så (α_1, α_2) er tr.basis for L/K. I modsat fald .... ∎

Et int.omr. $R \supseteq K$ kaldes endeligt frembragt over K, hvis der findes $\alpha_1, \ldots, \alpha_n \in R$, så at $R = K[\alpha_1, \ldots, \alpha_m]$. Hvis L er R's kvot. legeme, sættes trgr.R/K = trgr.L/K. Da $L = K(\alpha_1, \ldots, \alpha_m)$ er e.f., bliver trgr.R/K altså $\leq n$, og der findes en tr.basis blandt $\alpha_1, \ldots, \alpha_m$.

Til et endeligt frambragt int.omr. $R = K[\alpha_1, \ldots, \alpha_m]$ over K findes øjensynlig en surjektiv K-homomorfi $\varphi: K[X_1, \ldots, X_m] \to R$. Da

$K[X_1,\ldots,X_n]/\mathrm{Ker}\,\varphi \cong R$ er et int.omr. er $\mathrm{Ker}\,\varphi$ et primideal i $K[X_1,\ldots,X_n]$.

Sætning. Lad R,R' være e.f. int.omr. over K. Hvis $\varphi: R \to R'$ er en surjektiv K-homomorfi, da er trgr.R'/K $\leq$ trgrR/K.

Bevis. Lad $\alpha_1',\ldots,\alpha_t'$ være en tr.basis for R'/K, og vælg $\alpha_1,\ldots,\alpha_t \in R$ så at $\varphi(\alpha_i) = \alpha_i'$, i = 1,...,t, da ses det let, at $\alpha_1,\ldots,\alpha_t$ er alg. uafh. over K.

Tilføjelse. Hvis trgr.R'/K = trgr.R/K, da er φ en isomorfi.

Bevis. Vi skal vise, at $\mathrm{Ker}\,\varphi = 0$. Vælges $\alpha_1',\ldots,\alpha_t'$ og $\alpha_1,\ldots,\alpha_t$ som før, kan vi af trgr.R/K = t slutte, at $\alpha_1,\ldots,\alpha_t$ er en tr.-basis for R/K. Lad nu $u \in R\setminus(0)$. u er da rod i et egentligt pol. med koeff. i $K[\alpha_1,\ldots,\alpha_t]$:

$$(*)\quad F_g(\alpha_1,\ldots,\alpha_t)u^g+\ldots+F_0(\alpha_1,\ldots,\alpha_t) = 0,$$

hvor vi kan antage, at $F_0(\alpha_1,\ldots,\alpha_t) \neq 0$, og dermed $F_0(X_1,\ldots,X_n) \neq 0$. Anvendes φ på (*) fås

$$F_g(\alpha_1',\ldots,\alpha_t')\varphi(u)^n+\ldots+F_0(\alpha_1',\ldots,\alpha_t') = 0,$$

og da $F_0(\alpha_1',\ldots,\alpha_t') \neq 0$, må $\varphi(u) \neq 0$. ∎

Et int.omr. R siges at have Krulldimmensionen d, hvis der findes d primidealer, så

$$R \supset \mathfrak{p}_1 \supset \ldots \supset \mathfrak{p}_d \supset (0),$$

og hvis ingen primidealkæder med ikktrivielle primidealer indeholder mere end d primidealer.

Sætning. $R = K[X_1,\ldots,X_n]$ har Krulldim. n.

Bevis. Vi har $R \supset (X_1,\ldots,X_n) \supset \ldots \supset (X_1,X_2) \supset (X_1) \supset (0)$. Lad $\mathfrak{p}$ være et vilkårligt primideal (ikketrivielt), og betragt den kannoniske homomorfi $\varkappa : R \to R/\mathfrak{p}$. $\varkappa|_K$ er injektiv, thi er $k \neq 0$, og $\varkappa(k) = 0$, er $k \in \mathfrak{p}$ og dermed $\frac{1}{k}\cdot k = 1 \in \mathfrak{p}$ i modstrid med at $\mathfrak{p} \subset R$. Vi kan følgelig identificere $\varkappa(K)$ med K. Nu er $R/\mathfrak{p} = \varkappa(R) = \varkappa(K)[\varkappa(X_1),\ldots,\varkappa(X_n)] = K[\alpha_1,\ldots,\alpha_n]$. Lad nu $R \supset \mathfrak{p}_1 \supset \ldots \supset \mathfrak{p}_d \supset (0)$. Da $\varkappa : R \to R/\mathfrak{p}_d$ ikke er injektiv, er $n = \mathrm{trgr}_K R > \mathrm{trgr}_K R/\mathfrak{p}_d$. Da $\varkappa_1 : R/\mathfrak{p}_d \to R/\mathfrak{p}_{d-1}$ ikke er injektiv (kernen er jo $\mathrm{Ker}\,\varkappa_1 = \mathfrak{p}_{d-1}/\mathfrak{p}_d$) er $\mathrm{trgr}_K R/\mathfrak{p}_d > \mathrm{trgr}_K R/\mathfrak{p}_{d-1}$ o.s.v. Følgelig er $d \leq n$. ∎

Eks. Enhver primidealpotens i $K[X,Y]$ er primær. Lad nemlig $\mathfrak{p}$ være et ikketrivielt primideal i $R = K[X,Y]$. Vælges $a \in \mathfrak{p}$, $a \neq 0$ er da ikke enhed d: $a = \pi_1 \ldots \pi_n \in \mathfrak{p}$, hvoraf fx $\pi_1 \in \mathfrak{p}$ og dermed $(\pi_1) \subseteq \mathfrak{p}$. Nu er (π_1) et primideal, og $(0) \subset (\pi_1) \subseteq \mathfrak{p} \subset R$. Hvis $\mathfrak{p} = (\pi_1)$, er $\mathfrak{p}^n = (\pi_1)^n$ primært, og hvis $\mathfrak{p} \supset (\pi_1)$, er $\mathfrak{p}$ iflg. sætnin-

gen maximalt, og dermed $\mathfrak{q}^n$ primært.

Noethers Normaliseringslemma. Lad $R = K[\alpha_1,\ldots,\alpha_m]$, hvor legemet K har uendelig mange elementer. Sættes $d = \mathrm{trgr}R/K \leq m$, da findes $y_1,\ldots,y_d \in R$, K-lin.komb. af $\alpha_1,\ldots,\alpha_m$, så at R er hel over $K[y_1,\ldots,y_d]$. Specielt er $y_1,\ldots,y_d$ en transcendensbasis for R/K.

Induktionsbevis. $n = 1$: Enten er α_1 alg over K, så at $R = K[\alpha_1]$ er alg. over K og dermed hel over K, specielt er trgr.R/K = 0. Eller α_1 er transcendent over K, men så er $R = K[\alpha_1]$ hel over $K[\alpha_1]$, specielt er trgr. R/K = 1.

Antag sætningen for n, og lad $R = K[\alpha_1,\ldots,\alpha_{m+1}]$. Enten er $d = n+1$, så at R er hel over $K[\alpha_1,\ldots,\alpha_{m+1}]$. Eller $d \leq n$, og da findes en tr.basis for R/K, fx. blandt $\alpha_1,\ldots,\alpha_m$. Nu er α_{m+1} alg. over $K(\alpha_1,\ldots,\alpha_m)$, altså rod i et polynomium ded koeff. i $K[\alpha_1,\ldots,\alpha_m]$. Der findes altså et pol. $0 \neq F(T,X_1,\ldots,X_m) \in K[T,X_1,\ldots,X_m]$, så at α_{m+1} er rod i $F(T,\alpha_1,\ldots,\alpha_m)$. Sæt $z_i = \alpha_i - a_i\alpha_{m+1}$, $i = 1,\ldots,n$, hvor $a_i \in K$; vi søger da at bestemme a_i så at R er hel over $K[z_1,\ldots,z_m]$.

Vi ved, at $0 = F(\alpha_{m+1},\alpha_1,\ldots,\alpha_m) = F(\alpha_{m+1},z_1+a_1\alpha_{m+1},\ldots,z_m+a_m\alpha_{m+1})$. Ordnes $F(T,X_1,\ldots,X_m)$ efter faldende grader, har vi

$$F(T,X_1,\ldots,X_m) = f_q(T,X_1,\ldots,X_m)+\ldots+f_0(T,X_1,\ldots,X_m),$$

hvor $f_j(T,X_1,\ldots,X_m)$ er homogen af grad j, og hvor vi kan antage, at $f_q \neq 0$. Højestegradskoefficienten til α_{m+1} i $F(\alpha_{m+1},z_1+a_1\alpha_{m+1},\ldots,z_m+a_m\alpha_{m+1})$ er nu $f_q(1,a_1,\ldots,a_m) \in K$, og da K har uendelig mange elementer kan vi vælge $a_i \in K$, så at $f_q(1,a_1,\ldots,a_m) \neq 0$. α_{m+1} er nu rod i et polynomium dem koeff. i $K[z_1,\ldots,z_m]$, hvor højestegradskoef. $= f_q(1,a_1,\ldots,a_m) \in K\setminus(0)$, og derfor også rod i et normeret pol. i $K[z_1,\ldots,z_m]$ ɔ: α_{m+1} er hel over $K[z_1,\ldots,z_m]$. Da $\alpha_1 = z_1+a_1\alpha_{m+1}$, $\ldots$, $\alpha_m = z_m+a_m\alpha_{m+1}$ også er hele over $K[z_1,\ldots,z_m]$ må $R = K[\alpha_1,\ldots,\alpha_m,\alpha_{m+1}]$ være hel over $K[z_1,\ldots,z_m]$.

Iflg. induktionsantagelsen findes $y_1,\ldots,y_d$, K-lin.komb. af $z_1,\ldots,z_m$, så at $K[z_1,\ldots,z_m]$ er hel over $K[y_1,\ldots,y_d]$. Af transitiviteten følger endelig, at $R = K[\alpha_1,\ldots,\alpha_{m+1}]$ er hel over $K[y_1,\ldots,y_d]$, og $y_1,\ldots,y_d$ er K-lin.komb. af $\alpha_1,\ldots,\alpha_{m+1}$. ∎

"lying-over"sætningen. Lad R,R' være int.omr. med R' hel over R. Hvis $\mathfrak{p} \subseteq R$ er primideal, da findes $\mathfrak{p}' \subseteq R'$ primideal, så at $R \cap \mathfrak{p}' = \mathfrak{p}$.

Bevis. Antag $\mathfrak{p} \subset R$, og sæt $\mathfrak{P} = \{\mathfrak{o}' \subsetneq R' \mid \mathfrak{o}' \cap R \subseteq \mathfrak{p}\}$, da er $\mathfrak{P} \neq \emptyset$, da $(0) \in \mathfrak{P}$. $\mathfrak{P}$ er induktivt ordnet ved $\subseteq$, så iflg. Zorn's lemma har $\mathfrak{P}$ et maximalt element $\mathfrak{p}'$.

*) $\exists z \in R : z \in (\mathfrak{q}' + R'x) \setminus \mathfrak{q}'$

Først vises, $R \cap \mathfrak{q}' = \mathfrak{q}$. Indirekte: da findes $x \in \mathfrak{q} \setminus (R \cap \mathfrak{q}')$, så $x \notin \mathfrak{q}'$. Nu er $\mathfrak{q}' + R'x \supset \mathfrak{q}'$, altså $R \cap (\mathfrak{q}' + R'x) \not\subseteq \mathfrak{q}$. *) Vi har $z = p' + r'x$ eller $z \equiv r'x \pmod{\mathfrak{q}'}$. Da R' er hel over R, er $r'^m + a_1 r'^{m-1} + \ldots + a_m = 0$, hvor $a_i \in R$, og dermed $(r'x)^m + a_1 x (r'x)^{m-1} + \ldots + a_0 x^m = 0$, hvoraf $z^m + a_1 x z^{m-1} + \ldots + a_0 x^m \equiv 0 \pmod{\mathfrak{q}'}$, altså $\in \mathfrak{q}'$, men også $\in R$, d: $\in \mathfrak{q}' \cap R \subseteq \mathfrak{q}$. Da $x \in \mathfrak{q}$ fås $z^m \in \mathfrak{q}$ og dermed $z \in \mathfrak{q}$.

Dernæst vises, at $\mathfrak{q}'$ er et primideali R'. Indirekte, da fandes $\mathfrak{a}' \supset \mathfrak{q}'$, $\mathfrak{b}' \supset \mathfrak{q}'$ med $\mathfrak{a}'\mathfrak{b}' \subseteq \mathfrak{q}'$. Nuer $\mathfrak{a}' \cap R \supseteq \mathfrak{q} \cap R = \mathfrak{q}$, men $\supset$ gælder iflg, maximaliteten af $\mathfrak{q}'$. Analogt ses, at $\mathfrak{b}' \cap R \supset \mathfrak{q}$. Imidlertid er $(\mathfrak{a}' \cap R)(\mathfrak{b}' \cap R) \subseteq \mathfrak{a}'\mathfrak{b}' \cap R \subseteq \mathfrak{q}' \cap R = \mathfrak{q}$ i modstrid med at $\mathfrak{q}$ er primideal. ∎

Mere triviel er Lying-under sætningen

"Lying-under"sætningen. <u>Lad $R \subseteq R'$ være int.omr. med R' hel over R. Hvis $\mathfrak{q}' \subsetneq R'$ er et primideal $\neq (0)$, da er $\mathfrak{q} = R \cap \mathfrak{q}'$ et primideal $\neq (0)$.</u>

Bevis. $\mathfrak{q} = R \cap \mathfrak{q}'$ er et primideal. Vælg nu $p' \in \mathfrak{q}' \setminus (0)$. Vi har $p'^m + a_1 p'^{m-1} + \ldots + a_m = 0$, hvor $a_i \in R$, og hvor vi kan antage, at $a_m \neq 0$, men $a_m = -p'^m - a_1 p'^{m-1} - \ldots - a_{m-1} p' \in \mathfrak{q}' \cap R$ og $\neq (0)$. ∎

Eks. $R = \hat{Z}$, $R' = \hat{Z}[X]$, $\mathfrak{q}' = (X) \neq (0)$, men $\mathfrak{q}' \cap R = (0)$.

Hilberts nulpunktssætning (Hns_1). <u>Lad R være et e.f. int.omr. over K, da er R algebraisk over $K \iff R$ er et legeme.</u>

Bevis. "$\Rightarrow$" er trivielt.

<u>Første bevis</u> for "$\Leftarrow$": 1) Antag først, at K har uendelig mange elementer. Indirekte: Vi antager, at trgr.$R/K \geq 1$, og viser, at R har et ikketrivielt primideal. Iflg. Noethers norm.lemma findes $y_1, \ldots, y_d \in R$, så at R er hel over $\hat{R} = K[y_1, \ldots, y_d] \cong K[X_1, \ldots, X_d]$. $\hat{R}$ har et ikke-trivielt primideal, fx $\hat{\mathfrak{q}} = (y_1, \ldots, y_d)$, og iflg. lying-oversætn. findes et primideal $\mathfrak{q} \subsetneq R$, så at $\hat{R} \cap \mathfrak{q} = \hat{\mathfrak{q}}$, men så er $\mathfrak{q}$ et ikketrivielt primideal i R.

2) Antag dernæst, at K er et endeligt legeme. Lad $R = K[x_1, \ldots, x_m]$ og antag, at trgr.$R/K \geq 1$. Lad L være R's kvot.legeme og lad $\tilde{L}$ være et algebraisk afsluttet hylster af L. K's algebraiske hylster $\tilde{K}$, i $\tilde{L}$ er da et algebraisk afsluttet hylster af K, og har derfor uendelig mange elementer (ses let!). Nu sættes $\tilde{R} = \tilde{K}[x_1, \ldots, x_m]$, da har vi

$$\begin{array}{ccccc} \tilde{K} & \subseteq & \tilde{R} = \tilde{K}[x_1, \ldots, x_m] & \subseteq & \tilde{L} \\ \cup\!| & & \cup\!| & & \cup\!| \\ K & \subseteq & R = K[x_1, \ldots, x_m] & \subseteq & L, \end{array}$$

og trgr.$\tilde{R}/\tilde{K} \geq 1$, thi ellers var $x_1, \ldots, x_m$ algebraiske over $\tilde{K}$ d: $\in \tilde{K}$

o: algebraiske over K. Endvidere er $\tilde{R}$ hel over R, thi $\alpha_1,\ldots,\alpha_m \in R$, og $\tilde{K}$ er alg. over K og dermed hel over K.
Iflg. 1) findes $\tilde{\mathfrak{P}} \subsetneq \tilde{R}$ ikketrivielt primideal, men så er $\mathfrak{P} = \tilde{\mathfrak{P}} \cap R$ et ikketrivielt primideal i R iflg "lying7under"sæt. (og idet vi bemærker, at $\tilde{\mathfrak{P}} \cap R \subset R$, da ellers $1 \in \tilde{\mathfrak{P}}$) ∎

Andet bevis for "⇐":(Zariski) Antag $R = K[\alpha_1,\ldots,\alpha_m]$ er et legeme; vi skal vise, at α_j'erne er algebraiske over K. Induktion efter n. n = 1: Hvis α_1 vær transcendent ville $R = K[\alpha_1] \cong K[X]$ ikke være et legeme. Antag nu sætningen for n-1, og lad $R = K[\alpha_1,\ldots,\alpha_m]$ være et legeme. Antag fx at α_1 er transcendent. Nu er α_1 R, og da R er et legeme, er $K(\alpha_1) \subsetneq R = K[\alpha_1,\ldots,\alpha_m]$ altså $R = K(\alpha_1)[\alpha_2,\ldots,\alpha_m]$. Iflg. induktionsforudsætningen er $R/K(\alpha_1)$ da algebraisk, vså $\alpha_2,\ldots,\alpha_m$ er rødder i egtl. pol. $\in K(\alpha_1)[X_2,\ldots,X_m]$ og dermed også rødder i egtl.pol.$\in K[\alpha_1][X_1,\ldots,X_n]$; fx.

$$f_0^{(2)}(\alpha_1)\alpha_2^{\nu} + f_1^{(2)}(\alpha_1)\alpha_2^{\nu-1} + \ldots + f_\nu^{(2)}(\alpha_1) = 0,$$

hvor $f_0^{(2)}(\alpha_1) \neq 0$. Multiplicerer vi denne relation med $f_0^{(2)}(\alpha_1)^{\nu-1}$ følger det, at $f_0^{(2)}(\alpha_1)\alpha_2$ er hel over $K[\alpha_1]$.
Analogt findes $f_0^{(k)}(\alpha_1) \neq 0$, k = 3,...,n, så at $f_0^{(k)}(\alpha_1)\alpha_k$ er hel over $K[\alpha_1]$. Sættes endelig $f = f_0^{(2)}\ldots f_0^{(n)} \in K[\alpha_1]$, $f \neq 0$, da er $f(\alpha_1)\alpha_k$ hel over $K[\alpha_1]$, k = 2,3,...,n, og dette gælder trivielt for k = 1.
Det følger nu, at der til hvert element $\alpha \in R = K[\alpha_1,\ldots,\alpha_m]$ findes et ρ så at $f(\alpha_1)^\rho\alpha$ er hel over $K[\alpha_1]$.
Er $h(\alpha_1) \in K[\alpha_1]$, da er $\frac{1}{h(\alpha_1)} \in K(\alpha_1) \subsetneq R$, så der findes ρ så at $f(\alpha_1)^\rho \frac{1}{h(\alpha_1)}$ er hel over $K[\alpha_1]$, og da $K[\alpha_1] \cong K[X]$ er helt afsluttet i sit kvot.legeme $K(\alpha_1)$, viser dette, at $f(\alpha_1)^\rho \frac{1}{h(\alpha_1)} \in K[\alpha_1]$ o: $h(\alpha_1) \mid f(\alpha_1)^\rho$.
Specielt må ethvert irreducibelt element i $K[\alpha_1]$ gå op i $f(\alpha_1)$, og dette er en modstrid, da $K[\alpha_1] \cong K[X]$ øjensynlig indeholder uendelig mange irreducible polynomier (jfr. Euklid) ∎

ALGEBRAISK GEOMETRI

Lad K være et vilkårligt legeme. Produktrummet K^m kaldes det affine rum over K og betegnes $\mathcal{A}_m(K)$. En delmængde $V \subseteq \mathcal{A}_m(K)$ kaldes en algebraisk varietet (eller mangfoldighed), hvis der findes endelig mange $f_1,\ldots,f_k \in K[X_1,\ldots,X_m]$ så at V er mængden af fælles nulpunkter for $f_1,\ldots,f_m$. V er da også mgd. af fælles nulpunkter for $(f_1,\ldots,f_m)$. Er $\mathfrak{o}$ et ideal i $K[X_1,\ldots,X_m]$, da sættes $\mathcal{V}(\mathfrak{o}) = \{\underline{\alpha} \in \mathcal{A}_m(K) \mid \forall f \in \mathfrak{o} : f(\underline{\alpha}) = 0\}$. Da $K[X_1,\ldots,X_m]$ er Noethersk, er mængderne $\mathcal{V}(\mathfrak{o})$ netop de algebraiske varieteter i $\mathcal{A}_m(K)$.

Er $E \subseteq \mathcal{A}_n(K)$ en vilkårlig delmængde, sættes $\mathcal{F}(E) = \{f \in K[\underline{X}] \mid \forall \underline{\alpha} \in E : f(\underline{\alpha}) = 0\}$. $\mathcal{F}(E)$ er et ideal i R.

Der gælder:

$\mathfrak{a} \subseteq \mathfrak{b} \Rightarrow \mathcal{V}(\mathfrak{a}) \supseteq \mathcal{V}(\mathfrak{b})$

$E \subseteq F \Rightarrow \mathcal{F}(E) \supseteq \mathcal{F}(F)$

$\mathcal{V}(\sum_I \mathfrak{a}_i) = \bigcap_I \mathcal{V}(\mathfrak{a}_i)$

$\mathcal{F}(\bigcup_I E_i) = \bigcap_I \mathcal{F}(E_i)$

$\mathcal{V}(\mathfrak{a}\mathfrak{b}) = \mathcal{V}(\mathfrak{a} \cap \mathfrak{b}) = \mathcal{V}(\mathfrak{a}) \cup \mathcal{V}(\mathfrak{b})$

$\mathcal{F}(\mathcal{V}(\mathfrak{a})) \supseteq \mathfrak{a}$; $\mathcal{V}(\mathcal{F}(E)) \supseteq E$.

Eks. For $\mathfrak{a} = (X^2)$, er $\mathcal{F}(\mathcal{V}(\mathfrak{a})) = (X) \supset \mathfrak{a}$.

Sætning. <u>V er algebraisk varietet</u> $\Leftrightarrow V = \mathcal{V}(\mathcal{F}(V))$.

Bevis. "$\Leftarrow$" er oplagt. "$\Rightarrow$": Er V en alg. varietet, er $V = \mathcal{V}(\mathfrak{a})$, hvoraf $\mathcal{F}(V) = \mathcal{F}(\mathcal{V}(\mathfrak{a})) \supseteq \mathfrak{a}$, og dermed $\mathcal{V}(\mathcal{F}(V)) \subseteq \mathcal{V}(\mathfrak{a}) = V$. ∎

Vi har

Idealer i $K[\underline{X}]$		Varieteter i $\mathcal{A}_n(K)$.
$\mathfrak{a}$	$\longrightarrow$	$\mathcal{V}(\mathfrak{a})$
$\mathcal{F}(V)$	$\longleftarrow$	V

hvoraf den første afbildning er surjektiv iflg. def, men normalt ikke injektiv, og den anden afb. er injektiv iflg. sætn. men normalt ikke surjektiv.

Korollar. <u>De algebraiske varieteter opfylder minimumsbetingelsen</u>.

Eks. Af relationerne følger, at fællesmængde af varieteter, iog foreningsmængde af endelig mange varieteter igen er varieteter; ved som system af afsluttede mængder i $\mathcal{A}_n(K)$ at tage varieteterne defineres den såkaldete Zariski-topologi i $\mathcal{A}_n(K)$. (Normalt ikke Hausdorff). Men <u>quasi-kompakt</u>, da maximumsbetingelsen må gælde for de åbne mængder. Det ses, at vi i kenne topologi har $\overline{E} = \mathcal{V}(\mathcal{F}(E))$, thi dette er klart den mindste varietet, der indeholder E.

V kaldes en <u>irreducibel</u> varietet, hvis $V = V_1 \cup V_2 \Rightarrow V = V_1$ eller $V = V_2$.

Sætning. <u>V er irreducibel</u> $\Leftrightarrow \mathcal{F}(V)$ er primideal.

Bevis. "$\Leftarrow$". Hvis $V = V_1 \cup V_2$, da er $\mathcal{F}(V) = \mathcal{F}(V_1) \cap \mathcal{F}(V_2)$, og da $\mathcal{F}(V)$ er primideal, er fx $\mathcal{F}(V_1) \subseteq \mathcal{F}(V)$, og dermed $V = \mathcal{V}\mathcal{F}(V) \subseteq \mathcal{V}\mathcal{F}(V_1) = V_1$, altså $V = V_1$.

"$\Rightarrow$". Antag $\mathcal{F}(V)$ ikke er primideal, da findes $f,g \notin \mathcal{F}(V)$, så $fg \in$

$\mathcal{I}(V)$. Nu er $\mathcal{V}(f, \mathcal{F}(V)) \subset V$ og $\mathcal{V}(g, \mathcal{F}(V)) \subset V$, men $\mathcal{V}(f, \mathcal{F}(V)) \cup \mathcal{V}(g, \mathcal{F}(V)) = V$, thi $\subseteq$ er oplagt, og er $\underline{\alpha} \in V$, $\underline{\alpha} \notin \mathcal{V}(f, \mathcal{F}(V))$, er $f(\underline{\alpha}) \neq 0$, men da $fg \in \mathcal{F}(V)$, er $f(\underline{\alpha})g(\underline{\alpha}) = fg(\underline{\alpha}) = 0$, hvoraf $g(\underline{\alpha}) = 0$ $\supset$: $\underline{\alpha} \in \mathcal{V}(g, \mathcal{F}(V))$.

Sætning. Enhver varietet er foreningsmængde af endelig mange irreducible, $V = \bigcup_i V_i$, og hvis fremstillingen er uforkortelig, ($\supset$: intet V_i er overflødigt), da er den entydig.

Bevis. Eksistens. Lad S være mængden af varieteter, der ikke er foreningsmgd. af irred., og lad V^* være et minimalt element i S, da er V^* reducibel, så $V^* = V_1 \cup V_2$, hvor $V_1 \subset V^*$, $V_2 \subset V^*$. Nu er $V_1, V_1 \notin S$; de er altså foreningsmgd. af irreducible, men så er V^* det også. Modstrid, altså $S = \emptyset$

Entydighed. Lad $V = \bigcup_i V_i = \bigcup_j V_j'$ være uforkortelige. Nu er $V_i = V_i \cap V = V_i \cap \bigcup_j V_j' = \bigcup_j (V_i \cap V')$, og da V_i er irreducibel, må fx $V_i = V_i \cap V_j'$, altså $V_i \subseteq$ et V'. Analogt ses, at $V_j' \subseteq V_{i_1}$, men af $V_i \subseteq V_j' \subseteq V_{i_1}$ fås $V_i = V_j'$ $(= V_{i_1})$ o.s.v. ∎

Lad V være en irreducibel varietet, da er $\mathcal{F}(V)$ et primideal i $R = K[X_1, \ldots, X_n]$ så $R/\mathcal{F}(V)$ er et integritetsområde, kaldet V's koordinatring.

For $V \neq \emptyset$ er $\mathcal{F}(V) \neq R$, og $\varkappa$: R på $R/\mathcal{F}(V)$ afbilder K isomorft på $\varkappa(K)$, altså $R/\mathcal{F}(V) = \varkappa(R) = \varkappa(K)[\varkappa(X_1), \ldots, \varkappa(X_n)] \cong K[\alpha_1, \ldots, \alpha_n]$, så koordinatringen $R/\mathcal{F}(V)$ er et endeligt frembragt int.omr. over K.

Eks. For en irreducibel "kurve" V gælder: V er singularitetsfri $\Leftrightarrow$ $R/\mathcal{F}(V)$ er helt afsluttet. (u. bevis) Fx er $V = \mathcal{V}(X^2 - Y^3)$; $\mathcal{F}(V) = (X^2 - Y^3)$ primideal. $R/\mathcal{F}(V) = K[X,Y]/(X^2 - Y^3) = K[\bar{X}, \bar{Y}]$ er ikke helt afsl. thi $\bar{X}^2 - \bar{Y}^3 = 0$, så $\left(\frac{\bar{X}}{\bar{Y}}\right)^2 - \bar{Y} = 0$, og hvis $\frac{\bar{X}}{\bar{Y}} \in K[\bar{X}, \bar{Y}]$ måtte $\bar{X} = \bar{r} \cdot \bar{Y}$ $\supset$: $X = Yr(X,Y) + (X^2 - Y^3)h(X,Y)$, men dette går galt for $Y = 0$.

For en irreducibel varietet V defineres dimmensionen af V som $\dim V = \mathrm{trgr}_K(R/\mathcal{F}(V))$, og for en vilkårlig værietet V med $V = \bigcup V_i$, uforkortelig, sættes $\dim V = \max_i \{V_i\}$. Er $\dim V = 1$, kaldes V en kurve.

For $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathcal{A}_n(K)$ sættes $\mathcal{M}_{\underline{\alpha}} = (X_1 - \alpha_1, \ldots, X_n - \alpha_n)$. Da $R/\mathcal{M}_{\underline{\alpha}} \cong K$ er $\mathcal{M}_{\underline{\alpha}}$ maximalt, og det er kalrt, at $\mathcal{F}(\{\underline{\alpha}\}) = \mathcal{M}_{\underline{\alpha}}$.

Eks. Lad $V \neq \emptyset$ være en irreducibel varietet, og lad $\underline{\alpha} \in V$, da er $\mathcal{F}(\{\underline{\alpha}\}) \supseteq \mathcal{F}(V)$, og $\mathcal{M}_{\underline{\alpha}}/\mathcal{F}(V)$ er et maximalt ideal i $R/\mathcal{F}(V)$. Kvotientringen $(R/\mathcal{F}(V))_{\mathcal{M}_{\underline{\alpha}}/\mathcal{F}(V)}$ er en lokal ring, kaldet <u>den geometriske lokale ring for V i $\underline{\alpha}$</u>. Man kan vise: Den geom.lok.ring i $\underline{\alpha}$ for en kurve er et P.I.D. ($\supset$: en diskret val.ring) $\Leftrightarrow$ V har ingen singularitet i $\underline{\alpha}$.

Hilberts nulpunktssætning (Hns_2). <u>Hvis K er algebraisk afsluttet, da er ethvert maximalt ideal $\mathcal{M}$ i $R = K[X_1,\ldots,X_n]$ af formen $\mathcal{M}_{\underline{\alpha}} = (X_1-\alpha_1,\ldots,X_n-\alpha_n)$.</u>

Bevis. Lad $\mathcal{M} \subset R$, og lad $R \xrightarrow{\pi} R/\mathcal{M} = \pi(R) = \pi(K)[\pi(X_1),\ldots,\pi(X_n)] = \pi(K)[\beta_1,\ldots,\beta_n]$ være den kan. homomorfi. $\pi(R) = R/\mathcal{M}$ er et e.f. int.omr. over $\pi(K) \cong K$, og - da $\mathcal{M}$ er maximalt - tillige et legeme. Iflg. Hns_1 er $\pi(R)$ algebraisk over $\pi(K)$ $\supset$: $\beta_1,\ldots,\beta_n$ er alg. over $\pi(K)$. Da K og dermed $\pi(K)$ er algebraisk afsluttet, er $\beta_1,\ldots,\beta_n \in \pi(K)$ $\supset$: $\pi(X_i) = \beta_i = \pi(\alpha_i)$, $\alpha_i \in K$, i = 1,...,n. Altså er $X_i - \alpha_i \in \operatorname{Ker}\pi = \mathcal{M}$, og dermed $\mathcal{M} \supseteq (X_1-\alpha_1,\ldots,X_n-\alpha_n) = \mathcal{M}_{\underline{\alpha}}$, hvoraf $\mathcal{M} = \mathcal{M}_{\underline{\alpha}}$. ∎

Korollar. <u>Hvis K er alg.afsl., da er $\mathcal{V}(\mathcal{O}) = \emptyset \Leftrightarrow \mathcal{O} = R = K[X_1,\ldots,X_n]$.</u>

Bevis. "$\Leftarrow$" er trivielt. "$\Rightarrow$" Hvis $\mathcal{O} \subset R$, er $\mathcal{O} \subseteq \mathcal{M} = \mathcal{M}_{\underline{\alpha}} \subset R$, så $\mathcal{V}(\mathcal{O}) \supseteq \mathcal{V}(\mathcal{M}) = \mathcal{V}(X_1-\alpha_1,\ldots,X_n-\alpha_n) = \{\underline{\alpha}\} \supset \emptyset$. ∎

Eks. $\underline{\alpha} \longrightarrow \mathcal{M}_{\underline{\alpha}}$ er altså surjektiv på mgd. Ω af maximalidealer. $(R/\mathcal{F}(V))_{\mathcal{M}_{\underline{\alpha}}/\mathcal{F}(V)}$ er derfor samtlige lokale komponenter af $R/\mathcal{F}(V)$.

Hilberts nulpunktssætning.(Hns_3). <u>Hvis K er algebraisk afsluttet, og $\mathcal{O} \subsetneq R = K[X_1,\ldots,X_n]$, da er $\mathcal{F}(\mathcal{V}(\mathcal{O})) = \operatorname{Rad}\mathcal{O}$.</u>

Bevis. 1) Vi har vist specialtilfældet, hvor $\mathcal{V}(\mathcal{O}) = \emptyset$.

2) "$\supseteq$" er trivielt, thi er $f \in \operatorname{Rad}\mathcal{O}$, er $f^\rho \in \mathcal{O}$, så f^ρ forsvinder på $\mathcal{V}(\mathcal{O})$, så at også f forsvinder på $\mathcal{V}(\mathcal{O})$, $\supset$: $f \in \mathcal{F}(\mathcal{V}(\mathcal{O}))$.

3) Bevis for "$\subseteq$". Vi har $\mathcal{O} = (f_1,\ldots,f_q)$, og antag at $f \in \mathcal{F}\mathcal{V}(\mathcal{O})\setminus(0)$ d.v.s. at f forsninder på de fælles nulpkt. for $f_1,\ldots,f_q$.

Rabinovic's trick: Sæt $\hat{R} = K[X_1,\ldots,X_n,T]$ og $\hat{\mathcal{O}} = (f_1,\ldots,f_q,1-Tf)$, da er $\mathcal{V}(\hat{\mathcal{O}}) = \emptyset \subseteq \mathbb{A}_{n+1}(K)$, og dermed $\hat{\mathcal{O}} = \hat{R}$. Specielt er

$$1 = \sum_1^q f_i(X_1,\ldots,X_n)g_i(X_1,\ldots,X_n,T) + [1-Tf(X_1,..,X_n)]g(X_1,\ldots,X_n,T).$$

Dette kan opfattes som en relation i $K(X_1,\ldots,X_n)[T]$, og sættes $T = \frac{1}{f(X_1,\ldots,X_n)} \in K(X_1,\ldots,X_n)$ fås

$$1 = \sum_1^q f_i(X_1,\ldots,X_n)g_i(X_1,\ldots,X_n,\frac{1}{f(X_1,\ldots,X_n)}).$$

Ved multiplikation med f^ρ for passende ρ fås

$$f^\rho = \sum_1^q f_j g_j^* \in \mathfrak{a},$$

o: $f \in \operatorname{Rad}\mathfrak{a}$. ∎

Korollar. Hvis K er alg.afsl., da er $\mathcal{V}(\mathfrak{a})$ irreducibel $\Leftrightarrow$ $\mathfrak{a}$ er quasiprimært.

Korollar. Hvis K er alg.afsl., da er $\mathcal{V}(\mathfrak{a}) = \mathcal{V}(\mathfrak{b}) \Leftrightarrow \operatorname{Rad}\mathfrak{a} = \operatorname{Rad}\mathfrak{b}$.

Korollar. Hvis K er alg.afsl., da findes en 1-1 forb. mellem varieteterne i $\mathcal{A}_n(K)$ og de idealer i $R = K[X_1,\ldots,X_n]$, der er gennemsnit af primidealer.

Bevis. Hvis $\mathfrak{a} = \mathcal{F}(V)$, da er $\operatorname{Rad}\mathfrak{a} = \mathcal{F}\mathcal{V}(\mathfrak{a}) = \mathcal{F}\mathcal{V}\mathcal{F}(V) = \mathcal{F}(V) = \mathfrak{a}$. Da R er Noethersk, er $\mathfrak{a} = \mathfrak{q}_1 \cap \ldots \mathfrak{q}_n$, og $\operatorname{Rad}\mathfrak{a} = \mathfrak{p}_1 \cap \ldots \mathfrak{p}_n$, og altså $\mathfrak{a} = \operatorname{Rad}\mathfrak{a} = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_n$, og er omvendt $\mathfrak{a} = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_n$, er $\mathfrak{a} = \operatorname{Rad}\mathfrak{a} = \mathcal{F}\mathcal{V}(\mathfrak{a})$. ∎

kommut.1-elem.

Eks. Vi har for en vilk.ring R vist, at $\operatorname{Rad}\mathfrak{a} = \bigcap_{\mathfrak{p}\supseteq\mathfrak{a}} \mathfrak{p}$. Nu defineres Jaxobson's radical som $\operatorname{Jac}\mathfrak{a} = \bigcap_{\mathfrak{m}\supseteq\mathfrak{a}} \mathfrak{m}$; det er kalrt, at $\operatorname{Rad}\mathfrak{a} \subseteq \operatorname{Jac}\mathfrak{a}$. Nu gælder: Hvis $\mathfrak{a} \subseteq K[X_1,\ldots,X_n]$, K alg.afsl., da er $\operatorname{Rad}\mathfrak{a} = \operatorname{Jac}\mathfrak{a}$. eller ensb.hermed: Hvis $R = K[\alpha_1,\ldots,\alpha_n]$ er endelig frembragt over K, alg.afsl., da er $\operatorname{Rad}(0) = \operatorname{Jac}(0)$. Bevis. $\operatorname{Rad}(0) = \bigcap \mathfrak{p}$, $\operatorname{Jac}(0) = \bigcap \mathfrak{m}$. Det er nok at vise, athvert $\mathfrak{p}$ er gennemsnit af maximale idealer: $\mathfrak{p} = \bigcap_{\mathfrak{m}\supseteq\mathfrak{p}} \mathfrak{m}$. Lad $\mathfrak{p} \subset R$, da er $\mathcal{V}(\mathfrak{p}) \neq \emptyset$, og skriver vi $\mathcal{V}(\mathfrak{p}) = \bigcup_j V_j$, hvor V_j gennemløber pkt. i $\mathcal{V}(\mathfrak{p})$ får vi $\mathfrak{p} = \operatorname{Rad}\mathfrak{p} = \mathcal{F}\mathcal{V}(\mathfrak{p}) = \mathcal{F}(\bigcup_j V_j) = \bigcap_j \mathcal{F}(V_j)$ = gennemsnit af maximalidealer.

Eks. I $R = K[[X]]$, har vi $\operatorname{Rad}(0) = (0)$, da RR er int. omr. og $\operatorname{Jac}(0) = (X)$, da RR er lokal med (X) som max,id

"Going-up"sætningen. Lad $R \subseteq R'$ være int.omr. med R' hel over R, lad $\mathfrak{p}'$ være primideal i R' og sæt $\mathfrak{p} = \mathfrak{p}' \cap R$, da vil $\mathfrak{p}$ minimalt $\Rightarrow$ $\mathfrak{p}'$ minimalt.

Bevis. Indirekte, da findes primideal $\mathfrak{q}'$ i R', så $(0) \subset \mathfrak{q}' \subset \mathfrak{p}' \subset R'$. Nu er $\mathfrak{q}' \cap R \neq (0)$ iflg. lying-under, og da $\mathfrak{q}' \cap R \subseteq \mathfrak{p}$, må $\mathfrak{q}' \cap R = \mathfrak{p}$. Lad $p' \in \mathfrak{p}' \setminus \mathfrak{q}'$, da har vi $p'^n + r_1 p'^{n-1} + \ldots + r_n = 0$. Her kan ikkealle r_j'erne $\in \mathfrak{p}$, da vi i så fald havde $p'^n \in \mathfrak{q}'$. Antag $r_\nu \notin \mathfrak{p}$, $r_{\nu+1},\ldots,r_n \in \mathfrak{p}$, da er $p'^{n-\nu}(p'^\nu + r_1 p'^{\nu-1} + \ldots + r_\nu) = -r_{\nu+1} p'^{n-\nu-1}$

$-\ldots-r_m \in \varphi R' \subseteq \mathfrak{q}'$. Da $p'^{m-\nu} \notin \mathfrak{q}'$, må $p'^{\nu}+r_1 p'^{\nu-1}+\ldots+r_\nu \in \mathfrak{q}' \subseteq \varphi'$, og dermed $r_\nu \in \varphi'$, altså $r_\nu \in \varphi' \cap R = \varphi$, modstrid. ∎

"Going-down"sætningen. <u>Lad $R \subseteq R'$ være int.omr. med R' hel over R, hvor R antages helt afsluttet i sit kvot.legeme K, lad φ' være primideal i R' og sæt $\varphi = \varphi' \cap R$, da vil φ' minimalt $\Rightarrow$ minimalt.</u>

Vi viser det ensbetydende:

Under de samme forudsætninger som i Going-down gælder: <u>Hvis $(0) \subset \mathfrak{q} \subset \varphi \subset R$, da findes et primideal $\mathfrak{q}' \subseteq \varphi'$, så at $\mathfrak{q}' \cap R = \mathfrak{q}$.</u>

Bevis. Mængden $S = \{ab' \mid a \in R \setminus \mathfrak{q} \wedge b' \in R' \setminus \varphi'\}$ er et multiplikativt system i R', så vi kan danne $\frac{R'}{S} = \left\{\frac{r'}{s} \mid r' \in R' \wedge s \in S\right\}$. Det er nok at vise, at $\mathfrak{q}\frac{R'}{S} \neq \frac{R'}{S}$, thi da er $\mathfrak{q}\frac{R'}{S} \subseteq \mathfrak{M} \subset \frac{R'}{S}$; da elementerne i S er enheder i $\frac{R'}{S}$ har vi $\mathfrak{M} \cap S = \emptyset$ og dermed $(\mathfrak{M} \cap R') \cap S = \emptyset$; sættes $\mathfrak{q}' = \mathfrak{M} \cap R'$ primideal i R' er altså $\mathfrak{q}' \cap S = \emptyset$, hvoraf $\mathfrak{q}' \subseteq \varphi'$. Endvidere er $\mathfrak{q}' \cap R = \mathfrak{q}$, thi da $(\mathfrak{q}' \cap R) \cap S = \emptyset$, er $\mathfrak{q}' \cap R \subseteq \mathfrak{q}$, og på den anden side er $\mathfrak{q} = \mathfrak{q} \cap R \subseteq \mathfrak{M} \cap R = \mathfrak{M} \cap (R' \cap R) = \mathfrak{q}' \cap R$.

Vi skal nu vise, at $\mathfrak{q}\frac{R'}{S} \neq \frac{R'}{S}$. Vi har $\mathfrak{q}\frac{R'}{S} = (\mathfrak{q}R')\frac{R'}{S}$, og skal altså vise, at $\mathfrak{q}R' \cap S = \emptyset$. Indirekte, da findes $s \in S$, så $s = q_1 r_1' + \ldots + q_m r_m'$. Da R' hel over R, er r_i' rod i et pol. $X^{n_i} + \ldots \in R[X]$, og vi ser, at ethvert potensprodukt, $r_1'^{\nu_1} \ldots r_m'^{\nu_m}$ er R-lin.komb. af $r_1'^{a_1} \ldots r_m'^{a_m}$, $0 \leq a_i < n_i$. Betegner $\underline{\alpha}_1$ søjlen med disse elementer, findes en matrix $\underline{A}$ med elementer <u>fra $\mathfrak{q}$</u>, så at $s\,\underline{\alpha}_1 = \underline{A}\,\underline{\alpha}_1$, og dermed $0 = \det(s\underline{E}-\underline{A})$; s er følgelig rod i $f(X) = \det(X\underline{E}-\underline{A}) = X^n + q_1 X^{n-1} + \ldots + q_n \in R[X]$, $q_i \in \mathfrak{q}$. Sættes $g(X) = \mathrm{Irr}(s,K)$ har vi $f(X) = g(X)h(X)$, og her er $g(X) \in R[X]$, da R er helt afsluttet, og dermed $h(X) \in R[X]$, ~~ifølg. Gauss' lemma.~~ da f og g er normerede

Anvendes den kann. homomorfi $f(X) \longrightarrow \overline{f}(X)$ af $R[X] \longrightarrow R/\mathfrak{q}[X]$, vil $\overline{g}(X)\overline{h}(X) = \overline{f}(X) = X^m$, så at $\overline{g}(X) = X^\nu$ (og $\overline{h}(X) = X^{m-\nu}$) (Dette indses ved at betragte ligningen i $R/\mathfrak{q}$'s kvot.legeme), og dermed $g(X) = X^\nu + \beta_1 X^{\nu-1} + \ldots + \beta_\nu$, $\beta_1, \ldots, \beta_\nu \in \mathfrak{q}$. og

$$(*) \qquad s^\nu + \beta_1 s^{\nu-1} + \ldots + \beta_\nu = 0.$$

På den anden side er $s = ab'$, hvor $a \in R \setminus \mathfrak{q}$, $b' \in R' \setminus \varphi'$; da b' er hel over R, er $k(X) = \mathrm{Irr}(b',K) = X^\mu + \gamma_1 X^{\mu-1} + \ldots + \gamma_\mu \in R[X]$, og $b'^\mu + \gamma_1 b'^{\mu-1} + \ldots + \gamma_\mu = 0$, og ved multiplikation med a^μ:

$$(**) \qquad s^\mu + \gamma_1 a s^{\mu-1} + \ldots + \gamma_\mu a^\mu = 0,$$

hvoraf $\nu \leq \mu$. På tilsvarende måde fås af $(*)$ ved division med a^ν, at $\mu \leq \nu$, altså $\mu = \nu$, men så må $\gamma_1 a = \beta_1, \ldots \gamma_\mu a^\mu = \beta_\mu$. Da $\beta_i \in \mathfrak{q}$, og $a^i \notin \mathfrak{q}$ må $\gamma_i \in \mathfrak{q}$, $i = 1, \ldots, \mu$, men så er $b'^\mu = -\gamma_1 b'^{\mu-1} - \ldots - \gamma_\mu \in \mathfrak{q}R' \subseteq \varphi'$, og dermed $b' \in \varphi'$, modstrid. ∎

Lemma. Lad $R = K[\alpha_1,\ldots,\alpha_m]$ være et e.f. int.omr. med $\mathrm{trgr}_K R = t \geq 1$, og φ et minimalt primideal i R, da er $\mathrm{trgr}_K(R/\varphi) = t-1$. (som har mening, thi da $t \geq 1$, er R ikke et legeme, så et minimalt primideal er ikketrivielt)

Bevis. 1) Hvis $t = n$, er $R \cong K[X_1,\ldots,X_m]$ et U.F.D., og hvis $f \in \varphi \setminus (0)$, er $f = p_1 \ldots p_r$, så fx $p_1 \in \varphi$, og dermed $(p_1) \subseteq \varphi$, men da p_1 er irreducibel og R et U.F.D. er (p_1) et primideal, og altså $= \varphi$. Vi har $\varphi = (p(X_1,\ldots,X_m))$ og vi kan antage, at fx X_m effektivt forekommer i p. Nu er $R/\varphi = K[\overline{X_1},\ldots,\overline{X_m}]$ og da $p(\overline{X_1},\ldots,\overline{X_m}) = 0$, er $\overline{X_1},\ldots,\overline{X_m}$ alg.afh., så at $\mathrm{trgr}_K(R/\varphi) \leq n-1$. På den anden side er $\overline{X_1},\ldots,\overline{X_{m-1}}$ alg. uafh., thi $f(\overline{X_1},\ldots,\overline{X_{m-1}}) = 0 \Rightarrow f(X_1,\ldots,X_{m-1}) \in \varphi \Rightarrow f(X_1,\ldots,X_{m-1}) = p(X_1,\ldots,X_m)g(X_q,\ldots,X_m) \Rightarrow f = 0$, da X_m ikke forekommer på venstre side. Følgelig er $\mathrm{trgr}_K R/\varphi = n-1 = t-1$.

2) K er uendeligt, og $\mathrm{trgr}_K(R) = t \leq n$. Iflg. Noethers normaliseringslemma findes nu t K-lin.komb., $z_1,\ldots,z_t$, af $\alpha_1,\ldots,\alpha_m$, så at R er hel over $K[z_1,\ldots,z_t] = \hat{R}$. $\hat{R}$ er U.F.D. og dermed helt afsluttet i sit kvot.legeme, så $\varphi \cap \hat{R}$ er minimalt iflg. Going-down. Af 1) slutter vi, at $\mathrm{trgr}_K(\hat{R}/\varphi \cap \hat{R}) = t-1$, og det er let at se, at denne trgr. netop er $\mathrm{trgr}_K(R/\varphi)$.

3) K er endeligt, og $\mathrm{trgr}_K R = t \leq n$. Lad L være R's kvot.legeme, lad $\tilde{L}$ være L's afgebraisk afsluttede hylster. K's algebraiske hylster, $\tilde{K}$, i L er et algebraisk afsluttet hylster af K, og har som sådan uendelig mange elementer. Vi sætter $\tilde{R} = \tilde{K}[\alpha_1,\ldots,\alpha_m]$.

$$\begin{array}{ccccc} \tilde{K} & \subseteq & \tilde{R} = \tilde{K}[\alpha_1,\ldots,\alpha_m] & \subseteq & \tilde{L} \\ \cup\!| & & \cup\!| & & \cup\!| \\ K & \subseteq & R = K[\alpha_1,\ldots,\alpha_m] & \subseteq & L, \end{array}$$

da er $\tilde{R}$ hel over R, så iflg. Lying-over findes $\tilde{\varphi} \subseteq \tilde{R}$ med $\tilde{\varphi} \cap R = \varphi$, og $\tilde{\varphi}$ er minimalt iflg. Going-up. Nu ses det let, at $\mathrm{trgr}_{\tilde{K}}\tilde{R} \geq 1$, så iflg. 2) er $\mathrm{trgr}_{\tilde{K}}(\tilde{R}/\tilde{\varphi}) = \mathrm{trgr}_{\tilde{K}}(\tilde{R}) - 1$. Da $\tilde{K}/K$ er algebraisk og $\tilde{R}/R$ er hel, og dermed algebraisk, er $\mathrm{trgr}_{\tilde{K}}\tilde{R} = \mathrm{trgr}_K\tilde{R} = \mathrm{trgr}_K R = t$, og da $\tilde{R}$ er hel over R, er også $\tilde{R}/\tilde{\varphi}$ hel over $R/\tilde{\varphi} \cap R = R/\varphi$ ɔ: $\mathrm{trgr}_{\tilde{K}}(\tilde{R}/\tilde{\varphi}) = \mathrm{trgr}_K(\tilde{R}/\tilde{\varphi}) = \mathrm{trgr}_K(R/\varphi)$. Ovenstående relation giver nu det ønskede. ∎

Lemma. Hvis $R = K[X_1,\ldots,X_n]$ og $\varphi_1 \subset \varphi_2 \subset R$, da er $\mathrm{trgr}_K(R/\varphi_1) - \mathrm{trgr}_K(R/\varphi_2) = 1 \Leftrightarrow$ der findes ingen primidealer mellem φ_1 og φ_2.

Bevis. "$\Rightarrow$": Indirekte: hvis $\varphi_1 \subset \mathfrak{o} \subset \varphi_2$, da er $R/\varphi_1 \to R/\mathfrak{o}$ ikke en isomorfi, så $\mathrm{trgr}_K(R/\varphi_1) - \mathrm{trgr}_K(R/\mathfrak{o}) \geq 1$. Analogt ses, at $\mathrm{trgr}(R/\mathfrak{o}) - \mathrm{trgr}(R/\varphi_2) \geq 1$, men så er $\mathrm{trgr}(R/\varphi_1) - \mathrm{trgr}(R/\varphi_2) \geq 2$.

"$\Leftarrow$" φ_2/φ_1 er iflg. forudsætning minimalt i $R/\varphi_1 \cong K[\overline{X_1},\ldots,\overline{X_m}]$, så iflg. det foregående lemma er $\mathrm{trgr}_K(R/\varphi_1 \,/\, \varphi_2/\varphi_1) = \mathrm{trgr}(R/\varphi_1) - 1$, men $R/\varphi_1 \,/\, \varphi_2/\varphi_1$ er K-isomorf med R/φ_2. ∎

For et primideal $\mathfrak{p}$ i en ring R siges <u>højden</u> $h(\mathfrak{p})$ af være h, hvis der findes en kæde

$$(*) \qquad \mathfrak{p} \supset \mathfrak{p}_1 \supset \dots \supset \mathfrak{p}_h,$$

og hvis ingen sådan kæde har mere end h+1 primidealer.

Bemærk. Der er - endda for Noetherske ringe - forkert, at enhver uforfinelig kæde $(*)$ har h elementer.

For et primideal $\mathfrak{p}$ i en ring R siges <u>dybden</u> $d(\mathfrak{p})$ af være d, hvis der findes en kæde

$$\mathfrak{p} \subset \mathfrak{p}_1 \subset \dots \subset \mathfrak{p}_d \subset R$$

og hvis ingen sådan kæde har mere end d+1 primidealer $(\subset R)$.
Det ses, at Krulldim.R = d(0) og <u>$d(\mathfrak{p}) = \text{Krulldim}(R/\mathfrak{p})$.</u>

Sætning. <u>Hvis $\mathfrak{p}$ er et primideal i $R = K[X_1,\dots,X_n]$, da er $d(\mathfrak{p}) = \text{trgr}_K(R/\mathfrak{p})$ og $h(\mathfrak{p}) = n - \text{trgr}_K(R/\mathfrak{p})$.</u> [<u>Der gælder endda: For enhver uforfinelig kæde $\mathfrak{p} \subset \mathfrak{p}_1 \subset \dots \mathfrak{p}_d \subset R$ er $d = \text{trgr}(R/\mathfrak{p})$, og for enhver uforfinelig kæde $\mathfrak{p} \supset \mathfrak{p}_1' \supset \dots \supset \mathfrak{p}_h' = (0)$ er $h = n - \text{trgr}(R/\mathfrak{p})$.</u>
Bevis (for [...]). Da $\mathfrak{p}_d$ er maximalt, er $R/\mathfrak{p}_d = K[\overline{X_1},\dots,\overline{X_n}]$ et legeme, og dermed iflg. Hns_1 $R/\mathfrak{p}_d$ algebraisk over K, så trgr $R/\mathfrak{p}_d = 0$. Nu er $\text{trgr}(R/\mathfrak{p}_{d-1}) = \text{trgr}(R/\mathfrak{p}_d)+1 = 1,\dots,\text{trgr}(R/\mathfrak{p}_1) = d-1$, $\text{trgr}(R/\mathfrak{p}) = d$, $\text{trgr}(R/\mathfrak{p}_1') = d+1,\dots,\text{trgr}(R/\mathfrak{p}_{h-1}') = d+h-1$, $\text{Trgr}(R/\mathfrak{p}_h') = \text{trgr}(R) = d+h$, hvoraf $d+h = n$. ∎

Bemærk. Ovenstående kan drejes til et bevis for Hns_1?

For en irreducibel varietet, V, har vi sat $\dim V = \text{trgr}_K R/\mathcal{F}(V)$. Hvis K er algebraisk afsluttet er der en 1-1 forb. mellem irreducible varieteter og primidealer, og dermed mellem kæder $V \supset V_1 \supset \dots \supset V_d \supset \emptyset$ og $\mathcal{F}(V) = \mathfrak{p} \subset \mathfrak{p}_1 \subset \dots \subset \mathfrak{p}_d \subset R$. Vi har derfor:

Korollar. <u>Hvis K er alg.afsl. og $V \subseteq \mathcal{A}_n(K)$ er en irreducibel varietet, da er $\dim V = d \Leftrightarrow$ der findes en uforfinelig kæde $V \supset V_1 \supset \dots \supset V_d \supset \emptyset$ af irreducible varieteter.</u>

Korollar. <u>$\dim V = n-1 \Leftrightarrow \mathcal{F}(V)$ er minimalt primideal $\Leftrightarrow \mathcal{F}(V) = (p(X_1,\dots,X_n))$, p irreducibel.</u>

Sætning. <u>Et maximalt ideal, $\mathfrak{M}$, i $R = K[X_1,\dots,X_n]$ (K vilk.), kan skrives $\mathfrak{M} = (p_1(X_1), p_2(X_1,X_2),\dots,p_n(X_1,\dots,X_n))$.</u> (og vi viser senere, at $\mathfrak{M}$ ikke kan frembringes af færre end n pol.)
Bevis. Iflg. Hns_1 er $R/\mathfrak{M} = K[\overline{X_1},\dots,\overline{X_n}]$ alg. over K, så vi har

$$K \subseteq K[\overline{X_1}] \subseteq K[\overline{X_1},\overline{X_2}] \subseteq \dots \subseteq K[\overline{X_1},\dots,\overline{X_n}]$$

alle legemer. Sæt $p_i(Z_i) = \mathrm{Irr}(\overline{X_i}, K[\overline{X_1},\ldots,\overline{X_{i-1}}])$, da findes polynomier $p_i(Z_1,\ldots,Z_i) \in K[Z_1,\ldots,Z_i]$, så at $p_i(\overline{X_1},\ldots,\overline{X_{i-1}},Z_i) = p_i(Z_i) \in K[\overline{X_1},\ldots,\overline{X_{i-1}}][Z_i]$. Nu er $p_i(\overline{X_1},\ldots,\overline{X_i}) = 0$, og dermed $p_i(X_1,\ldots,X_i) \in \mathfrak{M}$.

Ved minduktion viser vi nu, at $\mathfrak{M} \cap K[X_1,\ldots,X_i] = (p_1(X_1),\ldots,p_i(X_1,\ldots,X_i))$. i = 1: For $f(X_1) \in \mathfrak{M}$ er $f(\overline{X_1}) = 0$, hvoraf $f(X_1) = g(X_1)p_1(X_1) \in (p_1(X_1))$.

Antag påstanden for i-1, og lad $f(X_1,\ldots,X_i) \in \mathfrak{M}$, da er $f(\overline{X_1},\ldots,\overline{X_i}) = 0$, så $f(\overline{X_1},\ldots,\overline{X_{i-1}},X_i) = g(X_i)p_i(X_i) = g(\overline{X_1},\ldots,\overline{X_{i-1}},X_i)p_i(\overline{X_1},\ldots,\overline{X_{i-1}},X_i)$, altså $f(\overline{X_1},\ldots,\overline{X_{i-1}},X_i) - g(\overline{X_1},\ldots,\overline{X_{i-1}},X_i)p_i(\overline{X_1},\ldots,\overline{X_{i-1}},X_i) = 0$. Nu er

$$f(X_1,\ldots,X_i) - g(X_1,\ldots,X_i)p_i(X_1,\ldots,X_i) = X_i^N h_0(X_1,\ldots,X_{i-1}) + \ldots + h_N(X_1,\ldots,X_{i-1}),$$

hvor altså $h_k(\overline{X_1},\ldots,\overline{X_{i-1}}) = (0)$, og dermed $h_k(X_1,\ldots,X_{i-1}) \in \mathfrak{M}$, men så er $h \in (p_1,\ldots,p_{i-1})$ iflg. induktionsforudsætningen, og relationen viser nu, at $f \in (p_1,\ldots,p_i)$ ∎

Sætning.(Primbasis-). *Hvis $\mathfrak{P}$ er et primideal i $R = K[X_1,\ldots,X_m]$ af højden $h(\mathfrak{P}) = h$, da findes h polynomier $p_1,\ldots,p_h \in R$ og et pol. $F \notin \mathfrak{P}$, så at $\mathfrak{P} = (p_1,\ldots,p_h):F$.*

Bevis. Sættes $d = d(\mathfrak{P})$, er $d = \mathrm{trgr}(R/\mathfrak{P}) = n-h$. Vi har $R/\mathfrak{P} = K[\overline{X_1},\ldots,\overline{X_m}]$, og vi kan antage, at fx. $\overline{X_1},\ldots,\overline{X_d}$ er en tr.basis for $R/\mathfrak{P}$ over K. Hvis $f \in K[X_1,\ldots,X_d]$ og $f \in \mathfrak{P}$, er $f(\overline{X_1},\ldots,\overline{X_d}) = 0$ og dermed $f = 0$, så vi slutter, at $K[X_1,\ldots,X_d] \cap \mathfrak{P} = (0)$. Sættes $S = K[X_1,\ldots,X_d]\setminus(0)$, er altså $S \cap \mathfrak{P} = \emptyset$.

Restklassen $\overline{X_{d+1}}$ er algebraisk over $K[\overline{X_1},\ldots,\overline{X_d}]$ fx en rel.

$$\overline{X_{d+1}}^k f_0(\overline{X_1},\ldots,\overline{X_d}) + \ldots + f_k(\overline{X_1},\ldots,\overline{X_d}) = 0,$$

og dermed også en relation

$$X_{d+1}^k f_0(X_1,\ldots,X_d) + \ldots + f_k(X_1,\ldots,X_d).$$

Sættes $\hat{R} = \frac{R}{S}$, har vi $\hat{R} = K(X_1,\ldots,X_d)[X_{d+1},\ldots,X_m]$, og $\hat{\mathfrak{P}} = \mathfrak{P}\hat{R}$ er maximalt, da $\overline{X_{d+1}}$ mod $\hat{\mathfrak{P}}$ er alg. over $K(X_1,\ldots,X_d)$, o.s.v. Iflg. den foregående sætning, er $\hat{\mathfrak{P}} = (p_1(X_1,\ldots,X_{d+1})\ldots p_h)$, hvor $p_1,\ldots,p_h \in \hat{\mathfrak{P}} \cap R = \mathfrak{P}$, idet vi udnytter, at elementerne i S er enheder i R.

Nu er $\mathfrak{P} = (f_1,\ldots,f_s)$, og $f_1 = g_1p_1+\ldots+g_hp_h$, hvor $g_i \in \hat{R}$, men så findes $F_1 \in S$ (fællesnævner for g_i'erne) så $F_1f_1 \in Rp_1+\ldots Rp_h$. Analogt findes $F_i \in S$, så $F_if_i \in Rp_1+\ldots+Rp_h$. Nu er $F = F_1\ldots F_s \in S$, og $Ff_i \in Rp_1+\ldots+Rp_h$, altså $F\mathfrak{P} \subseteq Rp_1+\ldots+Rp_h$ ⟺ $\mathfrak{P} \subseteq (p_1,\ldots,p_h):F$. Er omvendt $h \in (p_1,\ldots,p_h):F$, vil $hF \in \mathfrak{P}$, og da $F \notin \mathfrak{P}$, må $h \in \mathfrak{P}$. ∎

KAPITEL VII DIMMENSIONSTEORI I NOETHERSKE RINGE=

I et Noethersk int.omr. R er $\mathfrak{p}^n$ ikke nødvendigvis primært. For et primideal $\mathfrak{p}$ i R sættes $\mathfrak{p}^{(n)} = (\mathfrak{p}R_{\mathfrak{p}})^n \cap R$ og kaldes den n'te symbolske potens af $\mathfrak{p}$.

Sætning. *$\mathfrak{p}^{(n)}$ er $\mathfrak{p}$-primær [$\mathfrak{p}^{(n)}$ er den entydigt bestemte $\mathfrak{p}$-primære minimalkomponent af $\mathfrak{p}^n$] og $\mathfrak{p} = \mathfrak{p}^{(1)} \supset \mathfrak{p}^{(2)} \supset \ldots$ og $\bigcap_1^\infty \mathfrak{p}^{(n)} = (0)$*

Bevis. $R_{\mathfrak{p}}$ er lokal ring med $\mathfrak{p}R_{\mathfrak{p}}$ som det maximale ideal, $\mathrm{Rad}(\mathfrak{p}R_{\mathfrak{p}}) = \mathfrak{p}R_{\mathfrak{p}}$, så $(\mathfrak{p}R_{\mathfrak{p}})^n$ er $\mathfrak{p}R_{\mathfrak{p}}$-primært, men så er $\mathfrak{p}^{(n)}$ $\mathfrak{p}$-primært, hvilket let eftervises. Da $\mathfrak{p}R_{\mathfrak{p}} \neq R$ og $R_{\mathfrak{p}}$ er int.omr., er $\bigcap (\mathfrak{p}R_{\mathfrak{p}})^n = (0)$, og dermed $\bigcap \mathfrak{p}^{(n)} = (0)$, og af $\mathfrak{p}R_{\mathfrak{p}} \supset (\mathfrak{p}R_{\mathfrak{p}})^2 \supset \ldots$ følger let, at $\mathfrak{p} = \mathfrak{p}^{(1)} \supset \mathfrak{p}^{(2)} \supset \ldots$ ∎

Vi har tidligere set, at hvis R er U.F.D. og $\mathfrak{p}$ er minimalt, da er $\mathfrak{p} = (\pi)$ et hovedideal. Omvendt: Hvis $\mathfrak{p} = (\pi)$ er primideal, og R er Noethersk int.omr. eller U.F.D., da er $\mathfrak{p}$ minimalt, thi er $\mathfrak{p}_1 \subset \mathfrak{p} = (\pi)$, er $\mathfrak{p}_1 = \pi\mathfrak{a}$, hvoraf $\mathfrak{p}_1 \supseteq (\pi)\mathfrak{a}$, så at $\mathfrak{p}_1 \supseteq (\pi)$ eller $\mathfrak{p}_1 \supseteq \mathfrak{a}$, altså $\mathfrak{p}_1 \supseteq \mathfrak{a}$, men så er $\mathfrak{p}_1 = \mathfrak{a}$. Af $\mathfrak{p}_1 = (\pi)\mathfrak{p}_1 = (\pi^2)\mathfrak{p}_1 = \ldots$ følger, hvis R er Noethersk, at $\mathfrak{p}_1 \subseteq \bigcap (\pi)^n = (0)$, altså $\mathfrak{p}_1 = (0)$, og hvis R er U.F.D. at der for $a \in \mathfrak{p}_1$ gælder $\pi^n \mid a$ for alle n, altså at a = 0.

~~Ekstra Minimalkomponenter hørende til ideal a kaldes også~~

Lad R være en Noethersk ring. De minimale elementer blandt primidealerne hørende til et ideal $\mathfrak{a}$ kaldes isolerede primidealer for $\mathfrak{a}$.

Lemma. *Lad R være Noethersk, da er $\mathfrak{p}$ isoleret primideal for $\mathfrak{a}$ $\Leftrightarrow$ $\mathfrak{p}$ er et mindste primideal $\supseteq \mathfrak{a}$.*

Bevis. Følger let af primær-dekompositionen. ∎

Eks. I en Noethersk ring er $h(\mathfrak{p}) = 0 \Leftrightarrow \mathfrak{p}$ isoleret primideal for (0).

Eks. At en vilkårlig ging R har primidealer af højde 0 følger let af Zorn's lemma, men

Bemærk. Der findes int.omr. uden primidealer af højde 1.

Krull's hovedidealsætning. *Lad R være et Noethersk int.omr. og $\mathfrak{p}$ et isoleret primideal for et hovedideal (a) $\neq$ R, da er $\mathfrak{p} = (0)$ for a = 0, og $\mathfrak{p}$ er minimalt (d: $h(\mathfrak{p}) = 1$) for $a \neq 0$, altså altid $h(\mathfrak{p}) \leq 1$.*

Omvendt er ethvert minimalt primideal isoleret primideal for et hovedideal $(a) \neq R$.

Bevis. "Omvendt": Hvis $\mathfrak{p} \supset (0)$ er minimalt og $a \in \mathfrak{p} \setminus (0)$, da er $\mathfrak{p} \supseteq (a) = \mathfrak{q}_1 \cap \ldots \mathfrak{q}_m$, så $\mathfrak{p}$ indeholder et isoleret primideal $\mathfrak{p}_j$ for (a), og da $\mathfrak{p}_j \neq (0)$, er $\mathfrak{p} = \mathfrak{p}_j$.

Lad nu $a \neq 0$, enhed, og lad $\mathfrak{p}$ være isoleret fra (a); vi skal vise, at $h(\mathfrak{p}) = 1$. Indirekte, da var $(0) \subset \mathfrak{p}_1 \subset \mathfrak{p}$. Ved overgang til kvotientringen $R_{\mathfrak{p}}$ kan vi derfor antage, at R er lokal, $\mathfrak{p}$ er maximalt og det eneste primideal i R, der $\supseteq (a)$. [thi $\mathfrak{p}R_{\mathfrak{p}}$ er det maximale ideal i $R_{\mathfrak{p}}$, og $(0) \subset \mathfrak{p}_1 R_{\mathfrak{p}} \subset \mathfrak{p} R_{\mathfrak{p}}$, og da $\mathfrak{p} \supseteq (a)$ vil $\mathfrak{p}R_{\mathfrak{p}} \supseteq (a)R_{\mathfrak{p}} = aR_{\mathfrak{p}}$, og hvis $\mathfrak{p}R_{\mathfrak{p}} \supseteq \hat{\mathfrak{p}} \supseteq aR_{\mathfrak{p}}$, vil $\mathfrak{p} \supseteq \hat{\mathfrak{p}} \cap R \supseteq aR_{\mathfrak{p}} \cap R \supseteq aR = (a)$, og da $\mathfrak{p}$ er isoleret for (a), er $\mathfrak{p} = \hat{\mathfrak{p}} \cap R$ og dermed $\mathfrak{p}R_{\mathfrak{p}} = \hat{\mathfrak{p}}$.]

Nu er $\mathfrak{p}_1 \supset \mathfrak{p}_1^{(2)} \supset \mathfrak{p}_1^{(3)} \supset \ldots$ og dermed $\mathfrak{p}_1 + (a) \supseteq \mathfrak{p}_1^{(2)} + (a) \supseteq \ldots \supseteq (a)$. Da $\mathfrak{p}$ er det eneste primideal, der indeholder (a), vil $R/(a)$ kun have ét primideal, og da $R/(a)$ er Noethersk, vil $R/(a)$ iflg Akizuki være d.c.c. Kæden $R/(a) \supseteq \mathfrak{p}_1 + (a)/(a) \supseteq \ldots \supseteq \mathfrak{p}_1^{(m)} + (a)/(a) \supseteq \ldots$ vil derfor "bryde af", så at vi for et n har $\mathfrak{p}_1^{(n)} + (a)/(a) = \mathfrak{p}_1^{(n+1)} + (a)/(a)$, og dermed $\mathfrak{p}_1^{(n)} + (a) = \mathfrak{p}_1^{(n+1)} + (a)$. Specielt er $\mathfrak{p}_1^{(n)} \subseteq (a) + \mathfrak{p}_1^{(n+1)}$.

For $x \in \mathfrak{p}_1^{(n)}$ er altså $x = ra + y$, hvor $y \in \mathfrak{p}_1^{(n+1)}$, og dermed $ra = x - y \in \mathfrak{p}_1^{(n)}$. Da $\mathfrak{p}_1^{(n)}$ er $\mathfrak{p}_1$-primær, og $a \notin \mathfrak{p}_1$! må $r \in \mathfrak{p}_1^{(n)}$. Vi har altså vist, at $\mathfrak{p}_1^{(n)} \subseteq \mathfrak{p}_1^{(n)} a + \mathfrak{p}_1^{(n+1)}$, og da $\supseteq$ er trivielt må

$$\mathfrak{p}_1^{(n)} = \mathfrak{p}_1^{(n)} a + \mathfrak{p}_1^{(n+1)}.$$

Irestklasseringen $R/\mathfrak{p}_1^{(n+1)}$ får vi nu:

$$\mathfrak{p}_1^{(n)}/\mathfrak{p}_1^{(n+1)} = (\bar{a})\, \mathfrak{p}_1^{(n)}/\mathfrak{p}_1^{(n+1)}.$$

Her er $\mathfrak{p}_1^{(n)}/\mathfrak{p}_1^{(n+1)} \neq 0$, da $\mathfrak{p}_1^{(n)} \supset \mathfrak{p}_1^{(n+1)}$, og da $a \notin \mathfrak{p}_1^{(n+1)}$ er $(\bar{a}) \neq (\bar{0})$. Endvidere er $R/\mathfrak{p}_1^{(n+1)}$ lokal, Noethersk, da R er lokal Noethersk, så vi er færdige når vi har vist

Lemma. I en lokal Noethersk ring R vil $\mathfrak{a}\mathfrak{b} = \mathfrak{a}$ medføre, at $\mathfrak{a} = (0)$ eller $\mathfrak{b} = R$.

Bevis. Antag $\mathfrak{b} \neq R$, da er $\mathfrak{b} \subseteq \mathfrak{M} \subset R$. Er $\mathfrak{a} = (a_1, \ldots, a_m)$, er $\mathfrak{a}\mathfrak{b} = \{ \sum_1^m b^{(i)} a_i \mid b^{(i)} \in \mathfrak{b} \}$, og da $\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{b}$ findes en matrix $\underline{\underline{B}}$ med elementer i $\mathfrak{b}$, så at $\underline{a}_1 = \underline{\underline{B}}\, \underline{a}_1$ d.v.s. $(\underline{\underline{E}} - \underline{\underline{B}}) \cdot \underline{a}_1 = \underline{0}_1$.

Nu er $\det(\underline{\underline{E}} - \underline{\underline{B}}) = 1 - b$, hvor $b \in \mathfrak{b} \subseteq \mathfrak{M}$, og $1 - b$ således er enhed, så der findes $c \in R$, så $c \cdot \det(\underline{\underline{E}} - \underline{\underline{B}}) = 1$, men så har $\underline{\underline{E}} - \underline{\underline{B}}$ en invers matrix, og relationen viser nu, at $\underline{a}_1 = \underline{0}_1$ altså $\mathfrak{a} = (0)$. ∎

[Korollar til lemma. I en lokal Noethersk ring er $\bigcap_1^\infty \mathfrak{M}^n = (0)$. indses som for int.områder, se p.V,8.]

Korollar. I et Noethersk int.omr. vil ethvert fra (0) forskelligt primideal indeholde et minimalt primedeal.

Vi har brug for flg. generalisation:

Sætning. Lad R være en Noethersk ring, og lad $\mathfrak{p}$ være isoleret primideal for $(a) \neq R$, da er $h(\mathfrak{p}) \leq 1$.

Bevis. Indirekte: $\mathfrak{p} \supset \mathfrak{p}_1 \supset \mathfrak{p}_2$. Da $\mathfrak{p}$ er et mindste primideal for (a), er $\mathfrak{p}$ et mindste primideal for $(a)+\mathfrak{p}_2$, og $\mathfrak{p} \supseteq (a)+\mathfrak{p}_2 \supseteq \mathfrak{p}_2$. I restklasseringen $R/\mathfrak{p}_2$ er $\mathfrak{p}/\mathfrak{p}_2 \supseteq (\bar{a}) \supseteq (0)$, og $\mathfrak{p}/\mathfrak{p}_2$ er et mindste primideal $(\bar{a})$, og dermed $h(\mathfrak{p}/\mathfrak{p}_2) \leq 1$, da $R/\mathfrak{p}_2$ er int. omr., i modstrid med $\mathfrak{p}/\mathfrak{p}_2 \supset \mathfrak{p}_1/\mathfrak{p}_2 \supset \mathfrak{p}_2/\mathfrak{p}_2 = (0)$. ∎

Lemma. Lad R være en Noethersk ring, og lad $\mathfrak{p} \supset \mathfrak{p}_1 \supset \mathfrak{p}_2$, $\mathfrak{p}_1', \ldots, \mathfrak{p}_k'$ være primidealer, så at $\mathfrak{p} \not\subseteq \mathfrak{p}_i'$ for alle i, da findes $\mathfrak{p}^*$, så $\mathfrak{p} \supset \mathfrak{p}^* \supset \mathfrak{p}_2$ og så $\mathfrak{p}^* \not\subseteq \mathfrak{p}_i'$ for alle i.

Bevis. Af $\mathfrak{p} \not\subseteq \mathfrak{p}_2$ og $\mathfrak{p} \not\subseteq \mathfrak{p}_i'$ følger (jfr.p.V,1), at $\mathfrak{p} \not\subseteq \mathfrak{p}_2 \cup \bigcup_i \mathfrak{p}_i'$. Vælg altså $a \in \mathfrak{p}$, $a \notin \mathfrak{p}_2$, $a \notin \mathfrak{p}_i'$, alle i. Nu er $\mathfrak{p} \supseteq (a)+\mathfrak{p}_2$, så $\mathfrak{p} \supseteq$ et isoleret primideal $\mathfrak{p}^*$ for $(a)+\mathfrak{p}_2$. Da $\mathfrak{p} \supseteq \mathfrak{p}^* \supseteq (a)+\mathfrak{p}_2 \supset \mathfrak{p}_2$, behøver vi blot at vise, at $\mathfrak{p} \neq \mathfrak{p}^*$. Indirekte: da vær $\mathfrak{p} = \mathfrak{p}^*$ isoleret for $(a)+\mathfrak{p}_2$. Nu er $R/\mathfrak{p}_2 \supset \mathfrak{p}/\mathfrak{p}_2 \supseteq (\bar{a}) \supset (0)$, og $\mathfrak{p}/\mathfrak{p}_2$ er isoleret for $(\bar{a})$, så iflg. Krull er $h(\mathfrak{p}/\mathfrak{p}_2) = 1$, i modstrid med $\mathfrak{p}/\mathfrak{p}_2 \supset \mathfrak{p}_1/\mathfrak{p}_2 \supset \mathfrak{p}_2/\mathfrak{p}_2 = (0)$. ∎

Korollar til lemma. Lad R være Noethersk, og $\mathfrak{p} \supset \mathfrak{p}_1 \supset \ldots \supset \mathfrak{p}_\ell$, $\mathfrak{p}_1', \ldots, \mathfrak{p}_k'$ primidealer, så at $\mathfrak{p} \not\subseteq \mathfrak{p}_i'$ for alle i, da findes $\mathfrak{p}_1^*, \ldots, \mathfrak{p}_{\ell-1}^*$, så at $\mathfrak{p} \supset \mathfrak{p}_1^* \supset \ldots \supset \mathfrak{p}_{\ell-1}^* \supset \mathfrak{p}_\ell$ og så $\mathfrak{p}_{\ell-1}^* \not\subseteq \mathfrak{p}_i'$ for alle i.

Bevis. Da $\mathfrak{p} \supset \mathfrak{p}_1 \supset \mathfrak{p}_2$ findes $\mathfrak{p}_1^*$ så $\mathfrak{p} \supset \mathfrak{p}_1^* \supset \mathfrak{p}_2$ og $\mathfrak{p}_1^* \not\subseteq \mathfrak{p}_i'$ for alle i. Nu er $\mathfrak{p}_1^* \supset \mathfrak{p}_2 \supset \mathfrak{p}_3$, så der findes $\mathfrak{p}_2^*$, så $\mathfrak{p}_1^* \supset \mathfrak{p}_2^* \supset \mathfrak{p}_3$ og $\mathfrak{p}_2^* \not\subseteq \mathfrak{p}_i'$ for alle i, o.s.v. ∎

Hovedsætning. Lad R være en Noethersk ring, og $\mathfrak{p}$ isoleret for et ideal $\mathfrak{a} = (a_1, \ldots, a_m) \neq R$, frembragt af m elementer, da er $h(\mathfrak{p}) \leq m$

Induktion efter m: $m = 1$ iflg. Krull. Antag sætningen for m-1, og lad $\mathfrak{p}$ være isoleret for $\mathfrak{a} = (a_1, \ldots, a_m)$. Lad $\mathfrak{p}_1', \ldots, \mathfrak{p}_k'$ være de isolerede primidealer for $(a_1, \ldots, a_m)$. Hvis $\mathfrak{p} \subseteq \mathfrak{p}_i'$ for et vist i er vi færdige iflg. ind.foruds., så vi antager, at $\mathfrak{p} \not\subseteq \mathfrak{p}_i'$ for alle i.

Lad $\mathfrak{p} \supset \mathfrak{p}_1 \supset \ldots \supset \mathfrak{p}_\ell$, da skal vi vise, at $1 \leq m$. Iflg. lemma kan vi antage, at $\mathfrak{p}_{\ell-1} \not\subseteq \mathfrak{p}_i'$ for alle i, men så er $\mathfrak{p}_{\ell-1} \not\subseteq \bigcup_i \mathfrak{p}_i'$,

altså findes $b \in \mathfrak{p}_{\ell-1}$, $b \notin \mathfrak{p}_i'$, alle i.
Da $b \in \mathfrak{p}$, er $\mathfrak{p} \supseteq (b, a_2, \ldots, a_m)$, så $\mathfrak{p}$ $\supseteq$et isoleret primideal $\mathfrak{p}^*$ for $(b, a_2, \ldots, a_m)$, og da $\mathfrak{p}^* \supseteq (b, a_2, \ldots, a_m) \supseteq (a_2, \ldots, a_m)$ vil $\mathfrak{p}^*$ $\supseteq$ et isoleret primidela $\mathfrak{p}_j'$ for $(a_2, \ldots, a_m)$; altså $\mathfrak{p}^* \supseteq \mathfrak{p}_j'$, og da $b \in \mathfrak{p}^* \setminus \mathfrak{p}_j'$ gælder endda $\mathfrak{p}^* \supset \mathfrak{p}_j'$.
Der gælder nu $\mathfrak{p} = \mathfrak{p}^*$, thi ellers var $\mathfrak{p} \supset \mathfrak{p}^* \supset \mathfrak{p}_j'$. Ved overgang til $R/(a_2, \ldots, a_m)$ ville $R/(a_2, \ldots, a_m) \supset \mathfrak{p}/(a_2, \ldots, a_m) \supseteq (\overline{a_1}) \supseteq (0)$, og $\mathfrak{p}/(a_2, \ldots, a_m)$ er isoleret primideal for $(\overline{a_1})$, altså iflg. Krull $h(\mathfrak{p}/(a_2, \ldots, a_m)) \leq 1$, i modstrid med at $\mathfrak{p}/(a_2, \ldots, a_m) \supset \mathfrak{p}^*/(a_2, \ldots, a_m) \supset \mathfrak{p}_j'/(a, \ldots, a)$.
Vi har altså opnået: $\mathfrak{p} = \mathfrak{p}^*$ er isoleret primideal for $(b, a_2, \ldots, a_m)$, $b \in \mathfrak{p}_{\ell-1}$. Nu er $\mathfrak{p} \supset \mathfrak{p}_1 \ldots \supset \mathfrak{p}_{\ell-1} \supseteq (b)$, så

(*) $\mathfrak{p}/(b) \supset \mathfrak{p}_1/(b) \supset \ldots \mathfrak{p}_{\ell-1}/(b) \supseteq (0)$.

Da $\mathfrak{p}$ er isoleret for $(b, a_2, .., a_m) \supseteq (b)$, er $\mathfrak{p}/(b)$ isoleret for $(b, a_2, \ldots, a_m)/(b) = (\overline{a_2}, \ldots, \overline{a_m})$. Iflg. induktionsantagelsen er altså $h(\mathfrak{p}/(b)) \leq n-1$, og dermed af (*): $\ell - 1 \leq n-1$ o: $\ell \leq n$. ∎

Korollar. <u>Ethvert primideal $\mathfrak{p} = (a_1, \ldots, a_m)$ i en Noethersk ring har højde $h(\mathfrak{p}) \leq m$.</u>

Bemærk. Der findes Noetherske ringe med primidealer af uendelig dybde.

Eks. Lad $\mathfrak{M}$ være maximalt i $R = K[X_1, \ldots, X_n]$, da er $\mathfrak{M} = (p_1(X_1), \ldots, p_m(X_1, \ldots, X_m))$ og da $h(\mathfrak{M}) = n$, kan $\mathfrak{M}$ ikke frembringes af færre elementer.

Eks. Lad $\mathfrak{p}$ være primideal i $R = K[X_1, \ldots, X_n]$, af $h(\mathfrak{p}) = h$, da er $\mathfrak{p} = (p_1, \ldots, p_h):F$, hvor $F \notin \mathfrak{p}$. Denne fremstilling er bedst mulig, thi er $\mathfrak{p} = (f_1, \ldots, f_t):F$, hvor $F \notin \mathfrak{p}$, er $\mathfrak{p}R_{\mathfrak{p}} = (f_1, \ldots, f_t):(1) = (f_1, \ldots, f_t)$, og $h(\mathfrak{p}R_{\mathfrak{p}}) = h(\mathfrak{p}) = h$, så $t \geq h$.

Vi har følgende mere trivielle "Omvending". <u>Lad R være Noethersk ring, og $\mathfrak{p}$ et primideal af $h(\mathfrak{p}) = h$, da er $\mathfrak{p}$ isoleret for et ideal $\mathfrak{a} = (a_1, \ldots, a_h)$ frembragt af h elementer.</u>

Bevis. <u>h = 0.</u> Vi har $h(\mathfrak{p}) = 0 \Leftrightarrow \mathfrak{p}$ er isoleret primideal for (0). Der findes kun endelig mange sådanne, fx. $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$.
<u>$h \geq 1$.</u> Vi konstruerer successivt h elementer, $a_1, \ldots, a_h \in \mathfrak{p}$, så at ethvert isoleret primideal for $(a_1, \ldots, a_h)$ har højde $\geq i$ i [Iflg. hovedsætning er denne højde i øvrigt $= i$] $i = 1, \ldots, h$.

$i = 1$. Da $h(\mathfrak{P}) = h \geq 1$, er $\mathfrak{P} \not\subseteq \tilde{\mathfrak{P}}_j$, alle j, og dermed $\mathfrak{P} \not\subseteq \bigcup_j \tilde{\mathfrak{P}}_j$ Altså findes $a_1 \in \mathfrak{P}$, så $a_1 \notin \tilde{\mathfrak{P}}_j$, alle j. Da de isolerede primidealer for (a_1) nu må være forskellige fra $\tilde{\mathfrak{P}}_j$'erne, har de alle højde ≥ 1

Antag, at $a_1,\ldots,a_i$ er fundet, $i < h$. Lad $(a_1,\ldots,a_i)$ have de isolerede primidealer $\mathfrak{P}_1,\ldots,\mathfrak{P}_s,\mathfrak{P}_{s+1},\ldots,\mathfrak{P}_t$, hvor $\mathfrak{P}_1,\ldots,\mathfrak{P}_s$ er af højde $= i$, og $\mathfrak{P}_{s+1},\ldots,\mathfrak{P}_t$ af højde $> i$ [iflg. hovedsætningen er denne sidste mængde i øvrigt tom]. Da $h(\mathfrak{P}_j) = i < h = h(\mathfrak{P})$, $j = 1,\ldots,s$, er $\mathfrak{P} \not\subseteq \mathfrak{P}_j$, og dermed $\mathfrak{P} \not\subseteq \bigcup_j \mathfrak{P}_j$, så der findes $a_{i+1} \in \mathfrak{P}$, så $a_{i+1} \notin \mathfrak{P}_j$, $j = 1,\ldots,s$. Lad nu $\hat{\mathfrak{P}}$ være isoleret for $(a_1,\ldots,a_i,a_{i+1})$. Da $\hat{\mathfrak{P}} \supseteq (a_1,\ldots,a_i)$, må $\hat{\mathfrak{P}} \geq \mathfrak{P}_j$ for et passende j. Hvis $1 \leq j \leq s$, må, da $a_{i+1} \in \hat{\mathfrak{P}} \setminus \mathfrak{P}_j$, $\hat{\mathfrak{P}} \supset \mathfrak{P}_j$, og dermed $h(\hat{\mathfrak{P}}) > h(\mathfrak{P}_j) = i$, og hvis $s+1 \leq j \leq t$, er $h(\hat{\mathfrak{P}}) \geq h(\mathfrak{P}_j) > i$, altså altid $h(\hat{\mathfrak{P}}) \geq i+1$.

Heraf følger påstanden let. ∎

LOKALE NOETHERSKE RINGE

For en lokal Noethersk ring R med det maximale ideal $\mathfrak{M}$ sættes dim R = $h(\mathfrak{M})$. Hvis R er int.omr. er altså dim R = Krulldim.R. Iflg. hovedsætningen er dim R = $h(\mathfrak{M})$ endelig.

Da vi for en vilkårlig kæde

$$\mathfrak{P}_h \subset \ldots \subset \mathfrak{P}_1 \subset \mathfrak{P} \subset \mathfrak{P}'_1 \subset \ldots \subset \mathfrak{P}'_d \subset R$$

har $\mathfrak{P}'_d \subseteq \mathfrak{M}$, slutter vi:

Sætning. <u>I en lokal Noethersk ring R, er både højde $h(\mathfrak{P})$ og dybde $d(\mathfrak{P})$ endelige, og $h(\mathfrak{P})+d(\mathfrak{P}) \leq$ dim R.</u>

Sætning. <u>Lad R være en lokal Noethersk ring, af dim R = d, da findes et $\mathfrak{M}$-primært ideal frembragt af d elementer, medens intet $\mathfrak{M}$-primært ideal kan frembringes af færre end d elementer.</u>

Bevis. $d = 0$, da er ethvert ideal, og specielt (0), $\mathfrak{M}$-primært. $d \geq 1$. Iflg. "Omvending" findes $a_1,\ldots,a_d \in \mathfrak{M}$, så $\mathfrak{M}$ er isoleret for $\mathfrak{A} = (a_1,\ldots,a_d)$. Nu er $\mathfrak{A} = \mathfrak{A}_{f_1} \cap \ldots \cap \mathfrak{A}_{f_m}$, hvor Rad $\mathfrak{A}_{f_1} = \mathfrak{M}$ o: $\mathfrak{A} = \mathfrak{A}_{f_1}$, og $\mathfrak{A}_{f_1}$ er $\mathfrak{M}$-primært. Hvis omvendt $\mathfrak{A}_f = (a_1,\ldots,a_\nu)$ er $\mathfrak{M}$-primært, er $\mathfrak{M}$ isoleret for $(a_1,\ldots,a_\nu)$, og dermed $d = h(\mathfrak{M}) \leq \nu$ iflg. hovedsætningen ∎

Sætning. <u>Lad R være lokal Noethersk, da er $\bigcap_1^\infty (\mathfrak{A} + \mathfrak{M}^\nu) = \mathfrak{A}$ for ethvert ideal .</u>

Bevis. Vi kan antage, at $\mathfrak{A} \subsetneq \mathfrak{M} \subset R$. I $R/\mathfrak{A}$ har vi $\mathfrak{M}^\nu + \mathfrak{A}/\mathfrak{A} =$

$(\mathfrak{M}/\mathfrak{o})^\nu$, så da $(\bigcap_1^\infty(\mathfrak{o}+\mathfrak{M}^\nu))/\mathfrak{o} \subseteq (\mathfrak{o}+\mathfrak{M}^\nu)/\mathfrak{o} = (\mathfrak{M}/\mathfrak{o})^\nu$ for alle ν, er $(\bigcap_1^\infty(\mathfrak{o}+\mathfrak{M}^\nu))/\mathfrak{o} \subseteq \bigcap_1^\infty(\mathfrak{M}/\mathfrak{o})^\nu = (0)$, da $R/\mathfrak{o}$ er lokal (jfr p.VII,2), og dermed $\bigcap_1^\infty(\mathfrak{o}+\mathfrak{M}^\nu) \subseteq \mathfrak{o}$. Da $\supseteq$ er trivielt følger = ∎

Vi har tidligere set, at $\mathfrak{o}/\mathfrak{o}\mathfrak{M}$ er en $R/\mathfrak{M}$-modul ɔ: et vektorrum over legemet $R/\mathfrak{M}$. Der gælder

Sætning. <u>Vektorrumsdimmensionen $\dim_{R/\mathfrak{M}}(\mathfrak{o}/\mathfrak{o}\mathfrak{M})$ = det mindste antal frembringere for $\mathfrak{o}$.</u>

Bevis. "$\leq$" er trivielt, thi hvis $\mathfrak{o} = (a_1,\ldots,a_m)$, vil $\overline{a_1},\ldots,\overline{a_m}$ frembringe vektorrummet $\mathfrak{o}/\mathfrak{o}\mathfrak{M}$.

"$\geq$". Antag $\overline{a_1},\ldots,\overline{a_\mu}$ er en $R/\mathfrak{M}$-basis for $\mathfrak{o}/\mathfrak{o}\mathfrak{M}$, da er $\tilde{\mathfrak{o}} = (a_1,\ldots,a_\mu) \subseteq \mathfrak{o}$, og $\tilde{\mathfrak{o}}/\mathfrak{o}\mathfrak{M} = \mathfrak{o}/\mathfrak{o}\mathfrak{M}$ ɔ: $\tilde{\mathfrak{o}}+\mathfrak{o}\mathfrak{M} = \mathfrak{o}$. Af $\mathfrak{o} = \tilde{\mathfrak{o}}+\mathfrak{o}\mathfrak{M} = \tilde{\mathfrak{o}}+(\tilde{\mathfrak{o}}+\mathfrak{o}\mathfrak{M})\mathfrak{M} = \tilde{\mathfrak{o}}+\mathfrak{o}\mathfrak{M}^2 = \ldots = \tilde{\mathfrak{o}}+\mathfrak{o}\mathfrak{M}^\nu = \ldots$ fås $\mathfrak{o} = \bigcap_1^\infty(\tilde{\mathfrak{o}}+\mathfrak{o}\mathfrak{M}^\nu) \subseteq \bigcap_1^\infty(\tilde{\mathfrak{o}}+\mathfrak{M}^\nu) = \tilde{\mathfrak{o}}$. ∎

Vi skitserer nu den videregående teori for lokale ringe:

Betragt først $\mathfrak{R} = K[X_1,\ldots,X_d]$ og sæt $\mathfrak{R}_i$ = den additive undergruppe bestående af homogene i'te-gradspol. samt 0, da er

$$\mathfrak{R} = \mathfrak{R}_0 \oplus \mathfrak{R}_1 \oplus \ldots \quad \text{og} \quad \mathfrak{R}_i\mathfrak{R}_j \subseteq \mathfrak{R}_{i+j}$$

En ring, der har en sådan opspaltning kaldes en <u>gradueret ring.</u>
Et ideal $\mathfrak{J}$ i $\mathfrak{R}$ kaldes <u>homogent</u>, hvis $f \in \mathfrak{J}$, $f = f_0+f_1+\ldots$ $f_i \in \mathfrak{R}_i$ medfører, at $f_i \in \mathfrak{J}$. For et homogent ideal har vi da

$$\mathfrak{J} = \mathfrak{J}\cap\mathfrak{R}_0 \oplus \mathfrak{J}\cap\mathfrak{R}_1 \oplus \ldots$$

Nu er $\dim_K\mathfrak{R}_m = \binom{n+d-1}{d-1}$ = antallet af m'tegrads pol. pol. Det viser sig, at der gælder $\dim_K(\mathfrak{J}\cap\mathfrak{R}_n)$ = polynomium i n for alle store n, hvoraf

$$\dim_K(\mathfrak{R}_n/\mathfrak{J}\cap\mathfrak{R}_n) = \text{polynomium i n for store n,}$$

kaldet det <u>karakteristiske polynomium</u> eller <u>Hilbertfunktionen</u> for $\mathfrak{J}$.

Samuel (1954):
Lad R være lokal med $\mathfrak{M}$ som maximalt ideal. $R/\mathfrak{M} \oplus \mathfrak{M}/\mathfrak{M}^2 \oplus \ldots$ kan da organiseres til en gradueret ring: For $a \in \mathfrak{M}^\nu/\mathfrak{M}^{\nu+1}$, $b \in \mathfrak{M}^\mu/\mathfrak{M}^{\mu+1}$, er $\overline{ab} \in \mathfrak{M}^{\nu+\mu}/\mathfrak{M}^{\nu+\mu+1}$ en definition, thi $(a+\mathfrak{M}^{\nu+1})(b+\mathfrak{M}^{\mu+1}) \subseteq ab+\mathfrak{M}^{\nu+\mu+1}$. Dette kaldes <u>den til R hørende gradueredе ring $\mathfrak{G}(R)$</u>

Antag $\mathfrak{M} = (m_1,\ldots,m_\nu)$, da er $\mathfrak{M}^n = (\ldots,m_1^{a_1}\ldots m_\nu^{a_\nu},\ldots)$. Vi sætter $\mathfrak{R} = R/\mathfrak{M}[X_1,\ldots,X_\nu] = K[X_1,\ldots,X_\nu]$, og har altså

$$\begin{array}{ccc} \mathfrak{R} & = & \mathfrak{R}_0 \oplus \mathfrak{R}_1 \oplus \ldots \\ & & \downarrow \quad\quad \downarrow \\ \mathfrak{G}(R) & = & R/\mathfrak{M} \oplus \mathfrak{M}/\mathfrak{M}^2 \oplus \cdots \end{array}$$

Afbildningen $\varphi : \mathcal{R} \to \mathcal{G}(R)$ defineret komponentvis ved $\varphi_0(\textcircled{a}) = \textcircled{a} \in R/\mathcal{M}$, $\varphi_1(\textcircled{a_1}X_1 + \ldots + \textcircled{a_\nu}X_\nu) = (a_1 m_1 + \ldots + a_\nu m_\nu) \in \mathcal{M}/\mathcal{M}^2$ osv er en veldefineret surjektiv homomorfi, så $\operatorname{Ker}\varphi = \mathcal{J}$ er et ideal i $\mathcal{R}$, og endda homogent. Følgelig er $\dim_K \mathcal{M}^n/\mathcal{M}^{n+1} = \dim_K \mathcal{R}_n/\mathcal{R}_n \cap \mathcal{J}$ = pol. i n for store n.
Det viser sig, at $\ell(R/\mathcal{M}^n)$ = d'tegradspol. i n for store n = $e(\mathcal{M})n^d + \ldots$. og $e(\mathcal{M})$ kaldes R's (eller $\mathcal{M}$'s) <u>multiplicitet</u>, og at $\ell(R/\mathcal{O}_f^n) = e(\mathcal{O}_f)n^d + \ldots$., hvor $e(\mathcal{O}_f)$ kaldes $\mathcal{O}_f$'s multiplicitet. [d = dim R = h($\mathcal{M}$) = mindste antal elementer, der frembringer et $\mathcal{M}$-primært ideal].

Vi har tidligere set, at $\dim_{R/\mathcal{M}}(\mathcal{M}/\mathcal{M}^2) \geq d = \dim R$. En lokal Noethersk ring kaldes en <u>regulær lokal ring</u>, hvis $\dim_{R/\mathcal{M}}(\mathcal{M}/\mathcal{M}^2) = \dim R = d$.

Følgende betingelser er ækvivalente i en lokal Noethersk ring:

1) $\mathcal{M}$ kan frembringes af d elementer
2) R er regulær lokal
3) Den til R hørende graduerede ring $\mathcal{G}(R)$ er isomorf med $R[X_1, \ldots, X_d]$.

Bemærk, at 1) $\Leftrightarrow$ 2) er oplagt.

ø Eks. <u>d = 0</u>. R er regulær lokal $\Leftrightarrow$ R er et legeme, er oplagt.

Eks. <u>d = 1.</u> R er regulær lokal $\Leftrightarrow$ R er et P.I.D., thi "$\Leftarrow$" er oplagt, og "$\Leftarrow$": 1) viser, at $\mathcal{M} = (\pi)$. Nu findes til $\mathcal{O} \neq R,(0)$, et n, så $\mathcal{O} \subseteq \mathcal{M}^n$, men $\mathcal{O} \not\subseteq \mathcal{M}^{n+1}$ [da $\bigcap \mathcal{M}^\nu = (0)$], altså et $a \in \mathcal{M}^n = (\pi^n)$, men $a \notin (\pi^{n+1})$, d: $a = r\pi^n$, $r \notin (\pi)$, men så er r enhed d: $\pi^n = r^{-1}a \in \mathcal{O}$, altså $\mathcal{O} = \mathcal{M}^n = (\pi^n)$. Endvidere er R int.omr. thi er $a = \varepsilon\pi^n$ en nuldivisor, $0 = ab = \varepsilon\varepsilon'\pi^{n+n'}$, da er $\pi^{n+n'} = 0$ og dermed $\mathcal{M}^{n+n'} = (0)$, så (0) er $\mathcal{M}$-primært i modstrid med at dim R = 1.

Eks. Lad $V \subseteq \mathcal{A}_n(K)$ være en irreducibel varietet; $\mathcal{F}(V) = (f_1, \ldots, f_\nu)$ er da et primideal. Et punkt $\underline{\alpha} \in V$ kaldes simpelt, hhvis $\operatorname{rg}\left\{\frac{\partial f_i(\alpha)}{\partial x_j}\right\} = n - \dim V$. Man kan vise, at $\underline{\alpha}$ er simpel $\Leftrightarrow$ Den geom.lok.ring for V i $\underline{\alpha}$ er regulær.

Man kan vise: R regulær $\Rightarrow$ R er int.omr.
R regulær $\Rightarrow$ R er helt afsluttet
R regulær $\Rightarrow$ $e(\mathcal{M}) = 1$
R regulær $\Rightarrow$ $d(\varphi) + h(\varphi) = d$.

Ved som basis for omegnene af 0 at tage $\mathfrak{M}^n$, $n \in \mathbb{N}$, defineres den $\mathfrak{M}$-adiske topologi i R. Ethvert R har et fuldstændigt hylster $\overline{R}$, der igen er lokalt, og for hvilket $\overline{\mathfrak{M}} \cap R = \mathfrak{M}$, ogder gælder:

$$R \text{ regulær} \iff \overline{R} \text{ er regulær.}$$

Sætning (I.S.Cohen 1946). Hvis R er reguæær lokal af dim R = d og fuldstændig, og Kar R = Kar $R/\mathfrak{M}$, da er $R \cong R/\mathfrak{M}[[X_1,\ldots,X_d]]$.

En R-modul M har homologisk dimmension dh(M) = n, hvis der findes en projektiv resolution

$$\cdots \longrightarrow 0 \longrightarrow 0 \longrightarrow P_n \longrightarrow P_{n-1} \longrightarrow \cdots \longrightarrow P_0 \longrightarrow M,$$

og hvis der ikke findes nogen "mindre".
R har global dimmension gl.dim.R = n, hvis $n = \sup_M \mathrm{dh}(M)$.

Sætning (J.-P. Serre 1955). Hvis R er lokal Noethersk, da er gl.dim.R $< \infty \iff$ R er regulær, og i bekræftende fald er gl.dim.R = dim R.

$$R \text{ regulær lokal} \Longrightarrow R_{\mathfrak{P}} \text{ er regulær.}$$

Sætning. Hvis R er regulær lokal, da er R et U.F.D.
Krull viste et specialtilfælde. Nagata (1958) viste: rigtig for d = 3 $\Longrightarrow$ rigtig for afle d. Auslander & Buchsbaum (1960) viste: rigtig for d = 3.

KAPITEL VIII DEDEKIND RINGE.

I det følgende betegner R et int.omr. med kvot.legemet K.

Ved et (bruddent) ideal i R FOrstås en R-modul $\mathcal{a}$, $(0) \neq \mathcal{a} \subsetneq K$, for hvilken der findes et $d \in R\setminus(0)$, så at $d\mathcal{a} \subseteq R$. $d\mathcal{a}$ er da et sædvanligt "helt" ideal. For brudne idealer $\mathcal{a}, \mathcal{b}$, er - med oplagte definitioner - $\mathcal{a}+\mathcal{b}$, $\mathcal{a}\cap\mathcal{b}$ og $\mathcal{a}\mathcal{b}$ igen idealer.

$\mathcal{a}$ kaldes endeligt frembragt, hvis der findes $k_1,\ldots,k_m \in K$, så $\mathcal{a} = Rk_1+\ldots+Rk_m = (k_1,\ldots,k_m)$.
Hvis R er P.I.D. er samtlige idealer hovedidealer, og hvis R er Noethersk er samtlige idealer endeligt frembragt.

($\{$brudne idealer$\}$, $\cdot$) ses let af danne en halvgruppe, $\mathcal{F}$, med R som neutralt element.
$\mathcal{a}$ kaldes <u>invertibelt</u>, hvis $\mathcal{a}$ er regulært i $\mathcal{F}$.

Eks. Et hovedideal er invertibelt.

Sætning. <u>Et helt ideal $\mathcal{a} \neq (0)$ er invertibelt $\Leftrightarrow$ der findes et helt ideal $\mathcal{b} \neq (0)$, så at $\mathcal{a}\mathcal{b}$ = hvodeideal.</u>
Bevis. Oplagt!

Sætning. <u>Et invertibelt ideal er endeligt frembragt.</u>
Bevis. Af $\mathcal{a}\mathcal{a}' = R$ følger $1 = \sum_1^m a_i a_i'$, $a_i \in \mathcal{a}$, $a_i' \in \mathcal{a}'$. Nu er $(a_1,\ldots,a_m) \subseteq \mathcal{a}$, og for $a \in \mathcal{a}$ er $aa' \in R$, så $a = \sum_1^m (aa_i')a_i \in (a_1,\ldots,a_m)$. ∎

Sætning. <u>Hvis R er lokal, da er hvert invertibelt ideal et hovedideal.</u>
Bevis. Vi har $\mathcal{a} = (a_1,\ldots,a_m)$ iflg den foregående sætn. Induktion efter n: <u>n = 1.</u> færdige. n = 2. Af $(a_1,a_2)\,\mathcal{a}' = R$ fås $1 = a_1a_1'+a_2a_2'$, og da $a_1a_1' \in R$ og $a_2a_2' \in R$, må mindst et af disse, fx a_1a_1' være en enhed, altså $a_1a_1'r = 1$, men så er $a_2 = a_1a_1'ra_2$ $\Rightarrow$: $a_2 \in (a_1)$. <u>n-1 $\rightarrow$ n.</u> Af $(a_1,\ldots,a_m)\,\mathcal{a}' = R$ følger $1 = \sum_i a_ia_i'$, og $a_ia_i' \in R$ medfører, at fx. a_1a_1' er enhed, altså $a_1a_1'r = 1$, men så er $a_2 = a_1a_1'ra_2 \in (a_1)$, $\mathcal{a} = (a_1,a_3,\ldots,a_m)$

Opg. Hvis R er U.F.D., da er hvert invertibelt ideal et hovedideal. Vi har $\mathcal{a} = (a_1,\ldots,a_m)$, hvoraf $1 = a_1a_1'+\ldots+a_ma_m'$. Nu er $\mathcal{b} = \bigcap_1^m (a_i'^{-1})$ et hxovedideal, da R er U.F.D., og $\mathcal{a} = \mathcal{b}$, thi $\subseteq$ er oplagt, da $aa_i' \in R$ medfører $a \in (a_i'^{-1})$ for alle $a \in \mathcal{a}$, og "$\supseteq$": thi for $x \in \mathcal{b}$, er $x = \frac{n_i}{a_i}$, i = 1,...,n, altså $x = \sum_1^m a_ia_i'x = \sum a_ir_i \in \mathcal{a}$.

Eks. $\mathcal{A}$ er invertibelt $\Leftrightarrow$ $\mathcal{A}$ er projektiv R-modul

Lemma 1. Hvis et produkt $\mathcal{A}_1 \dots \mathcal{A}_m$ er invertibelt, da er hvert $\mathcal{A}_j$ også invertibelt.
oplagt.

Lemma 2. Hvis $\mathcal{A}$ er et prokukt af invertible primidealer, da er dette $\mathcal{A}$'s eneste fremstilling som prokukt af primidealer.
Bevis. Lad $\mathcal{A} = \mathfrak{p}_1 \dots \mathfrak{p}_m$ invertible primidealer, og $\mathcal{A} = \mathfrak{q}_1 \dots \mathfrak{q}_n$ primidealer. Er $\mathfrak{p}_1$ et mindste blandt $\{\mathfrak{p}_j\}$ vil $\mathfrak{p}_1 \supseteq \mathcal{A} = \mathfrak{q}_1 \dots \mathfrak{q}_n$ og dermed $\mathfrak{p}_1 \supseteq \mathfrak{q}_j$, og analogt vil $\mathfrak{q}_j \supseteq \mathfrak{p}_i$, min af $\mathfrak{p}_1 \supseteq \mathfrak{q}_j \supseteq \mathfrak{p}_i$ fås $\mathfrak{p}_1 = \mathfrak{q}_j$ ($= \mathfrak{p}_i$), fx $\mathfrak{p}_1 = \mathfrak{q}_1$, men så er $\mathfrak{p}_2 \dots \mathfrak{p}_m = \mathfrak{p}_1^{-1}\mathcal{A}$ $= \mathfrak{q}_2 \dots \mathfrak{q}_n$, og påstanden følger ved induktion. ∎

Hovedsætning. I et integritetsområde R er flg. bet. ækvivalente:

Ⓐ
i) R er Noethersk
ii) Ethvert ikke-trivielt primideal er maximalt
iii) R er helt afsluttet (i K).

Ⓓ Ethvert helt ideal kan (entydigt) skrives som produkt af primidealer.

Ⓖ Ethvert ideal $\neq (0)$ er invertibelt o: $\mathcal{F}$ er en gruppe.

Ⓛ
i) R er Noethersk
ii) $R_{\mathfrak{m}}$ er P.I.D. for alle maximalidealer $\mathfrak{m}$ i R.

og ringen kaldes da en Dedekindring.

Forbemærkning. Betingelserne A i,ii,iii er uafhængige: Eks. på i, ¬ii,iii: $R = K[X,Y]$. Oplagt! Eks. på i,ii, ¬iii: $R = \dot{Z}[\sqrt{-3}]$. i, da $R \cong \dot{Z}[X]/(X^2+3)$. ii, thi er $a+b\sqrt{-3} \in \mathfrak{p} \setminus (0)$ og sættes $N = a^2+3b^3 = (a+b\sqrt{-3})(a-b\sqrt{-3}) \in \mathfrak{p}$, da har vi en kannonisk surjektiv homomorfi $R/(N) \longrightarrow R/\mathfrak{p}$, og da $R/(N)$ er endelige, er også $R/\mathfrak{p}$ endelig o: et legeme, så $\mathfrak{p}$ er maximalt. ¬iii, har vi set (p.V,12,eks.). Eks. på ¬i,ii,iii: Lad K være legemet af alg. tal, og R ringen af helt alg. tal over $\dot{Z}$. ¬i, thi $(\sqrt{2}) \subsetneq (\sqrt[4]{2}) \subsetneq (\sqrt[8]{2}) \subsetneq \dots$ og her må $\subset$ gælde, thi var fx. $(\sqrt{2}) = (\sqrt[4]{2})$ ville $\sqrt[4]{2} = \sqrt{2}r$, $r \in R$, men $r = \frac{1}{\sqrt[4]{2}}$, så $\mathrm{Irr}(\frac{1}{\sqrt[4]{2}}, \dot{Q}) = X^4 - \frac{1}{2} \notin \dot{Z}[X]$ viser, at $r \notin R$. ii: R er hel over $\dot{Z}$. Lad $\mathfrak{p} \neq (0)$, $\mathfrak{p} \subsetneq R$, da er $\mathfrak{p} \cap Z = (p)$ maximalt, så for $\mathfrak{p} \subseteq \mathfrak{m} \subset R$ har vi $\mathfrak{m} \cap \dot{Z} = (p)$, men da (p) er minimalt, vil $\mathfrak{m}$ være minimalt iflg. Going-up, altså $\mathfrak{p} = \mathfrak{m}$ er maximalt. iii er oplagt.

Bemærk. Man kan vise, at bet. L i,ii er uafhængige.

Bevis. for hovedsætningen. Ⓐ $\Rightarrow$ Ⓓ er vist (p.V,14). Ⓓ $\Rightarrow$ Ⓖ:

Vi viser, at Ⓓ ÷(entydighed) ⇒ Ⓖ [Efter beviset for hovedsætningen får vi da følgende Tilføjelse (Matusita 1944). Entydigheden i D er overflødig.] Først et

Lemma. D ÷(entydighed) ⇒ Et invertibelt primideal er maximalt.
Bevis. Lad $(0) \subset \mathfrak{p} \subset R$, og $a \in R \setminus \mathfrak{p}$, da skal vi vise, at $\mathfrak{p}+(a) = R$. Nu er $\mathfrak{p}+(a) = \mathfrak{p}_1 \dots \mathfrak{p}_m$, $\mathfrak{p}+(a^2) = \mathfrak{o}_1 \dots \mathfrak{o}_m$ hvor $\mathfrak{p}_i, \mathfrak{o}_j$ er primidealer (der $\supseteq \mathfrak{p}$). Ved overgang til $R/\mathfrak{p}$ fås

$$(\textcircled{a}) = (\mathfrak{p}_1/\mathfrak{p}) \dots (\mathfrak{p}_m/\mathfrak{p}) \quad , \quad (\textcircled{a^2}) = (\mathfrak{o}_1/\mathfrak{p}) \dots (\mathfrak{o}_m/\mathfrak{p}),$$

hvor $\mathfrak{p}_i/\mathfrak{p}$, $\mathfrak{o}_j/\mathfrak{p}$ er primidealer i integritetsområdet $R/\mathfrak{p}$. Vi har $(\textcircled{a^2}) = (\textcircled{a})^2 = (\mathfrak{p}_1/\mathfrak{p})^2 \dots (\mathfrak{p}_m/\mathfrak{p})^2 = \mathfrak{o}_1/\mathfrak{p} \dots \mathfrak{o}_m/\mathfrak{p}$. Da hovedidealet $(\textcircled{a^2})$ er invertibelt, følger det af lemma 1 og 2, at $n = 2m$, og efter omnummerering: $\mathfrak{p}_{2i-1}/\mathfrak{p} = \mathfrak{p}_{2i}/\mathfrak{p} = \mathfrak{o}_i/\mathfrak{p}$, $i = 1,\dots,m$, og dermed også $\mathfrak{p}_{2i-1} = \mathfrak{p}_{2i} = \mathfrak{o}_i$, men så er

$$[\mathfrak{p}+(a)]^2 = \mathfrak{p}_1^2 \dots \mathfrak{p}_m^2 = \mathfrak{o}_1 \dots \mathfrak{o}_m = \mathfrak{p}+(a^2).$$

Specielt er $\mathfrak{p} \subseteq \mathfrak{p}+(a^2) = [\mathfrak{p}+(a)]^2 \subseteq \mathfrak{p}^2+(a)$. For $p \in \mathfrak{p}$, har vi altså $p = z+ra$, hvor $z \in \mathfrak{p}^2$, så $ra = p-z \in \mathfrak{p}$, hvoraf $r \in \mathfrak{p}$, da $a \notin \mathfrak{p}$ altså $p \in \mathfrak{p}^2+\mathfrak{p}(a)$. Da den omvendte inklusion er triviel, følger det, at $\mathfrak{p} = \mathfrak{p}^2+\mathfrak{p}(a) = \mathfrak{p}(\mathfrak{p}+(a))$.
Da $\mathfrak{p}$ vær invertibelt, er altså $\mathfrak{p}+(a) = R$. ∎

Lad nu $\mathfrak{p} \neq (0)$ være et vilk. primideal, og lad $(0) \subsetneq (b) \subseteq \mathfrak{p}$. Vi har $(b) = \mathfrak{p}_1 \dots \mathfrak{p}_s$ invertible primidealer, og derfor maximalidealer ifl. lemma, og af $\mathfrak{p} \supseteq (b) = \mathfrak{p}_1 \dots \mathfrak{p}_s$ fås $\mathfrak{p} \supseteq \mathfrak{p}_j$, d: $\mathfrak{p} = \mathfrak{p}_j$ invertibelt.
Nu er ethvert helt ideal $\mathfrak{o} = \mathfrak{p}_1 \dots \mathfrak{p}_s$ invertibelt, men så er også ethvert brudden ideal invertibelt. ∎

Ⓖ ⇒ Ⓛ: i) R er Noethersk iflg. sætningen om at hvert invert. ideal er endeligt frembragt. ii) Ethvert ideal i $R_{\mathfrak{M}}$ er udvidelsen af sin kontraktion, altså af formen $\mathfrak{o}R_{\mathfrak{M}}$. Af $\mathfrak{o}\mathfrak{o}^{-1} = R$ følger nu $(\mathfrak{o}R_{\mathfrak{M}})(\mathfrak{o}^{-1}R_{\mathfrak{M}}) = \mathfrak{o}\mathfrak{o}^{-1}R_{\mathfrak{M}} = RR_{\mathfrak{M}} = R_{\mathfrak{M}}$, så $\mathfrak{o}R_{\mathfrak{M}}$ er invert. Men vi har vist, at i et lokalt int.omr. er ethvert invert. ideal et hovedideal ∎

Ⓛ ⇒ Ⓐ: i) er givet. ii) Indirekte: Af $(0) \subset \mathfrak{p} \subset \mathfrak{M} \subset R$ følger $(0) \subset \mathfrak{p}R_{\mathfrak{M}} \subset \mathfrak{M}R_{\mathfrak{M}} \subset R$, og da $\mathfrak{p}R_{\mathfrak{M}}$ er primideal og $R_{\mathfrak{M}}$ er P.I.D., er dette en modstrid. iii) $R_{\mathfrak{M}}$ P.I.D. ⇒ $R_{\mathfrak{M}}$ U.F.D. ⇒ $R_{\mathfrak{M}}$ er helt afsluttet ⇒ (p.V,13) R er helt afsluttet. ∎

Lille morsomhed. Hvis blot ethvert primideal er invert., da er R en Dedekind ring. Vi viser Ⓛ: Foruds. ⇒ Ethvert primideal er endl.frembragt ⇒ (p.V,9) R er Noethersk, og Foruds. ⇒ $\mathfrak{M}$ invert. ⇒ $\mathfrak{M}R_{\mathfrak{M}}$ er inv. ⇒ $\mathfrak{M}R_{\mathfrak{M}}$ hovedideal ⇒ $R_{\mathfrak{M}}$ er P.I.D. (da lokal).

Eks. Af opgaven p.VIII,1 følger: R er P.I.D. $\Leftrightarrow$ R er Dedekind og U.F.D.

Sætning. Lad R være en Dedekind ring, da kan hvert bruddent ideal $\mathcal{a} \neq (0)$ entydigt skrives

$$\mathcal{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{w_{\mathfrak{p}}(\mathcal{a})}, \quad w_{\mathfrak{p}}(\mathcal{a}) \in \mathbb{Z},$$

hvor $w_{\mathfrak{p}}(\mathcal{a}) = 0$ for næsten alle $\mathfrak{p}$.

(2). $\mathcal{a}$ er helt ideal $\Leftrightarrow w_{\mathfrak{p}}(\mathcal{a}) \geq 0$

(3). $\mathcal{a} \subseteq \mathcal{b} \Leftrightarrow w_{\mathfrak{p}}(\mathcal{a}) \geq w_{\mathfrak{p}}(\mathcal{b})$

(4). $w_{\mathfrak{p}}(\mathcal{a}+\mathcal{b}) = \min\{w_{\mathfrak{p}}(\mathcal{a}), w_{\mathfrak{p}}(\mathcal{b})\}$

(5). $w_{\mathfrak{p}}(\mathcal{a} \cap \mathcal{b}) = \max\{w_{\mathfrak{p}}(\mathcal{a}), w_{\mathfrak{p}}(\mathcal{b})\}$

(6). $w_{\mathfrak{p}}(\mathcal{a}\mathcal{b}) = w_{\mathfrak{p}}(\mathcal{a}) + w_{\mathfrak{p}}(\mathcal{b})$

Bevis. Et bruddent ideal $\mathcal{a}$ kan skrives $\mathcal{a} = \mathcal{b}\mathcal{c}^{-1}$, hvor $\mathcal{b}, \mathcal{c}$ er hele, så eksistens af opspaltningen er oplagt. Entydigheden følger nu ved brug af entydigheden for hele idealer. (2) er oplagt. (3). Vi har $\mathcal{a} \subseteq \mathcal{b} \Leftrightarrow \mathcal{b}^{-1}\mathcal{a} \subseteq \mathcal{b}^{-1}\mathcal{b} = R \Leftrightarrow w_{\mathfrak{p}}(\mathcal{b}^{-1}\mathcal{a}) \geq 0$ $\Leftrightarrow w_{\mathfrak{p}}(\mathcal{a}) \geq w_{\mathfrak{p}}(\mathcal{b})$. (4) og (5) følger heraf, og (6) er trivielt. ∎

Vi skriver $\mathcal{a} \mid \mathcal{b}$, hvis der findes et helt ideal $\mathcal{c}$, så $\mathcal{a}\mathcal{c} = \mathcal{b}$. Det er kalrt, at $\mathcal{a} \mid \mathcal{b} \Leftrightarrow w_{\mathfrak{p}}(\mathcal{a}) \leq w_{\mathfrak{p}}(\mathcal{b})$, altså $\Leftrightarrow \mathcal{b} \subseteq \mathcal{a}$.

Sætning.(jfr. sædv. talteori). Kongruensen $ax \equiv b \ (\mathcal{c})$ har en løsning $\Leftrightarrow (\mathcal{c},(a)) \mid (b)$.

thi begge er ensbet. med $b \in \mathcal{c} + (a)$ ∎

En nødvendig betingelse for at et system af kongruenser

$$x \equiv b_1 \ (\mathcal{a}_1), \ \ldots, \ x \equiv b_m \ (\mathcal{a}_m)$$

hær en læsning er øjensynlig, at de såkaldte forenelighedsbet.

$$b_i - b_j = b_i - x + x - b_j \in \mathcal{a}_i + \mathcal{a}_j$$

er opfyldt. Hvis disse bet. er tilstrækkelige (for alle n) siges k.r.s. (kinesiske restklassesætning) at gælde. For n = 2 er forenelighedsbetingelserne altid tilstrækkelige, thi er $b_1 - b_2 = a_1 + a_2$, og sættes $x = b_1 - a_1 = b_2 + a_2$ vil $x \equiv b_1 \ (\mathcal{a}_1)$ og $x \equiv b_2 \ (\mathcal{a}_2)$.

Eks. $R = \mathbb{Z}[t]$. $x \equiv 0 \ (2)$, $x \equiv 0 \ (t)$, $x \equiv 2 \ (t-2)$, opfylder forenelighedsbet., men har ingen løsning, thi af 1. og 2. kongr. følger, at $4 \mid x(2)$, og af 3. kongruens følger $x(2) = 2$.

Sætning. I en kommutativ ring er flg. bet. ækvivalente:

1) $(\mathcal{a}+\mathcal{b}) \cap \mathcal{c} = (\mathcal{a} \cap \mathcal{c}) + (\mathcal{b} \cap \mathcal{c})$

2) $\mathfrak{a}+(\mathfrak{b}\cap\mathfrak{c}) = (\mathfrak{a}+\mathfrak{b})\cap(\mathfrak{a}+\mathfrak{c})$.

3) k.r.s.

Bevis. 1) $\Rightarrow$ 2): $(\mathfrak{a}+\mathfrak{b})\cap(\mathfrak{a}+\mathfrak{c}) = [\mathfrak{a}\cap(\mathfrak{a}+\mathfrak{c})] + [\mathfrak{b}\cap(\mathfrak{a}+\mathfrak{c})]$
$= \mathfrak{a} + \mathfrak{a}\cap\mathfrak{c} + \mathfrak{b}\cap\mathfrak{a} + \mathfrak{b}\cap\mathfrak{c} = \mathfrak{a} + (\mathfrak{b}\cap\mathfrak{c})$.

2) $\Rightarrow$ 3). Induktion efter n. n = 2 er vist. n-1 $\rightarrow$ n. Betragt

$$x \equiv b_1 \ (\mathfrak{a}_1), \ldots, x \equiv b_n \ (\mathfrak{a}_n), \quad \text{hvor } b_i - b_j \in \mathfrak{a}_i + \mathfrak{a}_j,$$

og lad c være en løsning til de n-1 første ligninger, altså

$$c \equiv b_i \ (\mathfrak{a}_i), \ i = 1, \ldots, n-1.$$

Nu har systemet

$$x \equiv c \ (\textstyle\bigcap_1^{n-1}\mathfrak{a}_i), \ x \equiv b_n \ (\mathfrak{a}_n),$$

en løsning, thi da $c-b_n = c-b_i+b_i-b_n \in \mathfrak{a}_i+\mathfrak{a}_n$, er (iflg. 2): $c-b_n \in \bigcap_1^{n-1}(\mathfrak{a}_i+\mathfrak{a}_n) = (\bigcap_1^{n-1}\mathfrak{a}_i)+\mathfrak{a}_n$, ɔ: forenelighedsbet. er opfyldt.

3) $\Rightarrow$ 1): "$\supseteq$" er trivielt. "$\subseteq$": At skrive $c \in (\mathfrak{a}+\mathfrak{b})\cap\mathfrak{c}$ på formen c = x+y, hvor $x \in \mathfrak{a}\cap\mathfrak{c}$ og $y \in \mathfrak{b}\cap\mathfrak{c}$ er ensbetydende med at finde $x \equiv 0 \ (\mathfrak{a})$, $x \equiv c \ (\mathfrak{b})$, $x \equiv c \ (\mathfrak{c})$, og her findes en løsning, da forenelighedsbetingelserne er opfyldt, og da er $c = x+(c-x) \in (\mathfrak{a}\cap\mathfrak{c}) + (\mathfrak{b}\cap\mathfrak{c})$ ∎

Af beviset for 3) $\Rightarrow$ 1) fremgår:

Korollar. 3): k.r.s. $\Leftrightarrow$ 3'): k.r.s. gælder for n = 3.

Sætning. Lad R være et Noethersk område, da er R dedekind $\Leftrightarrow$ k.r.s. gælder i R.

Bevis. "$\Rightarrow$" (Første bevis). Da max{ , } og min{ , } er distributive m.h.t. "hinanden", er $w_\varphi((\mathfrak{a}+\mathfrak{b})\cap\mathfrak{c}) = w_\varphi((\mathfrak{a}\cap\mathfrak{c})+(\mathfrak{b}\cap\mathfrak{c}))$ for alle φ, hvoraf ovenstående bet. 1) er opfyldt.

"$\Rightarrow$"(Andet bevis) Da $R_\mathfrak{M}$ er et lokalt P.I.D., er idealerne i $R_\mathfrak{M}$ fuldstændigt ordnet (de er jo $R_\mathfrak{M} \supsetneq \mathfrak{M}R_\mathfrak{M} \supsetneq \mathfrak{M}^2R_\mathfrak{M} \supsetneq \ldots \supseteq (0)$), så $\tilde{\mathfrak{a}}+\tilde{\mathfrak{b}} = \tilde{\mathfrak{a}}\cup\tilde{\mathfrak{b}}$ for idealer i $R_\mathfrak{M}$. Idet vi udvider og kontraherer for alle $\mathfrak{M}$ og udnytter, at $\cup$, $\cap$ er distributive m.h.t. hin. kan vi fx. vise bet. 1)

"$\Leftarrow$" Vi viser (L), og skal altså vise, at $R_\mathfrak{M}$ er P.I.D. for alle $\mathfrak{M}$. Vi bemærker først, at ideallatticet i $R_\mathfrak{M}$ er distributivt, da dette gælder for latticet i R, og da hvert ideal i $R_\mathfrak{M}$ er udvidelse af sin kontraktion. Det er nok at vise, at $R_\mathfrak{M}$ er en valuationsring(jfr. V,13,eks.). Lad altså $a,b \in R_\mathfrak{M}\setminus(0)$, da har vi $(a) = [(a-b)+(b)]\cap(a) = [(a-b)\cap(a)] + [(b)\cap(a)]$, så $a = (a-b)x+ay$, hvor $(a-b)x \in (a)$ og $ay \in (b)$ ɔ: $a \mid bx$ og $b \mid ay$. Hvis x er enhed, vil $a \mid b$, og hvis y er enhed vil $b \mid a$, og hvis både x,y er ikkeenheder, vil 1-x-y være en enhed, så at $a(1-x-y) = -bx$ medfører, at $b \mid a$. ∎

Sætning. Lad R være et Noethersk område, da er R Dedekind $\Leftrightarrow$ For-

kortningsregelen gælder for hele idealer.

Bevis. "$\Rightarrow$" iflg. (G). "$\Leftarrow$" Vi viser (L) = Det er tilstrækkeligt at vise, at hvert ideal i $R_{\mathfrak{M}}$ frembragt af 2 elementer er invertibelt, thi et sådant er da et hovedideal, og dermed også alle e.f. (d.v.s.)alle) idealer hovedidealer. Vi kan øjensynlig nøjes med at betragte idealer af formen $aR + bR = (a,b)$, hvor $a,b \in R\setminus(0)$. Vi har $(a,b)(a^2,b^2) = (a,b)(a^2,ab,b^2)$, hvoraf $(a^2,b^2) = (a^2,ab,b^2)$. Specielt er $ab = a^2x+b^2y$. Vi har

$$(a,b)(ax,by) = (a^2x,aby,abx,b^2y) \supseteq (ab)$$

og vi er færdige, når vi har vist = (jfr. p.VIII,1). Hertil skal vi vise, at $ab \mid a^2x$ og $ab \mid b^2y$ d: $b \mid ax$ og $a \mid by$. Nu er $(ax)(a,b) = (a^2x,abx) = (ab-b^2y,abx) \subseteq (ab,b^2) = (b)(a,b)$, og dermed $(ax,b)(a,b) = (b)(a,b)$, hvoraf $(ax,b) = (b)$, altså $b \mid ax$. Analogt ses, at $a \mid by$. ∎

Sætning. Lad R være en Dedekind ring, og $(0) \neq \mathcal{A} \subseteq \mathcal{B}$ være hele idealer, da findes $d \in \mathcal{B}$, så at $\mathcal{A}+(d) = \mathcal{B}$.

Bevis. Lad $\mathcal{A} = \mathfrak{p}_1^{\alpha_1} \dots \mathfrak{p}_m^{\alpha_m}$, $\mathcal{B} = \mathfrak{p}_1^{\beta_1} \dots \mathfrak{p}_n^{\beta_n}$, hvor altså $0 \leq \beta_i \leq \alpha_i$ $i = 1,\dots,n$. Nu sættes $\mathcal{C}_1 = \mathfrak{p}_1^{\beta_1}\mathfrak{p}_2^{\beta_2+1} \dots \mathfrak{p}_m^{\beta_m+1}, \dots, \mathcal{C}_m = \mathfrak{p}_1^{\beta_1+1} \dots \mathfrak{p}_{m-1}^{\beta_{m-1}+1}\mathfrak{p}_m^{\beta_m}$, og $\mathcal{C} = \mathfrak{p}_1^{\beta_1+1} \dots \mathfrak{p}_n^{\beta_n+1}$. Det ses, at $\mathcal{C} \subset \mathcal{C}_i$, så vi kan vælge $d_i \in \mathcal{C}_i \setminus \mathcal{C}$. Vi har $d_i \equiv 0 \ (\mathfrak{p}_i^{\beta_i})$, $d_i \equiv 0 \ (\mathfrak{p}_j^{\beta_j+1})$, $j \neq i$, og $d_i \not\equiv 0 \ (\mathfrak{p}_i^{\beta_i+1})$. Vi sætter $d = d_1+\dots+d_m$, da er $d \equiv 0 \ (\mathfrak{p}_i^{\beta_i})$, $d \not\equiv 0 \ (\mathfrak{p}_i^{\beta_i+1})$, altså $(d) = \mathfrak{p}_1^{\beta_1} \dots \mathfrak{p}_m^{\beta_m}\mathfrak{b}$, hvor $\mathfrak{p}_i \nmid \mathfrak{b}$. Nu er imidlertid $\mathcal{A}+(d) = (\mathcal{A},(d)) = (\mathfrak{p}_1^{\alpha_1} \dots \mathfrak{p}_m^{\alpha_m}, \mathfrak{p}_1^{\beta_1} \dots \mathfrak{p}_m^{\beta_m}\mathfrak{b}) = \mathfrak{p}_1^{\beta_1} \dots \mathfrak{p}_m^{\beta_m} = \mathcal{B}$. ∎

Korollar 1. Hvis $\mathcal{A} \neq (0)$, da er $R/\mathcal{A}$ et P.I.R.

Bevis. Idealerne i $R/\mathcal{A}$ er af formen $\mathcal{B}/\mathcal{A} = ((d))$. ∎

R int.omn.

Eks. R er Dedekind ring $\Leftrightarrow$ $R/\mathcal{A}$ er P.I.R. for $\neq (0)$

Bevis. "$\Rightarrow$" iflg. Korollar 1. "$\Leftarrow$". R er Noethersk (jfr. p.V,4). Vi viser nu den distributive lov 1) p. VIII,4: $(\mathcal{A}+\mathfrak{b}) \cap \mathcal{C} = (\mathcal{A} \cap \mathcal{C}) + (\mathfrak{b} \cap \mathcal{C})$. Hvis $\mathcal{A}, \mathfrak{b}$ eller $\mathcal{C} = (0)$, er 1) triviel. Da (0) er et primideal, kan vi følgelig antage, at $\mathcal{A} \cap \mathfrak{b} \cap \mathcal{C} \neq (0)$. Ved overgang til $R/(d)$, hvor $0 \neq d \in \mathcal{A} \cap \mathfrak{b} \cap \mathcal{C}$, ses, at det er tilstrækkeligt at bevise 1) for $R/(d)$, men $R/(d)$ er et P.I.R., og for et sådant gælder 1), jfr. Krull's struktursætning, p .V,7.

Korollar 2. Ethvert ideal i en Dedekindring R kan frembringes af to elementer.

Korollar 3. Lad $\mathcal{C} \neq (0)$ være givet, da findes til hvert $\mathcal{A} \neq (0)$

et idela $\mathfrak{b}$, med $(\mathfrak{b},\tau)=(1)$, så at $\mathfrak{a}\mathfrak{b}$ er et hovedideal.
Bevis. Vi har $(0)\subset \mathfrak{a}\tau \subseteq \mathfrak{a}$, så $\mathfrak{a}=(\mathfrak{a}\tau,(d))$. Nu er $\mathfrak{a}\mid(d)$, så den findes $\mathfrak{b}$, så $\mathfrak{a}\mathfrak{b}=(d)$, og $\mathfrak{a}=(\mathfrak{a}\tau,\mathfrak{a}\mathfrak{b})=\mathfrak{a}(\tau,\mathfrak{b})$, hvoraf $(\mathfrak{b},\tau)=(1)$. ∎

Sætning. Lad $\mathfrak{a}=\mathfrak{p}_1^{\alpha_1}\dots\mathfrak{p}_m^{\alpha}$ være et ideal i en Dedekind ring R, da er $R/\mathfrak{a}\cong R/\mathfrak{p}_1^{\alpha_1}\oplus\dots+R/\mathfrak{p}_m^{\alpha_m}$.
Bevis. Følger straks af at $\mathfrak{p}_1,\dots,\mathfrak{p}_m$ er parvis komaximale. ∎

Sætning. Lad R være en Dedekind ring, og $\{\alpha_i\}$ et fuldst.repr.syst. for restklasserne mod. $\mathfrak{p}$, da findes $\pi\in R$ så $\mathfrak{p}\parallel(\pi)$ (iflg. korollar 3), og $\{\alpha_{i_0}+\alpha_{i_1}\pi+\dots+\alpha_{i_{m-1}}\pi^{m-1}\}$ er da et fuldst.rep.syst. for restklasserne mod. $\mathfrak{p}^m$.
Bevis. "Eksistens". Lad $a\in R$, da er $a\equiv\alpha_{i_0}\ (\mathfrak{p})$. Kongruensen $\pi x\equiv a-\alpha_{i_0}\ (\mathfrak{p}^2)$ har nu en løsning, idet $(\mathfrak{p}^2,(\pi))=\mathfrak{p}\mid(a-\alpha_0)$, og for denne løsning er $x\equiv\alpha_{i_1}\ (\mathfrak{p})$. Nu er $\pi x\equiv\pi\alpha_{i_1}\ (\mathfrak{p}^2)$, og dermed $a\equiv\alpha_{i_0}+\pi\alpha_{i_1}\ (\mathfrak{p}^2)$. Kongruensen $\pi^2x\equiv a-\alpha_{i_0}-\alpha_{i_1}\pi\ (\mathfrak{p}^3)$ har nu en løsning, idet $(\mathfrak{p}^3,(\pi^2))=\mathfrak{p}^2$ o.s.v.
"Entydighed". Hvis $\alpha_{i_0}+\alpha_{i_1}\pi+\dots+\alpha_{i_{m-1}}\pi^{m-1}\equiv\alpha_{i_0}'+\dots+\alpha_{i_{m-1}}'\pi^{m-1}\ (\mathfrak{p}^m)$, er $\alpha_{i_0}\equiv\alpha_{i_0}'\ (\mathfrak{p})$, hvoraf $\alpha_{i_0}=\alpha_{i_0}'$. Nu er $\pi(\alpha_{i_1}+\dots+\alpha_{i_{m-1}}\pi^{m-2})\equiv\pi(\alpha_{i_1}'+\dots\alpha_{i_{m-1}}'\pi^{m-2})\ (\mathfrak{p}^m)$, hvoraf $\alpha_{i_1}+\dots+\alpha_{i_{m-1}}\pi^{m-2}\equiv a_{i_1}'+\dots+\alpha_{i_{m-1}}'\pi^{m-2}\ (\mathfrak{p}^{m-1})$, o.s.v. ∎

Sætning. Lad R være en Dedekind ring med kvot.legemet K, lad L/K være en endelig separabel udvidelse, og lad $\overline{R}$ være R's helt afsluttede hylster i L, da er $\overline{R}$ en Dedekind ring, med kvot.legemet L;
[endda: Ethvert $\alpha\in L$ kan skrives $\alpha=\frac{\overline{r}}{r}$, $\overline{r}\in\overline{R}$, $r\in R$.]
Bemærk. L/K separabel er overflødigt.
Bevis. Først den sidste påstand. Lad $\alpha\in L$, da er α rod i $r_0X^m+\dots+r_m\in R[X]$, hvor $r_0\neq 0$, så $(r_0\alpha)^m+r_1(r_0\alpha)^{m-1}+\dots+r_mr_0^{m-1}=0$ d: $r_0\alpha\in\overline{R}$ eller $\alpha=\overline{r}/r_0$.
Første påstand: Vi viser Ⓐ iii: R er helt afsluttet (i L), trivielt. ii: Lad $(0)\subset\overline{\mathfrak{p}}\subset\overline{R}$, da er $\overline{\mathfrak{p}}\cap R\neq(0)$, da $\overline{R}$ er hel over R, og dermed minimalt, men så er (Going-up) $\overline{\mathfrak{p}}$ minimalt, og dermed maximalt.
i: L/K er simpel, altså $L=K(\vartheta)$, og her kan vi øjensynlig antage, at $\vartheta\in\overline{R}$. Lad nu M/L være en endelig udvidelse, så at M/K er normal (jfr. Alg. IV,6), da har vi

$$\begin{array}{ccc}\overline{R} & \subseteq & L \subseteq M \\ \cup\!| & & \cup\!| \\ R & \subseteq & K\end{array}$$

Lad $\mathrm{Irr}(\vartheta,K) = (X-\vartheta_1)\ldots(X-\vartheta_n)$, hvor $\vartheta_i \in M$, $\vartheta_i \neq \vartheta_j$, $i \neq j$, og hvor f.eks. $\vartheta_1 = \vartheta \in L$. Lad nu $\xi \in \overline{R}$; da $1,\vartheta,\ldots,\vartheta^{n-1}$ er en K-basis for L, er $\xi = a_0+a_1\vartheta+\ldots+a_{n-1}\vartheta^{n-1}$; sæt

$$(*) \quad \xi_i = a_0+a_1\vartheta_i+\ldots+a_{n-1}\vartheta_i^{n-1} \in M, \; i = 1,\ldots,n.$$

Da ϑ er hel over R, er også ϑ_i hel over R.
Nu kan isomorfien $K(\vartheta) \to K(\vartheta_i)$ fortsættes til en automorfi σ i M, med $\sigma_{|K} = \mathrm{id}_K$ (idet vi kan antage, at M er et spaltningslegeme for $\mathrm{Irr}(\vartheta,K)$), så $\sigma(\vartheta) = \vartheta_i$, men så er $\sigma(\xi) = \xi_i$, og dermed ξ_i er hel over R.
Relationerne $(*)$ kan skrives $\underline{\xi}_{|} = \underline{\underline{A}}\,\underline{a}_{|}$, hvor $\underline{\underline{A}}$ er matricen (ϑ_i^j), $i = i,..,n$ $j = 0,\ldots,n-1$. Her er $d = \det \underline{\underline{A}} =$ Van der Monde det. $= \prod_{i<j}(\vartheta_i-\vartheta_j) \neq 0$, og hel over R. Anvendes en automorfi $\sigma \in \mathrm{Gr}(M/K)$ på $\underline{\underline{A}}$ fås en permutation af rækkerne, $\sigma(d) = \sigma(\det \underline{\underline{A}}) = \det \sigma(\underline{\underline{A}}) = \pm\det \underline{\underline{A}} = \pm d$, hvoraf $\sigma(d^2) = d^2$. Følgelig er $d^2 \in K$, og hel over R, altså $d^2 \in R$. Da $\underline{\underline{A}}$ er hel over R følger det af de sædvanlige regler for dannelse af invers matrix, at $d\underline{\underline{A}}^{-1}$ er hel over R, og dermed også, at $d^2\underline{\underline{A}}^{-1}$ er hel over R. Af $\underline{\xi}_{|} = \underline{\underline{A}}\,\underline{a}_{|}$ slutter vi nu, at $d^2\underline{a}_{|} = d^2\underline{\underline{A}}^{-1}\underline{\xi}_{|}$ er hel over R (da $\underline{\xi}_{|}$ vær hel over R), og da elementerne ligger i K, må de altså ligge i R. Følgelig er

$$\xi = a_0 d^2\frac{1}{d^2} + a_1 d^2\frac{\vartheta}{d^2} + \ldots + a_{n-1} d^2\frac{\vartheta^{n-1}}{d^2} \in R\left\{\frac{1}{d^2},\ldots,\frac{\vartheta^{n-1}}{d^2}\right\}$$

Vi har således vist, at

$$\overline{R} \subseteq \text{Den fri R-modul } R\left\{\frac{1}{d^2},\ldots,\frac{\vartheta^{n-1}}{d^2}\right\}.$$

Et vilkårligt helt ideal $\overline{\mathcal{A}}$ i $\overline{R}$ er specielt en R-modul $\subseteq \overline{R} \subseteq$ endeligt frembragt fri R-modul, så $\overline{\mathcal{A}}$ er e.f. som R-modul, og derfor også e.f. som $\overline{R}$-modul. Følgelig er $\overline{R}$ Noethersk. ∎

Undervejs så vi:
Tilføjelse. <u>$\overline{R} \subseteq$ endeligt frembragt fri R-modul.</u>
en tilføjelse, der ikke gælder for inseparable udvidelser.

Eks. Lad K være alg.afsl. og V en irr.varietet af dim V = 1 i $\mathcal{A}_n(K)$, altså en kurve. $\mathcal{F}(V)$ er da et primideal i $R = K[X_1,\ldots,X_n]$. $R/\mathcal{F}(V)$ er et int.omr.(Noethersk), med de maximale idealer $\mathcal{M}_{\underline{\alpha}}/\mathcal{F}(V)$, $\underline{\alpha} \in V$. Vi har bemærket, at $\underline{\alpha} \in V$ er regulær $\Leftrightarrow$ den geom.lok.ring, $(R/\mathcal{F}(V))_{\mathcal{M}_{\underline{\alpha}}/\mathcal{F}(V)}$, for V i $\underline{\alpha}$ er et P.I.D. Vi slutter heraf:
<u>V er regulær $\Leftrightarrow$ $R/\mathcal{F}(V)$ er en Dedekind ring.</u>

KAPITEL IX ALGEBRAISK TALTEORI.

INDSKUD OM NORM OG SPOR=

Lad K/k være en endelig separabel udvidelse, og lad M/K være en endelig udvidelse af K, så at M/k er normal; sæt G = Gr(M/k), da svarer K til undergruppen H = Gr(M/K) i G.
Lad $\sigma,\tau \in G$, med $\sigma|_K = \tau|_K$, da er $\sigma^{-1}|_K \tau|_K = \mathrm{id}_K \Leftrightarrow (\sigma^{-1}\tau)|_K = \mathrm{id}_K \Leftrightarrow \sigma^{-1}\tau \in H \Leftrightarrow \tau \in \sigma H$. Lad $[K:k] = n$, og lad $G = \sigma_1 H \cup \ldots \sigma_m H$ være en repræsentation af G i sideklasser mod.H, da vil $\underline{\sigma_1,\ldots\sigma_n}$ altså give samtlige ~~xxx~~ isomorfier af K.
For $\alpha \in K$ kaldes $\sigma_1(\alpha),\ldots,\sigma_n(\alpha)$ de til α konjugerede elementer m.h.t. K/k; disse afhænger altså ikke af valget af den normale udvidelse M.
For $\alpha \in K$ sættes normen af α, $N_{K/k}(\alpha) = \prod_1^n \sigma_i(\alpha)$, og sporet af α, $S_{K/k}(\alpha) = \sum_1^n \sigma_i(\alpha)$.
Der gælder nu: $N(\alpha) \in k,\ S(\alpha) \in k.$

(1) $N(\alpha) = 0 \Leftrightarrow \alpha = 0$

(2) $N(\alpha\beta) = N(\alpha)N(\beta)$

(3) $N(a) = a^n$ for $a \in k$.

(4) $S(\alpha+\beta) = S(\alpha)+S(\beta)$

(5) $S(a\alpha) = aS(\alpha)$ for $a \in k$.

(6) $S(a) = na$ for $a \in k$,

hvilket let eftervises.

Endvidere gælder for en separabel udvidelse L/k med $L \supseteq K$, og $\alpha \in L$ Transitivitetssætning.

(7) $N_{L/k}(\alpha) = N_{K/k}(N_{L/K}(\alpha))$.

(8) $S_{L/k}(\alpha) = S_{K/k}(S_{L/K}(\alpha))$.

Bevis. Lad M/L være en endelig udvidelse, så at M/k er normal; sæt G = Gr(M/k), H = Gr(M/K) og N = Gr(M/L), da er $G \supseteq H \supseteq N \supseteq E$, svarende til $k \subseteq K \subseteq L \subseteq M$. Lad nu $G = \bigcup_\sigma \sigma H$ være en repræsentation af G i venstre-H-sideklasser, og $H = \bigcup_\tau \tau N$ er repræsentation af H i venstr-N-sideklasser, da er $G = \bigcup_{\sigma,\tau} \sigma\tau N$ er repræsentation af G i venstre-N-sideklasser, hvilket let eftervises. Og heraf følger påstanden let. ∎

Korollar. Hvis $\alpha \in K$, og $[L:K] = m$, da er

(9) $N_{L/k}(\alpha) = [N_{K/k}(\alpha)]^m$.

(10) $S_{L/k}(\alpha) = m\, S_{K/k}(\alpha)$.

Sætning. Lad $\alpha \in K$ og sæt $\mathrm{Irr}(\alpha,k) = X^m + a_1 X^{m-1} \ldots + a_m$, og $[K:k] = n$ da er

(11) $N_{K/k}(\alpha) = [(-1)^m a_m]^{n/m} = (-1)^n (a_m)^{n/m}$

(12) $S_{K/k}(\alpha) = -\frac{n}{m} a_1$.

Bevises ved at betragte $k \subseteq k(\alpha) \subseteq K$ og anvende korollar. ∎

Vi betragter i det følgende en endelig udvidelse $K/\dot{Q}$; Med R betegner vi $\dot{Z}$'s helt afluttede hylster i K, og vi sætter $n = [K:\dot{Q}]$.

$$\begin{array}{ccc} R & \subseteq & K \\ \cup\!| & & \cup\!| \\ \dot{Z} & \subseteq & \dot{Q} \end{array}$$

Nu er R en Dedekind ring; og ydermere, (da $\dot{Q}$ er fuldkomment, og $K/\dot{Q}$ altså separabel) $R \subseteq$ e.f. fri $\dot{Z}$-modul, og dermed ($\dot{Z}$ er P.I.D.): R er en e.f. fri $\dot{Z}$-modul.

Lad $\omega_1, \ldots, \omega_\nu$ være en $\dot{Z}$-basis for R, da er $\omega_1, \ldots, \omega_\nu$ en $\dot{Q}$-basis for K, hvilket let eftervises. Specielt er $\nu = n$. $(\omega_1, \ldots, \omega_n)$ kaldes en hel-tals-basis.

Vi kan gå endnu videre:

Lad $\mathcal{O}\!\!\mathcal{l} \neq (0)$ være et helt ideal i R. Da $\mathcal{O}\!\!\mathcal{l} \subseteq R \subseteq$ e.f. fri Z-modul, er $\mathcal{O}\!\!\mathcal{l}$ en e.f. fri Z-modul; lad $(\omega_1, \ldots, \omega_\nu)$ være en $\dot{Z}$-basis for $\mathcal{O}\!\!\mathcal{l}$, da er $(\omega_1, \ldots, \omega_\nu)$ en $\dot{Q}$-basis for K, thi: Vi viser først, at $\mathcal{O}\!\!\mathcal{l} \cap \dot{Z} \neq (0)$, thi er $\alpha \in \mathcal{O}\!\!\mathcal{l} \setminus (0)$, er $N(\alpha) \in \dot{Z} \setminus (0)$, $N(\alpha) = \alpha_1 \ldots \alpha_n$, hvor $\alpha = \alpha_1$, så $\alpha_2 \ldots \alpha_n = N(\alpha)/\alpha \in K$, og hel, altså $\in R$, men så er $N(\alpha) = (\alpha_2 \ldots \alpha_n)\alpha \in \mathcal{O}\!\!\mathcal{l} \cap \dot{Z}$. Lad $\xi \in K$, da er $\xi = r/s$, hvor $r \in R$, $s \in \dot{Z}$, og $\xi = r/s = rN(\alpha)/sN(\alpha) = \text{Elem.} \in \mathcal{O}\!\!\mathcal{l} / \text{Elem.} \in \dot{Z}$.

For $\alpha_1, \ldots, \alpha_n \in K$, (n elementer!) defineres diskriminanten for $(\alpha_1, \ldots, \alpha_n)$ som

$$\Delta(\alpha_1, \ldots, \alpha_n) = \begin{vmatrix} \alpha_1^{(1)} & \cdots & \alpha_1^{(n)} \\ \vdots & & \vdots \\ \alpha_n^{(1)} & \cdots & \alpha_n^{(n)} \end{vmatrix}^2 = \det(S(\alpha_i \alpha_j)) \in \dot{Q}.$$

Sætning. Lad $(\omega_1, \ldots, \omega_n)$ være en heltalsbasis for $K/\dot{Q}$, da er $d = \Delta(\omega_1, \ldots, \omega_n) \neq 0$ et for K karakteristisk tal, kaldet K's diskriminant.

For vilk. $\alpha_1, \ldots, \alpha_n \in R$ er $\Delta(\alpha_1, \ldots, \alpha_n) = k^2 d$, hvor $k \in \dot{Z}$.

$(\alpha_1, \ldots, \alpha_n)$ er heltalsbasis $\Leftrightarrow k = \pm 1$.

Bevis. Vi har $\underline{\underline{\alpha}}_1 = \underline{\underline{A}}\, \underline{\underline{\omega}}_1$, hvor $\underline{\underline{A}}$ er en $(n \times n)$-matrix fra $\dot{Z}$. Ved konjugering fås $\underline{\underline{\alpha}}_1^{(i)} = \underline{\underline{A}}\, \underline{\underline{\omega}}_1^{(i)}$, $i = 1, \ldots, n$ altså

$$\begin{Bmatrix} \alpha_1^{(1)} & \dots & \alpha_m^{(1)} \\ \vdots & & \vdots \\ \alpha_1^{(m)} & \dots & \alpha_m^{(m)} \end{Bmatrix} = \underline{\underline{A}} \begin{Bmatrix} \omega_1^{(1)} & \dots & \omega_m^{(1)} \\ \vdots & & \vdots \\ \omega_1^{(m)} & \dots & \omega_m^{(m)} \end{Bmatrix}$$

hvoraf $\Delta(\alpha_1,\dots,\alpha_m) = (\det A)^2 \Delta(\omega_1,\dots,\omega_m)$.
Nu er $(\alpha_1,\dots,\alpha_m)$ heltalsbasis $\Leftrightarrow$ $(\alpha_1,\dots,\alpha_m)$ er $\dot{Z}$-basis for $\dot{Z}$-modulen R $\Leftrightarrow$ $\underline{\underline{A}}$ er unimodulær $\Leftrightarrow$ det $\underline{\underline{A}} = \pm 1$ $\Leftrightarrow \Delta(\alpha_1,\dots,\alpha_m) = \Delta(\omega_1,\dots,\omega_m)$, idet $d \neq 0$, da vi kan angive et sæt med en fra 0 forskellig diskriminant: Vi har jø $K = \dot{Q}(\vartheta)$, hvor vi kan antage $\vartheta \in R$; nu er $\vartheta^{(1)},\dots,\vartheta^{(m)}$ rødderne i $\mathrm{Irr}(\vartheta,\dot{Q})$, altså indb.forksk. og følgelig $\Delta(1,\vartheta,\dots,\vartheta^{m-1}) = \prod_{i<j}(\vartheta^{(i)} - \vartheta^{(j)})^2 \neq 0$. ∎

Kvadratiske udvidelser

Hvis $[K:\dot{Q}] = 2$, da er $K = \dot{Q}(\sqrt{m})$, hvor $m \in \dot{Z}$ er kvadratfri. For $\alpha = a+b\sqrt{m} \in K$ er $\mathrm{Irr}(\alpha,\dot{Q}) = (X-(a+b\sqrt{m}))(X-(a-b\sqrt{m})) = X^2-2aX+(a^2-b^2m)$, $\alpha = a+b\sqrt{m}$ er hel over $\dot{Z}$ $\Leftrightarrow$ $2a \in \dot{Z}$ og $(a^2-b^2m) \in \dot{Z}$ $\Rightarrow$ $2a \in Z$ og $(2a)^2 - (2b)^2 m \in \dot{Z}$ $\Rightarrow$ $2a \in \dot{Z}$ og $2b \in \dot{Z}$ $\Rightarrow \alpha = a+b\sqrt{m} = \frac{1}{2}(a'+b'\sqrt{m})$, $a',b' \in \dot{Z}$.
Hvis (I) $m \equiv 2,3 \pmod 4$, da er α hel $\Leftrightarrow a'^2 - b'^2 m \equiv 0 \pmod 4$ $\Leftrightarrow \begin{Bmatrix}0\\1\end{Bmatrix} + \begin{Bmatrix}0\\1\end{Bmatrix}\begin{Bmatrix}2\\3\end{Bmatrix} = 0$ $\Leftrightarrow$ $a' \equiv b' \equiv 0 \pmod 2$ $\Leftrightarrow$ $\alpha = a+b\sqrt{m}$, $a,b \in \dot{Z}$. En heltalsbasis er altså $(1,\sqrt{m})$, og $d = \begin{vmatrix} 1 & 1 \\ \sqrt{m} & -\sqrt{m} \end{vmatrix}^2 = 4m$.
Hvis (II) $m \equiv 1 \pmod 4$, da er α hel $\Leftrightarrow a'^2 - b'^2 m \equiv 0 \pmod 4$ $a'^2 - b'^2 \equiv 0 \pmod 4$ $\Leftrightarrow a'-b' \equiv 0 \pmod 2$ $\Leftrightarrow \alpha = \frac{1}{2}(a'+b'\sqrt{m}) = \frac{1}{2}(a'-b')+b'\frac{1+\sqrt{m}}{2} = a_1+b_1\cdot\frac{1+\sqrt{m}}{2}$, $a_1,b_1 \in \dot{Z}$. En heltalsbasis er altså $(1,\frac{1+\sqrt{m}}{2})$ og $d = \begin{vmatrix} 1 & \frac{1+\sqrt{m}}{2} \\ 1 & \frac{1-\sqrt{m}}{2} \end{vmatrix}^2 = m$.

Eks. $m = -1$. $K = \dot{Q}(\sqrt{-1})$. $(1,\sqrt{-1})$ er heltalsbasis, $R = Z[\sqrt{-1}]$, $d = -4$.

$m = -2$. $K = \dot{Q}(\sqrt{-2})$. $(1,\sqrt{-2})$ er heltalsbasis, $R = Z[\sqrt{-2}]$ $d = -8$.

$m = -3$. $K = \dot{Q}(\sqrt{-3})$; $(1,\frac{1}{2}+\frac{1}{2}\sqrt{-3})$ eller $(1,\frac{1}{2}+\frac{1}{2}\sqrt{-3})$ er heltalsbasis, $R = Z[-\frac{1}{2}+\frac{1}{2}\sqrt{-3}] = Z[\rho]$, $\rho^3 = 1$, $d = -3$.

$m = -5$. $K = \dot{Q}(\sqrt{-5})$; $(1,\sqrt{-5})$ er heltalsbasis, $R = Z[\sqrt{-5}]$ $d = -20$. Bemærk: $Z[\sqrt{-5}]$ er altså Dedekind, men ikke P.I.D., thi fx er $\mathfrak{a} = \{a+b\sqrt{-5} \mid a \equiv b \pmod 2\}$ et ideal, der ikke er hovedideal. Følgelig er $Z[\sqrt{-5}]$ ikke U.F.D. (jfr.p.II,4).

Stickelbergers sætning. Der gælder altid $d \equiv 0,1 \pmod 4$.
Bevis (Schur). Lad $\omega_1,\dots,\omega_m$ være en heltalsbasis, da er

$$d = \begin{vmatrix} \omega_1^{(1)} & \dots & \omega_m^{(1)} \\ \vdots & & \\ \omega_1^{(m)} & \dots & \omega_m^{(m)} \end{vmatrix}^2 = \left[\sum_{(i_1,\dots,i_m) \text{ er lige}} \omega_1^{(i_1)} \cdots \omega_m^{(i_m)} - \sum_{(j_1,\dots,j_m) \text{ ulige}} \omega_1^{(j_1)} \cdots \omega_m^{(j_m)} \right]^2$$

$(P-N)^2 = (P+N)^2-4PN$.
Lad nu $\dot{Q} \subsetneq K \subsetneq M$, med $M/\dot{Q}$ endelig normal, og lad $\sigma_1,\ldots,\sigma_n \in Gr(M/\dot{Q})$ være samtlige n isomorfier af K; for $\tau \in Gr(M/Q)$ er $\tau\sigma_1,\ldots\tau\sigma_n$ igen samtlige isomorfier af K. Da $\sigma_i(\omega_j) = \omega_j^{(i)}$, finder vi $\tau(P+N) = P+N$ og $\tau(PN) = PN$, $\circ$: $P+N \in \dot{Q}$ og $PN \in \dot{Q}$, og da begge er hele, er altså $P+N, PN \in \dot{Z}$, og dermed $(P+N)^2-4PN \equiv 0,1 \pmod 4$

Eks. I $K = Q(\sqrt{m})$, er $\Delta(1,\sqrt{m}) = 4m = k^2d$, hvoraf $|k| = 1,2$. Hvis $m \equiv 2,3 \pmod 4$ må $|k| = 1$, så da er $(1,\sqrt{m})$ en heltalsbasis, idet $\sqrt{m}$ øjensynlig er hel over $\dot{Z}$. For $m \equiv 1 \pmod 4$ er $(1,\frac{1}{2}+\frac{1}{2}\sqrt{m}) = m = k^2d$, så $|k| = 1$, så $(1,\frac{1}{2}+\frac{1}{2}\sqrt{m})$ er heltalsbasis, idet det let eftervises, at $\frac{1}{2}+\frac{1}{2}\sqrt{m}$ er hel over $\dot{Z}$.

Da $K/\dot{Q}$ er separabel, er $K = Q(\vartheta)$, hvor $\vartheta \in R$. Da $Irr(\vartheta,\dot{Q})$ har reelle koef., kan vi ordne rødderne: $\vartheta^{(1)},\ldots,\vartheta^{(n_1)}, \vartheta^{(n_1+1)},\ldots,\vartheta^{(n_1+n_2)}, \vartheta^{(n_1+n_2+1)},\ldots,\vartheta^{(n_1+2n_2)}$ i reelle og par af konjugerede rødder $\circ$: $\vartheta_i \in \dot{R}$, $i = 1,\ldots,r_1$ $\overline{\vartheta^{(n_1+n_2+i)}} = \vartheta^{(n_1+i)}$, $i = 1,\ldots,r_2$ og $n = r_1+2r_2$.
Nu er $k^2d = \Delta(1,\vartheta,\ldots,\vartheta^{n-1}) =$

$$\begin{vmatrix} 1 & \vartheta^{(1)} & \cdots & \vartheta^{(1)n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \vartheta^{(n)} & \cdots & \vartheta^{(n)n-1} \end{vmatrix}^2 = (\det \underline{\underline{A}})^2.$$

Kompleks konjugering giver anledning til r_2 rækkeombyninger i $\underline{\underline{A}}$. Hvis r_2 er lige, er altså $\det \overline{\underline{\underline{A}}} = \det \underline{\underline{A}}$, hvoraf $(\det \underline{\underline{A}})^2 > 0$, og hvis r_2 er ulige, er $\det \overline{\underline{\underline{A}}} = -\det \underline{\underline{A}}$, hvoraf $(\det \underline{\underline{A}})^2 < 0$.

Altså

$$\underline{\text{sign } d = (-1)^{r_2}}$$

IDEALTEORI I R

Om enhederne i R gælder $\underline{\varepsilon \in R \text{ er enhed} \Leftrightarrow N(\varepsilon) = \pm 1}$ (enhed i $\dot{Z}$). thi er $\varepsilon\varepsilon' = L$, da er $N(\varepsilon)N(\varepsilon') = 1$, altså $N(\varepsilon) = \pm 1$, og $\pm 1 = N(\varepsilon) = \varepsilon^{(1)}\ldots\varepsilon^{(n)}$, da er $\frac{1}{\varepsilon} = \frac{1}{\varepsilon^{(1)}} = \varepsilon^{(2)}\ldots\varepsilon^{(n)}$ hel over $\dot{Z}$, $\circ$: $\frac{1}{\varepsilon} \in R$.

Bemærk. Hvis $p,q \in \dot{Z}$, $(p.q) = f \in \dot{Z}$, da er $(pR,qR) = fR$ thi $f = px+qy$, så $fR \subseteq pR+qR$, og $p\alpha+q\beta = f(\frac{p}{f}\alpha+\frac{q}{f}\beta) \in fR$.

Lad nu $\mathfrak{p} \neq (0)$ være et primideal i R, da er $\mathfrak{p} \cap \dot{Z} \neq (0)$, da R er hel over $\dot{Z}$, og $\mathfrak{p} \cap \dot{Z}$ er et primideal i $\dot{Z}$, altså $\mathfrak{p} \cap \dot{Z} = p\dot{Z}$, hvor $p > 0$ er et primtal. Specielt er $p \in \mathfrak{p}$, og dermed $pR \subseteq \mathfrak{p}$ $\circ$: $\mathfrak{p} \mid pR$ eller $pR = \mathfrak{p}\mathfrak{A}$.

Er $p \neq q$ primtal, er $pR = \mathfrak{P}_1 \ldots \mathfrak{P}_n$ og $qR = \mathfrak{Q}_1 \ldots \mathfrak{Q}_s$, og $(p,q) = 1$, så $\{\mathfrak{P}_i\}$ og $\{\mathfrak{Q}_j\}$ er disjunkte. Specielt har R uendelig mange primidealer.

Sætning. Lad $\mathfrak{A} \neq (0)$ være et helt ideal i R, da er $R/\mathfrak{A}$ endelig.
Bevis. Vi kan (jfr.IX,2) finde $a \in \mathfrak{A} \cap \dot{Z}$, $a \neq 0$, og dermed $aR \subseteq \mathfrak{A}$. Det er følgelig nok at vise, at R/aR er endelig. Lad $\omega_1, \ldots, \omega_n$ være heltalsbasis, da kan hvert $\alpha \in R$ entydigt skrives $\alpha = a_1\omega_1 + \ldots + a_n\omega_n + a(h_1\omega_1 + \ldots + h_n\omega_n)$, hvor $0 \leq a_i < |a|$ så R/aR har netop $|a^n|$ elementer. ∎

Antallet af restklasser mod.$\mathfrak{A}$ kaldes normen af $\mathfrak{A}$, og er altså endelig. Det betegnes $\mathfrak{N}(\mathfrak{A})$.

Sætning. Lad $\mathfrak{A} \neq (0)$ være et helt ideal i R, og $\alpha_1, \ldots, \alpha_n$ en $\dot{Z}$-basis for $\mathfrak{A}$. Hvis $\Delta(\alpha_1, \ldots, \alpha_n) = k^2 d$, da er $\mathfrak{N}(\mathfrak{A}) = |k|$. Hvis $\mathfrak{A} = (\alpha)$ er et hovedideal, er $\mathfrak{N}((\alpha)) = |N(\alpha)|$.
Bevis. Lad $\omega_1, \ldots, \omega_n$ være en heltalsbasis, da er $\underline{\alpha}_{|} = \underline{A}\,\underline{\omega}_{|}$, hvor det $\underline{A} = k$. Iflg. elementardivisorsætningen (p.I,25) findes en basis $(\beta_1, \ldots, \beta_n)$ for $\mathfrak{A}$ og en basis $(\rho_1, \ldots, \rho_n)$ for R, så at

$$\underline{\beta}_{|} = (m_i)\,\underline{\rho}_{|},$$

hvor (m_i) betegner en (heltals-) diagonal-matrix med diagonaleleMENterne m_i, $i = 1, \ldots, n$. Nu er $\underline{\beta}_{|} = \underline{P}\,\underline{\alpha}_{|}$, $\underline{\rho}_{|} = \underline{Q}\,\underline{\omega}_{|}$, hvor det $\underline{P} = \pm 1$, det $\underline{Q} = \pm 1$, så $\underline{\alpha}_{|} = \underline{P}^{-1}(m_i)\underline{Q}\,\underline{\omega}_{|}$, altså $\underline{A} = \underline{P}^{-1}(m_i)\underline{Q}$ og dermed $|\det \underline{A}| = |m_1 \ldots m_n|$, men $|m_1 \ldots m_n| = (R:\mathfrak{A}) = \mathfrak{N}(\mathfrak{A})$.
Er specielt $\mathfrak{A} = (\alpha)$, er $r\alpha = (h_1\omega_1 + \ldots + h_n\omega_n)\alpha = h_1(\alpha\omega_1) + \ldots + h_n(\alpha\omega_n)$, så $(\alpha\omega_1, \ldots, \alpha\omega_n)$ er en $\dot{Z}$-basis for (α). Nu er

$$\Delta(\alpha\omega_1, \ldots, \alpha\omega_n) = \begin{vmatrix} \alpha^{(1)}\omega_1^{(1)} & \ldots & \alpha^{(1)}\omega_n^{(1)} \\ \vdots & & \\ \alpha^{(n)}\omega_1^{(n)} & \ldots & \alpha^{(n)}\omega_n^{(n)} \end{vmatrix}^2 =$$

$(\alpha^{(1)} \ldots \alpha^{(n)})^2 \Delta(\omega_1, \ldots, \omega_n) = N(\alpha)^2 d$, så $|N(\alpha)| = |k| = \mathfrak{N}((\alpha))$. ∎

Sætning. $\mathfrak{N}(\mathfrak{A}\mathfrak{B}) = \mathfrak{N}(\mathfrak{A})\mathfrak{N}(\mathfrak{B})$.
Bevis. Det er nok at vise, at $\mathfrak{N}(\mathfrak{P}_1^{m_1} \ldots \mathfrak{P}_n^{m_n}) = \mathfrak{N}(\mathfrak{P}_1)^{m_1} \ldots \mathfrak{N}(\mathfrak{P}_n)^{m_n}$. Her er for det første $\mathfrak{N}(\mathfrak{P}_1^{m_1} \ldots \mathfrak{P}_n^{m_n}) = \mathfrak{N}(\mathfrak{P}_1^{m_1}) \ldots \mathfrak{N}(\mathfrak{P}_n^{m_n})$, da $R/\mathfrak{P}_1^{m_1} \ldots \mathfrak{P}_n^{m_n} \cong R/\mathfrak{P}_1^{m_1} \oplus \ldots \oplus R/\mathfrak{P}_n^{m_n}$. Endvidere er $\mathfrak{N}(\mathfrak{P}^m) = \mathfrak{N}(\mathfrak{P})^m$, hvilket følger af strukturs ætningen p.VIII,7. ∎

Restklassen (α) mod.$\mathfrak{A}$ kaldes primisk, hvis $(\alpha, \mathfrak{A}) = R$ [uafh. af valget af α]. Antallet af primiske restklasser mod.$\mathfrak{A}$ betegnes $\Phi(\mathfrak{A})$.

Sætning. $\varphi(\mathfrak{o})$ er (svagt) multiplikativ, og $\varphi(\mathfrak{o}) = \mathcal{N}(\mathfrak{o}) \prod_{\mathfrak{p}\mid\mathfrak{o}} (1 - \frac{1}{\mathcal{N}(\mathfrak{p})})$.
Bevis. v.s. = $\varphi(\mathfrak{o})$ er multiplikativ, da $(\mathfrak{a},\mathfrak{b}) = (1)$ medfører $R/\mathfrak{a}\mathfrak{b} = R/\mathfrak{a} \oplus R/\mathfrak{b}$, hvoraf ~~altså~~ $\varphi(\mathfrak{a}\mathfrak{b}) = \varphi(\mathfrak{a})\varphi(\mathfrak{b})$, og h.s. er oplagt multiplikativ. Følgelig er det nok at vise = for $\mathfrak{o} = \mathfrak{p}^m$. Et fuldst.rep.syst. for de primiske restklasser er nu $\{\alpha_{i_0} + a_{i_1}\pi + \ldots + \alpha_{i_{m-1}}\pi^{m-1} \mid \alpha_{i_0} \notin \mathfrak{p}\}$, så $\varphi(\mathfrak{p}^m) = (\mathcal{N}(\mathfrak{p})-1)\mathcal{N}(\mathfrak{p})^{m-1} = \mathcal{N}(\mathfrak{p}) \cdot (1 - \frac{1}{\mathcal{N}(\mathfrak{p})})$. ∎

Opgave. Vis Gauss' sætning: $\mathcal{N}(\mathfrak{o}) = \sum_{\mathfrak{v}\mid\mathfrak{o}} \varphi(\mathfrak{v})$.

Lad nu $\mathfrak{p} \neq (0)$ være et primideal, og $\mathfrak{p} \cap \dot{Z} = p\dot{Z}$, da er $pR = \mathfrak{p}\mathfrak{o}$, så $\mathcal{N}(\mathfrak{p})\mathcal{N}(\mathfrak{o}) = \mathcal{N}(\mathfrak{p}\mathfrak{o}) = \mathcal{N}(pR) = |N(p)| = p^n$, så $\mathcal{N}(\mathfrak{p}) \mid p^n$.
Altså
Sætning. <u>$\mathcal{N}(\mathfrak{p})$ er en potens p^f $(1 \leqq f \leqq n)$ af det entydigt bestemte primtal p, som $\mathfrak{p}$ går op i.</u>
f kaldes <u>$\mathfrak{p}$'s grad</u>

Eks. $\mathfrak{p}$ er et 1.gradsprimideal $\Leftrightarrow$ ethvert $\alpha \in R$ er $\equiv$ helt rat.tal (mod.$\mathfrak{p}$), kalrt, da begge er $\Leftrightarrow$ $R/\mathfrak{p} \cong \dot{Z}/p\dot{Z}$

Den kan. homomorfi $\dot{Z}/\mathfrak{p} \cap \dot{Z} \to \dot{R}/\mathfrak{p}$ er injektiv, hvilket let ses, så legemet $R/\mathfrak{p}$ er en udvidelse af legemet $Z/\mathfrak{p} \cap \dot{Z} = \dot{Z}/p\dot{Z}$ af grad f.

Antag nu, at vi har en fremstilleng $pR = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_g^{e_g}$, hvor $\mathfrak{p}_j$'erne er forskellige, $\mathfrak{p}_j$ er af grad f_j, altså $\mathcal{N}(\mathfrak{p}_j) = p^{f_j}$, da er $p^n = \mathcal{N}(pR) = \mathcal{N}(\mathfrak{p}_1)^{e_1} \ldots \mathcal{N}(\mathfrak{p}_g)^{e_g} = p^{e_1 f_1} \ldots p^{e_g f_g}$, så vi slutter:

$$\boxed{n = e_1 f_1 + \ldots + e_g f_g}$$

e kaldes <u>$\mathfrak{p}$'s forgreningseksponent</u>, og primtallet $p \in \dot{Z}$ kaldes <u>uforgrenet</u>, hvis alle $e_j = 1$, ellers <u>forgrenet</u>.

Dedekinds diskriminantsætning. <u>Hvis p er forgrenet, da er $p \mid d$.</u>
Bemærk. Den omvendte slutning gælder også, men svær!
Bevis. Hvis p er forgrenet, er $pR = \mathfrak{p}^2\mathfrak{o}$. Nu er $\mathfrak{p}^2\mathfrak{o} \subset \mathfrak{p}\mathfrak{o}$, så der findes $\alpha \in \mathfrak{p}\mathfrak{o} \setminus \mathfrak{p}^2\mathfrak{o}$. Af $\alpha R \subseteq \mathfrak{p}\mathfrak{o}$ følger $\mathfrak{p}\mathfrak{o} \mid \alpha R$, hvoraf $pR = \mathfrak{p}^2\mathfrak{o} \mid \mathfrak{p}^2\mathfrak{o}^2 \mid \alpha^2 R$, altså $p \mid \alpha^2$, og af $\alpha \notin \mathfrak{p}^2\mathfrak{o} = pR$ følger $p \mid \alpha$.
For $\omega \in R$ er $S(\alpha\omega) = \alpha^{(1)}\omega^{(1)} + \ldots + \alpha^{(n)}\omega^{(n)}$ og altså $S(\alpha\omega)^p \equiv (\alpha^{(1)}\omega^{(1)})^p + \ldots (\alpha^{(n)}\omega^{(n)})^p$ (mod.p). Da $p \mid \alpha^2$ vil $p \mid \alpha^p\omega^p$ og også $\not\equiv p \mid (\alpha^{(1)}\omega^{(1)})^p$, så $S(\alpha\omega)^p \equiv 0 + \ldots + 0$ (mod.p), men da $S(\alpha\omega) \in \dot{Z}$ betyder dette at $p \mid S(\alpha\omega)^p$ og dermed at $p \mid S(\alpha\omega)$.
Lad nu $\omega_1, \ldots, \omega_n$ være en heltalsbasis, så $\alpha = h_1\omega_1 + \ldots + h_n\omega_n$. Da $p \nmid \alpha$ kan vi fx antage, at $p \nmid h_1$. Nu er $S(\alpha\omega_i) = S(h_1\omega_1\omega_i + \ldots + h_n\omega_n\omega_i) =$

$h_1 S(\omega_1\omega_j)+\ldots+h_n S(\omega_n\omega_j)$. Da $S(\alpha\omega_j) \equiv 0 \pmod p$ får vi ved overgang til restklasselegemet $\dot{Z}/p\dot{Z}$, at

$$h_1 S(\omega_1\omega_j) + \ldots + h_n S(\omega_n\omega_j) = 0 \quad j = 1,\ldots,n.$$

Da $h_1 \neq 0$ slutter fi, at $\det(S(\omega_j\omega_i)) = 0$, altså at $d = \det(S(\omega_j\omega_i)) \in p\dot{Z}$. ∎

Kvadratiske udvidelser.

$K = Q(\sqrt{m})$, $m \in \dot{Z}$ kvadratfri. Lad $p \in \dot{Z}$ være et primtal, da er der tre muligheder for opløsningen af pR: Hvis $g = 2$, er $e_1 = f_1 = e_2 = f_2 = 1$ Altså $pR = \mathfrak{p}_1\mathfrak{p}_2$ (indb.forsk.) $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p$; p kaldes da fuldstændig ~~forgrenet.~~ opløst. Hvis $g = 1$, er $e_1 f_1 = 2$, så enten er $e_1 = 2$, $f_1 = 1$, $pR = \mathfrak{p}^2$, $N(\mathfrak{p}) = p$, hvor p kaldes ~~fuldt opløseligt~~, forgrenet, wller $e_1 = 1$, $f_1 = 2$, $pR = \mathfrak{p}$ er da selv et primideal, $N(pR) = p^2$ × p kaldes trægt.

p er ulige. 1) Hvis p er fuldt opløseligt, er $pR = \mathfrak{p}_1\mathfrak{p}_2$, $f_1 = f_2 = 1$; iflg. eks.IX,6 er $\sqrt{m} \equiv r_1 \ (\mathfrak{p}_1)$, og altså $m \equiv r_1^2 \ (\mathfrak{p}_1)$ og dermed også $m \equiv r_1^2 \ (p)$. Nu er $m \not\equiv 0 \ (p)$, thi vi har $\sqrt{m} \equiv r_2 \ (\mathfrak{p}_2)$, og dermed $m \equiv r_2^2 \ (p)$, og hvis $m \equiv 0 \ (p)$ ville altså $r_1^2 \equiv r_2^2 \equiv 0 \ (p)$ og altså $r_1 \equiv r_2 \equiv 0 \ (p)$, så at $r_1 \equiv r_2 \equiv 0 \ \{(\mathfrak{p}_1)\ (\mathfrak{p}_2)$, hvoraf $\sqrt{m} \equiv 0 \ \{(\mathfrak{p}_1)\ (\mathfrak{p}_2)\}$ ⊃: $\sqrt{m} \equiv 0 \ (\mathfrak{p}_1\mathfrak{p}_2 = pR)$, men så ville $\frac{\sqrt{m}}{p} \in R$ i modstrid med de fundne heltalsbaser. Følgelig er $(\frac{m}{p}) = 1$.

2) Hvis p er forgrenet, er (Dedekind) $p|d$ og dermed $p|m$.

3) Hvis p er trægt, er $(\frac{m}{p}) = -1$, thi ellers var $m \equiv r^2 \ (p)$, så $(\sqrt{m}+r)(\sqrt{m}-r) \equiv 0 \ (pR)$, hvoraf $\frac{\sqrt{m}\pm r}{p} \in R$ i modstrid med de fundne heltalsbaser.

Det ses nu, at de omvendte inklusioner også må gælde, altså

$$p \text{ er opløst} \iff (\tfrac{m}{p}) = 1 \iff (\tfrac{d}{p}) = 1$$
$$p \text{ forgrenet} \iff (\tfrac{m}{p}) = 0 \iff (\tfrac{d}{p}) = 0$$
$$p \text{ er trægt} \iff (\tfrac{m}{p}) = -1 \iff (\tfrac{D}{p}) = -1.$$

$p = 2$. 1) Hvis 2 er opløst, er $2R = \mathfrak{p}_1\mathfrak{p}_2$, og $m \not\equiv 2,3 \pmod 4$, thi som før får vi $\sqrt{m} \equiv r_1 \ (\mathfrak{p}_1)$, $\sqrt{m} \equiv r_2 \ (\mathfrak{p}_2)$, og $r_1^2 \equiv r_2^2 \ (2)$, hvoraf $r_1 \equiv r_2 \ (2)$, men så er $\sqrt{m}-r_1 \equiv 0 \ (\mathfrak{p}_1\mathfrak{p}_2 = 2R)$ og altså $\frac{\sqrt{m}-r_1}{2} \in R$, og de fundne heltalsbaser viser, at $m \equiv 1 \ (4)$. Videre: $\frac{1+\sqrt{m}}{2} \equiv r \ (\mathfrak{p}_1)$ $\Rightarrow 1+\sqrt{m} \equiv 2r_1 \ (2\mathfrak{p}_1) \Rightarrow \sqrt{m} \equiv 2r-1 \ (2\mathfrak{p}_1) \Rightarrow \sqrt{m}+2r-1 = (\sqrt{m}-(2r-1)) + 2(2r-1) \equiv 0 \ (2R) \Rightarrow m \equiv -(2r-1) \ (2R) \Rightarrow m-(2r-1)^2 = (\sqrt{m}-(2r-1))(\sqrt{m}+(2r-1)) \equiv 0 \ (4\mathfrak{p}_1) \Rightarrow \frac{1}{4}(m-(2r-1)^2) \equiv 0 \ (\mathfrak{p}_1)$ $\frac{1}{4}(m-(2r-1)) \equiv 0 \ (2) \Rightarrow m-(2r-1)^2 \equiv 0 \ (8) \Rightarrow m \equiv 1 \ (8)$, altså $d = m \equiv 1 \pmod 8$.

2) hvis 2 er forgrenet, er $\mathfrak{p}|d$, altså $d \equiv 0 \pmod 4$, $m \equiv 2,3 \ (4)$

3) Hvis 2 er trægt, er 2R et primideal. Hvis $m \equiv 2 \ (4)$, er $m \equiv 0 \ (2)$

$\sqrt{m}\sqrt{m} \equiv 0 \ (2R)$, hvoraf $\sqrt{m} \equiv 0 \ (2R)$ eller $\frac{\sqrt{m}}{2} \in R$, og hvis $m \equiv 3 \ (4)$, er $(1+\sqrt{m})^2 = 1+m+2\sqrt{m} \equiv 2\sqrt{m} \ (4R)$, hvoraf $(1+\sqrt{m})^2 \equiv 0 \ (2R)$, og der med $\frac{1+\sqrt{m}}{2} \in R$, og begge dele er i iokstrid med de fundne heltalsbaser. Følgelig er $m \equiv 1 \ (\text{mod}.4)$. Hvis $m \equiv 1 \ (8)$, vi ville $(\sqrt{m}-1)(\sqrt{m}+1) \equiv 0 \ (8R)$, og altså $\frac{\sqrt{m}-1}{2}\frac{\sqrt{m}+1}{2} \equiv 0 \ (2R) \Rightarrow \frac{\sqrt{m}\pm 1}{4} \in R$ i modstrid med de fundne heltalsbaser. Følgelig er $d = m \equiv 5 \ (8)$. ☐

Det følger nu, at også de omvendte implikationer må gælde.

Indføres symbolet

$$\left(\frac{d}{2}\right) = \begin{cases} 0 & \text{hvis } d \equiv 0 \ (4) \\ 1 & \text{hvis } d \equiv 1 \ (8) \\ -1 & \text{hvis } d \equiv 5 \ (8) \end{cases}$$

[altså kun defineret for $d \equiv 0,1 \ (4)$] da er betingelserne altså de samme som for ulige primtal.

Eks. $K = \dot{Q}(\sqrt{-5})$, $d = -20$, $R = \dot{Z}[\sqrt{-5}]$. Vi har $6 = 2\cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ primopløsning. (Betragt $N(2) = 4$ o.s.v.) 2 er forgrenet, da $\left(\frac{-20}{2}\right) = 0$, og 3 er fuldt opløst, da $\left(\frac{-20}{3}\right) = \left(\frac{1}{3}\right) = 1.$, så vi har $2R = \mathfrak{p}_2^2$, og $3R = \mathfrak{p}_3\mathfrak{p}_3'$. Nu er $(3,1+\sqrt{-5})$ divisor i 3, altså $= (1), \mathfrak{p}_3, \mathfrak{p}_3', \mathfrak{p}_3\mathfrak{p}_3' = 3R$. Her er (1) udelukket, thi ellers var $1 = 3r+(1+\sqrt{-5})s$ og dermed $2 = 6r+2(1+\sqrt{-5})s = (1+\sqrt{-5})t$, altså $(1+\sqrt{-5}) \mid 2$, og $\mathfrak{p}_3\mathfrak{p}_3' = 3R$ er udelukket, thi da var $3 \mid 1+\sqrt{-5}$. Følgelig kan vi sætte $\mathfrak{p}_3 = (3,1+\sqrt{-5})$. Analogt ses, at $(3,1-\sqrt{-5})$ er $= \mathfrak{p}_3, \mathfrak{p}_3'$, men da $(3,1-\sqrt{-5})(3,1+\sqrt{-5}) = (9,3-3\sqrt{-5}, 3+3\sqrt{-5},6) = 3R$, må $\mathfrak{p}_3' = (3,1-\sqrt{-5})$ gælde. Analogt finder vi $\mathfrak{p}_2 = (2,1+\sqrt{-5})$, min så er $\mathfrak{p}_2\mathfrak{p}_3 = (2,1+\sqrt{-5})(3,$
1 $1+\sqrt{-5}) = (6,2+2\sqrt{-5}),3+3\sqrt{-5},(1+\sqrt{-5})^2) = (1+\sqrt{-5})$, og $\mathfrak{p}_2\mathfrak{p}_3' = (1-\sqrt{-5})$. Opspaltningen $6R = 2R\cdot 3R = (1+\sqrt{-5})(1-\sqrt{-5})$ svarer altså til $6R = (\mathfrak{p}_2^2)(\mathfrak{p}_3\mathfrak{p}_3') = (\mathfrak{p}_2\mathfrak{p}_3)(\mathfrak{p}_2\mathfrak{p}_3')$.

<u>Cyklotomiske udvidelser.</u>

Vi betragter et cirkeldelingslegeme $K = \dot{Q}_m = \dot{Q}(e^{\frac{2\pi i}{m}}) = \dot{Q}(\zeta_m)$, hvor ζ_m er en primitiv m'te enhedsrod. Vi her $n = [K:\dot{Q}] = \varphi(m)$, $\text{Irr}(\zeta_m, \dot{Q}) = F_m(X) = \prod_{(a,m)=1}(X-\zeta_m^a)$; Galoisgruppen for $K/\dot{Q}$ er isomorf med $G(m)$ gruppen af prim.restkl. mod.m. $1,\zeta,\ldots,\zeta^{\varphi(m)-1}$ er en $\dot{Q}$-basis for K [Det <u>er</u> faktisk en heltalsbasis, hvilket ikke vises], og for $f(\zeta) \in K$ finder vi $N_{K/\dot{Q}}(f(\zeta)) = \prod_{(a,m)=1} f(\zeta_m^a)$. Der gælder

$$F_m(1) = \begin{cases} p \text{ for } m = p^\nu \\ 1 \text{ ellers,} \end{cases}$$

thi da $\sum_{d|m}\mu(d) = 0$ for $m > 1$, er $F_m(X) = \prod_{d|m}(X^{\frac{m}{d}}-1)^{\mu(d)} = \prod_{d|m}(X^{\frac{m}{d}}-1)^{\mu(d)}/(X-1)^{\mu(d)} = \prod_{d|m}(X^{\frac{m}{d}-1}+X^{\frac{m}{d}-2}+\ldots+X+1)^{\mu(d)}$, så $F_m(1) = \prod_{d|m}(\frac{m}{d})^{\mu(d)}$. [For $m = p^\nu$ finder vi $F_m(1) = (\frac{p^\nu}{1})^1(\frac{p^\nu}{p})^{-1}1\ldots 1 = p$, og

Følgelig er $m = \prod_{d|m} E_m(1)$, og da "den påstående funktion" også opfylder dette, følger påstanden. Korollar:

$$N_{K/\mathbb{Q}}(1-\zeta_m) = \begin{cases} p & \text{hvis } m = p^\nu \\ 1 & \text{ellers.} \end{cases}$$

Hvis $m = p^\nu$ har vi altså $\mathfrak{N}(1-\zeta_m) = p$, hvoraf [idet $\mathfrak{N}(\mathfrak{A}) = p \Rightarrow \mathfrak{A}$ er primideal] $(1-\zeta_m)$ er et 1.grads primideal. For $a \not\equiv 0\ (p)$ er $1-\zeta$ og $1-\zeta^a$ associerede, så $pR = \prod_{(a,m)=1}(1-\zeta^a) = \prod_{(a,m)=1}(1-\zeta) = (1-\zeta)^{\varphi(m)} = (1-\zeta)^m$, så $(1-\zeta_m)$ har forgreningsexp. $e = n$, og p er fuldstændig forgrenet.

Hvis m ikke er primtalspotens er $1-\zeta_m$ en enhed.

Vi har $\Delta(1, \zeta, \ldots, \zeta^{\varphi(m)-1}) = dk^2$ [Her er endda $k^2 = 1$] Der gælder:

Sætning. <u>$\Delta = \Delta(1, \zeta, \ldots, \zeta^{m-1})$ (og så meget mere d) indeholder kun primtal, der går op i m.</u>

Bevis. Vi har $\Delta = \prod_{i<j}(\zeta^{(i)} - \zeta^{(j)}) = \pm \prod_{i\neq j}(\zeta^{(i)} - \zeta^{(j)}) = \pm \prod_{\substack{a\neq b \\ (a,m)=1 \\ (b,m)=1}} (\zeta^a - \zeta^b)$. Her er $\zeta^a - \zeta^b = \zeta^a(1-\zeta^{b-a})$, og $\zeta^{b-a} = \zeta_k$, en k'te primitiv enhedsrod, hvor $k|m$. Nu er $N_{\dot{\mathbb{Q}}_k/\dot{\mathbb{Q}}}(1-\zeta_k) = 1, p$, så $N_{K/\dot{\mathbb{Q}}}(1-\zeta_k) = N_{\mathbb{Q}/\dot{\mathbb{Q}}_k}(N_{\dot{\mathbb{Q}}_k K/\dot{\mathbb{Q}}_k}(1-\zeta_k)) = N_{\dot{\mathbb{Q}}_k/\dot{\mathbb{Q}}}(1-\zeta_k)^\alpha = 1, p^\alpha$, og $p|k|m$. Heraf ses, at $N(\Delta) = \prod N(\zeta^a - \zeta^b) = \prod N(1-\zeta^{b-a}) = \prod_k N(1-\zeta_k) =$ produkt af primtal p, der går op i m. Påstanden følger nu af $N(\Delta) = \Delta^m$. ∎

Korollar. <u>Hvis $p \nmid m$, da er pR uforgrenet.</u>

Sætning. <u>Hvis $p \nmid m$ og $pR = \varphi_1 \ldots \varphi_g$, med $\mathfrak{N}(\varphi_j) = p^{f_j}$, da er $f_1 = \ldots = f_g = f =$ ord (p) mod.m (= det mindste positive tal f for hvilket $p^f \equiv 1\ (\text{mod}.m)$.</u>

Bevis. 1) Lad $\varphi_j | pR$, $\mathfrak{N}(\varphi_j) = p^{f_j}$. R/φ_j er et endeligt legeme med p^{f_j} elementer, så for $\alpha \in R \setminus \varphi_j$ er $\alpha^{p^{f_j}-1} \equiv 1\ (\varphi_j)$. Specielt er $\zeta^{p^{f_j}-1} \equiv 1\ (\varphi_j)$. Heraf følger imidlertid $\zeta^{p^{f_j}-1} = 1$, thi ellers var $\varphi_j \supseteq (1-\zeta^{p^{f_j}-1}) \supseteq \prod_{\nu=1}^{m-1}(1-\zeta^\nu) = mR$ og dermed $pZ \supseteq mZ$ i modstrid med at $p \nmid m$. Følgelig er $p^{f_j} \equiv 1\ (\text{mod}.m)$, så $f \leq f_j$.

2) $1, \zeta, \ldots, \zeta^{m-1}$ er en $\dot{\mathbb{Q}}$-basis for K. Iflg. beviset p.VIII,8 har vi for $\alpha \in R$, endda $\Delta\alpha = r_0 + r_1\zeta + \ldots + r_{m-1}\zeta^{m-1}$, hvor $r_j \in \dot{Z}$. Nu er $\Delta^p \alpha^p = (r_0 + r_1\zeta + \ldots + r_{m-1}\zeta^{m-1})^p \equiv r_0^p + \ldots + r_{m-1}^p(\zeta^p)^{m-1}$ (pR) og dermed $\Delta^p\alpha^p \equiv r_0^p + r_1^p\zeta^p + \ldots + r_{m-1}^p(\zeta^p)^{m-1}$ (φ_j). Da $\Delta, r_j \in \dot{Z}$, er $\Delta^p \equiv \Delta\ (\varphi_j)$ og $r_j^p \equiv r_j\ (\varphi_j)$, så vi får $\Delta\alpha^p \equiv r_0 + r_1\zeta^p + \ldots + r_{m-1}(\zeta^p)^{m-1}$ (φ_j). heraf følger $\Delta^p(\alpha^p)^p \equiv (r_0 + \ldots + r_{m-1}(\zeta^p)^{m-1})^p \equiv r_0^p + r_1^p\zeta^{p^2} + \ldots + r_{m-1}^p(\zeta^{p^2})^{m-1}$ (φ_j), altså $\Delta\alpha^{p^2} \equiv r_0 + r_1\zeta^{p^2} + \ldots + r_{m-1}(\zeta^{p^2})^{m-1}$ (φ_j), osv ... $\Delta\alpha^{p^f} \equiv r_0 + r_1\zeta^{p^f} + \ldots + r_{m-1}(\zeta^{p^f})^{m-1} = r_0 + r_1\zeta + \ldots + r_{m-1}\zeta^{m-1} = \alpha\Delta\ (\varphi_j)$, altså $\Delta\alpha^{p^f} \equiv \Delta\alpha\ (\varphi_j)$. Her er $\Delta \notin \varphi_j$, da $p \nmid m$, så vi slutter, at $\alpha^{p^f} \equiv \alpha\ (\varphi_j)$. Nu er $(R/\varphi_j) \setminus (0)$ cyklisk, så der findes en primitiv rod $\rho \in R$, så $\rho^{p^{f_j}-1} \equiv 1\ (\varphi_j)$. Da også $\rho^{p^f-1} \equiv 1\ (\varphi_j)$, må $p^{f_j}-1 \leq p^f - 1$ d: $f_j \leq f$. ∎

Korollar. Ethvert endeligt legeme kan realiseres som $R/\ .$

thi for $m = p^f - 1$, har (p) orden f (mod.m), så i $K = \dot{Q}_m$ er $pR = \varphi_1 \cdots \varphi_g$, da $p \nmid m$, og $\mathcal{N}(\varphi_i) = p^{f_i} = p^f$, altså $R/\varphi_i = GF(p^f)$

Eks. $m = 3$. $Q_3 = Q(\frac{1}{2}(-1+\sqrt{-3})) = Q(\sqrt{-3})$. Vi har $pR = \varphi_1\varphi_2 \Leftrightarrow (\frac{-3}{p}) = 1$, dels $pR = \varphi_1\varphi_2 \Leftrightarrow g = 2 \Leftrightarrow f = 1 \Leftrightarrow p \equiv 1$ (3), altså $(\frac{-3}{p}) = 1 \Leftrightarrow p \equiv 1$ (mod.3), en del af reciprocitetssætningen.

Eks. $m = \not{4}8$. $\dot{Q}_8 \supseteq Q(\sqrt{2})$ $n = \varphi(8) = 4$. Antag $p \equiv 1$ (8) da er $p\tilde{R} = \varphi_1\varphi_2\varphi_3\varphi_4$, hvor $f = 1$. Hvis $(\frac{2}{p}) = -1$, var pR et primideal i R, så $pR = \varphi_1 \cap \tilde{R}$. Den kan.hom. $R/pR = R/\varphi_1 \cap \tilde{R} \to \tilde{R}/\varphi_1$ er injektiv, men da R/pR har $\mathcal{N}(pR) = p^2$ elementer, og $\tilde{R}/\varphi_1$ har $p^f = p$ elementer, er dette en modstrid. Følgelig er $(\frac{2}{p}) = 1$, så: $p \equiv 1$ (8) $\Rightarrow (\frac{2}{p}) = 1$.

I tilfældet $m = p$ primtal viser vi, at $1, \zeta, \ldots, \zeta^{p-2}$ er heltalsbasis. Sæt $\lambda = 1-\zeta$, da er det nok at vise, at $1, \lambda, \ldots, \lambda^{p-2}$ er heltalsbasis. Idet $\Delta = \Delta(1, \zeta, \ldots, \zeta^{p-2})$, har vi for $\alpha \in R$, at $\Delta\alpha \in \dot{Z}\{1, \ldots, \zeta^{p-2}\} \subseteq \dot{Z}\{1, \lambda, \ldots, \lambda^{p-2}\}$, og da Δ er er en potens af p, kan vi antage, at vi har $p^N\alpha = r_0 + r_1\lambda + \ldots + r_{p-2}\lambda^{p-2}$, hvor $r_\nu \in \dot{Z}$, og ikke alle $r_\nu \equiv 0$ (p). Her må $N = 0$, thi ellers var $r_0 + \ldots + r_{p-2}\lambda^{p-2} \equiv 0$ (pR). Nu er $pR = (1-\zeta)^{p-1} = (\lambda)^{p-1}$, og hvis $r_0, \ldots, r_{\mu-1} \equiv 0$ (p), ville $r_0 + \ldots + r_{\mu-1}\lambda^{\mu-1} \equiv 0$ (λ^{p-1}), og $r_{\mu+1}\lambda^{\mu+1} + \ldots + r_{p-2}\lambda^{p-2} \equiv 0$ $(\lambda^{\mu+1})$, hvoraf $r_\mu\lambda^\mu \equiv 0$ $(\lambda^{\mu+1})$ og dermed $r_\mu \equiv 0$ (λ). Da $r_\mu \in \dot{Z}$ er $r_\mu \in \lambda R \cap \dot{Z} = p\dot{Z}$. Ved induktion følger nu, at alle $r_\mu \equiv 0$ (p), i modstrid med antagelsen.

Nu er $d = \Delta = \prod_{\substack{a \not\equiv b \\ (a,p)=1 \\ (b,p)=1}} (\zeta^a - \zeta^b)$. Her er $\zeta^a - \zeta^b = \zeta^a(1-\zeta^{b-a}) \sim \lambda$, så $d = \Delta \sim \prod_{a,b}\lambda = \lambda^{(p-1)^2-(p-1)} = \lambda^{(p-1)(p-2)} \sim p^{p-2}$, altså $\Delta = \pm p^{p-2}$

Da $\operatorname{sgn} d = (-1)^{r_2} = (-1)^{\frac{p-1}{2}}$, har vi altså $\underline{d = \Delta = (-1)^{\frac{p-1}{2}} p^{p-2}}$.

Da $\sqrt{d} \in \dot{Q}_p$ (jfr. def.) følger det let heraf, at $\sqrt{(-1)^{\frac{p-1}{2}} p} \in \dot{Q}_p, p \geq 3$.

For $f(X) = a_0 + a_1X + \ldots + a_mX^m \in R[X]$, defineres indholdet af f, som $\mathcal{J}(f) = (a_0, \ldots, a_m) \subseteq R$.

Sætning. Hvis R er Dedekind, da er $\mathcal{J}(fg) = \mathcal{J}(f)\mathcal{J}(g)$, for $f, g \in R[X]$.

Bevis. Det er nok at vise, at $[\mathcal{J}(f)\mathcal{J}(g)]R_{\mathfrak{M}} = \mathcal{J}(fg)R_{\mathfrak{M}}$ for alle maximale idealer $\mathfrak{M}$. Nu er $\mathcal{J}(f)R_{\mathfrak{M}} = (a_0R + a_1R + \ldots + a_mR)R_{\mathfrak{M}} = a_0R_{\mathfrak{M}} + \ldots + a_nR_{\mathfrak{M}} = \mathcal{J}_{R_{\mathfrak{M}}}(f)$, hvor vi jo har $f \in R_{\mathfrak{M}}[X]$. Det er altså nok at bevise sætningen for et P.I.D., og det er let. ∎

Sætning. Lad $K/\dot{Q}$ være normal og sæt $G = Gr(K/\dot{Q})$, da er $\mathcal{N}(\mathfrak{a})R = \prod_{\sigma \in G}\sigma(\mathfrak{a})$ for et ideal $\mathfrak{a}$ i R.

Bevis. Lad $\mathfrak{a} = (\alpha_1, \ldots, \alpha_m)$, og sæt $f(X) = \alpha_1X + \ldots + \alpha_mX^m \in R[X]$, da er $\mathcal{J}(f) = \mathfrak{a}$. Sæt $g(X) = \prod_\sigma (\sigma f)(X) \in K[X]$; for $\tau \in G$ er $(\tau g)(X) = \prod_\sigma (\tau\sigma f)(X) = g(X)$, så $g(X) \in \dot{Q}[X]$, og da koeff. er hele, altså

$g(X) \in \dot{Z}[X]$, så $\mathfrak{J}(g) = aR$, med $a \in \dot{Z}$. På den anden side er $\mathfrak{J}(g) = \prod_\sigma \mathfrak{J}(\sigma f) = \prod_\sigma \sigma \mathfrak{J}(f) = \prod_\sigma \sigma(\mathfrak{o})$, hvoraf $|a|^n = \mathfrak{N}(aR) = \mathfrak{N}(\mathfrak{J}(g)) = \prod_\sigma \mathfrak{N}(\sigma(\mathfrak{o})) = \prod_\sigma \mathfrak{N}(\mathfrak{o}) = \mathfrak{N}(\mathfrak{o})^n$, så $\mathfrak{N}(\mathfrak{o}) = |a|$, og dermed $\mathfrak{N}(\mathfrak{o})R = |a|R = aR = \prod_\sigma \sigma(\mathfrak{o})$. ∎

Hvis $K/\dot{Q}$ er normal, og $\mathfrak{P} | pR$, vil $\sigma\mathfrak{P} | \sigma(pR) = pR$, og hvis $\mathfrak{P}' | pR$ vil $\mathfrak{P}' | p^f R = \mathfrak{N}(\mathfrak{P})R = \prod_\sigma \sigma(\mathfrak{P})$, og dermed $\mathfrak{P}' = \tau\mathfrak{P}$ for et $\tau \in G$. Altså fremkommer de forskellige $\mathfrak{P}'$er, der går op i pR som de forskellige automorfe billeder af et af dem. Da $\mathfrak{N}(\sigma\mathfrak{P}) = \mathfrak{N}(\mathfrak{P})$, er f_i'erne ens for alle $\mathfrak{P}_i$, og da $\mathfrak{P}^e \| pR \Leftrightarrow (\sigma\mathfrak{P})^e \| pR$, er også alle e_i'erne ens. Vi har derfor $pR = (\mathfrak{P}_1 \dots \mathfrak{P}_g)^e$, $\mathfrak{N}(\mathfrak{P}_i) = p^f$ og $efg = n$.

Antag stadig at $K/\dot{Q}$ er normal, og lad $\mathfrak{P}$ være et fast primideal i R. $G_Z = \{\sigma \in G \mid \sigma\mathfrak{P} = \mathfrak{P}\}$ kaldes "Zerlegungs"-gruppen for $\mathfrak{P}$. Det er klart en undergruppe i G. Nu er $\sigma\mathfrak{P} = \tau\mathfrak{P} \Leftrightarrow \sigma^{-1}\tau\mathfrak{P} = \mathfrak{P} \Leftrightarrow \sigma^{-1}\tau \in G_Z \Leftrightarrow \tau \in \sigma G_Z$. Følgelig er $(G:G_Z) = g$, og er $G = \sigma_1 G_Z \cup \dots \cup \sigma_g G_Z$, er $pR = (\sigma_1\mathfrak{P} \dots \sigma_g\mathfrak{P})^e$, og $\mathrm{ord}(G_Z) = n/g = ef$.
$G_T = \{\sigma \in G \mid \forall \alpha \in R: \sigma\alpha \equiv \alpha \ (\mathfrak{P})\}$ kaldes trægheds gruppen for $\mathfrak{P}$; det er klart en undergruppe i G, endda $G_T \subseteq G_Z$, thi for $\sigma \in G_T$ er $\sigma^{-1} \in G_T$; for $\alpha \equiv 0 \ (\mathfrak{P})$ er altså $\sigma^{-1}\alpha \equiv 0 \ (\mathfrak{P})$, og dermed $\alpha \equiv 0 \ (\sigma\mathfrak{P})$, d.v.s. $\mathfrak{P} \subseteq \sigma\mathfrak{P}$, og dermed $\mathfrak{P} = \sigma\mathfrak{P}$.
Vi definerer nu en afbildning $G_Z \to \mathrm{Gr}(R/\mathfrak{P}) = \mathrm{Gr}(R/\mathfrak{P} \ / \dot{Z}/(p))$, idet vi for $\sigma \in G_Z$ sætter $\bar{\sigma}(\overline{\alpha}) = \overline{\sigma\alpha}$. Definitionen er lovlig, thi $\overline{\alpha} = \overline{\beta} \Leftrightarrow \alpha \equiv \beta \ (\mathfrak{P}) \Rightarrow \sigma(\alpha) \equiv \sigma(\beta) \ (\mathfrak{P}) \Rightarrow \bar{\sigma}(\overline{\alpha}) = \bar{\sigma}(\overline{\beta})$, og det er klart en homomorfi. Det kan vises, at den er surjektiv; kernen er netop G_T, så vi slutter, at $G_T \lhd G_Z$, og her er faktorgruppen $G_Z/G_T = \mathrm{Gr}(R/\mathfrak{P}) = \mathrm{Gr}(GF(p^f))$ cyklisk af orden f, så $\mathrm{ord}(G_T) = ef/f = e$.
$G_{V_i} = \{\sigma \in G \mid \forall \alpha \in R: \sigma\alpha \equiv \alpha \ (\mathfrak{P}^{i})\}$ kaldes forgreningsgrupperne for $\mathfrak{P}$. Her er $G_{V_1} = G_T$. Man kan vise, at $G_{V_{i+1}} \lhd G_{V_i}$, med cyklisk faktorgruppe.
Denne proces må stoppe i den forstand, at $G_{V_i} = E$ fra et vist trin, thi der findes til $\sigma \neq e$ et $\alpha \in R$, så $\sigma(\alpha) \neq \alpha$, men så kan $\sigma(\alpha) \equiv \alpha \ (\mathfrak{P}^m)$ kun gælde for endelig mange n. Følgelig er

$$G_Z \rhd G_T = G_{V_1} \rhd G_{V_2} \rhd \dots \rhd E$$

en normalrække med cykliske faktorer.

$$\begin{array}{ccccccccccccc} G & \supseteq & G_Z & \rhd & G_T & \rhd & G_{V_2} & \rhd & \dots & \rhd & E \\ | & & | & & | & & | & & & & | \\ \dot{Q} & \subseteq & K_Z & \subseteq & K_T & \subseteq & K_V & \subseteq & \dots & \subseteq & K \end{array}$$

Kubiske kongruenser. Vi betragter kongruensen (*) $x^3 \equiv a \ (p)$, $a \not\equiv 0$

Hvis $p \equiv 2\ (3)$, er $(p-1,3) = 1$, så der findes k,h, så $1 = k(p-1)+h\cdot 3$ men så er $a = a^{k(p-1)+h\cdot 3} \equiv (a^h)^3\ (p)$ iflg. Fermat, så der findes en løsning - og ikka andre, thi er ρ en primitivrod, og er ρ^α, ρ^β løsninger, da er $3\alpha \equiv 3\beta\ (p-1)$, og dermed $\alpha \equiv \beta\ (p-1)$ o: $\rho^\alpha \equiv \rho^\beta\ (p)$.

Hvis $p \equiv 1\ (3)$, og (*) har en løsning, kaldes a en kub.rest, og ellers en kub.ikkerest. De kub.rester udgør den entydigt bestemte undergruppe $\{\rho^{3a} \mid 0 \le a < \frac{p-1}{3}\}$ af indeks 3 i $G(p)$, så der findes netop $\frac{p-1}{3}$. For en kub.rest $a \equiv x^3\ (p)$ er $a^{\frac{p-1}{3}} \equiv x^{p-1} \equiv 1\ (p)$, så a er rod i pol. $X^{\frac{p-1}{3}} - 1 \in \dot{Z}/(p)[X]$, og da dette pol. højst har $\frac{p-1}{3}$ rød der, må disse være de kub.rester. Altså: a kub.rest $\Leftrightarrow a^{\frac{p-1}{3}} \equiv 1\ (p)$

Eks. $K = \dot{Q}(\sqrt[3]{2})$ ikke normal. Man finger $\Delta(1,\sqrt[3]{2},\sqrt[3]{4}) = -108$, så $d \mid 108$, og $p \neq 2,3 \Rightarrow$ p er uforgrenet. Der er nu følgende muligheder: (1) $pR = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3$, $\mathcal{N}(\mathfrak{P}_j) = p$, (2) $pR = \mathfrak{P}_1\mathfrak{P}_2$, $\mathcal{N}(\mathfrak{P}_1) = p^2$, $\mathcal{N}(\mathfrak{P}_2) = p$ og (3) pR er trægt, $\mathcal{N}(pR) = p^3$.

Hvis $p \equiv 2\ (3)$, har $2 \equiv k^3\ (p)$ en løsning, så i $\dot{Z}/(p)[t]$ har vi $t^3 - \textcircled{2} = (t-\textcircled{k})(t^2+\textcircled{k}t+\textcircled{k}^2)$ og dermed $t^3-2 = (t-k)(t^2+kt+k^2)+pf(t)$, hvor $f(t) \in Z[t]$. For $t = \sqrt[3]{2}$ fås $(\sqrt[3]{2}-k)(\sqrt[3]{4}+k\sqrt[3]{2}+k^2) = -pf(\sqrt[3]{2}) \in pR$. Hvis p var trægt (o: hvis (3)) ville $\frac{\sqrt[3]{2}-k}{\mathfrak{P}} \in R$ eller $\frac{\sqrt[3]{4}+k\sqrt[3]{2}+k^2}{\mathfrak{P}} \in R$, imodstrid med resultatet p.VIII,8. Og hvis $pR = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3$ (o: hvis (1)), da var $\mathfrak{P}_j$ 1.gradsprimideal, så $\sqrt[3]{2} \equiv r_j\ (\mathfrak{P}_j)$ og dermed $2 \equiv r_j^3\ (p)$, men en sådan kongruens har kun én løsning, r, men af $\sqrt[3]{2} \equiv r\ (\mathfrak{P}_j)$ følger $\sqrt[3]{2} \equiv r\ (pR)$, igen i modstrid med p.VIII,8. Følgelig er $pR = \mathfrak{P}_1\mathfrak{P}_2$, hvor $f_1 = 2$, $f_2 = 1$.

Man kan tilsvarende vise, at hvis $p \equiv 1\ (3)$, da er p trægt, hvis 2 er kub. ikke-rest, og $pR = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3$, hvis 2 er kub.rest.

SÆTNINGER FRA GEOMETRISK TALTEORI.

Minkowsky's Gitterpunktssætning. Lad $\Delta \subseteq R^n$ være en konveks symmetrisk mængden med $V(\Delta) > 2^n$, da findes mindst ét fra 0 forskelleigt gitterpunkt i Δ.

Bevis(Mordell). Ved hyperplanerne $x_1 = \frac{2p_1}{t}, \ldots, x_n = \frac{2p_n}{t}$, $p_1, \ldots, p_n \in Z$ inddeles rummet i terninger med volumen $(\frac{2}{t})^n$, $t \in \dot{N}$. Betegner $\mathcal{M}(t)$ antallet af hjørnespidser $\in \Delta$, vil $\mathcal{M}(t)(\frac{2}{t})^n \longrightarrow V(\Delta)$ for $t \longrightarrow \infty$, så for passende $t = t_0$ er iflg. foruds. $\mathcal{M}(t_0)(\frac{2}{t_0})^n > 2^n$:

$\mathcal{M}(t_o) > t_o^n$.
$(p_1,\ldots,p_n)$ bestemmer et af de t_o^n n-tupler af restklasser mod.t_o, og da $\mathcal{M}(t_o) > t_o^n$ findes $\underline{\alpha}' = (\frac{2p_1'}{t_o},\ldots,\frac{2p_n'}{t_o}) \in \Delta\Omega$, og $\underline{\alpha}'' = (\frac{2p_1''}{t_o},\ldots,\frac{2p_n''}{t_o}) \in \Delta\Omega$, så at $\underline{\alpha}' \neq \underline{\alpha}''$ og $p_i' \equiv p_i''$ (mod.t). Nu er $\frac{1}{2}(\underline{\alpha}'-\underline{\alpha}'') \in \Delta\Omega$, og $\frac{1}{2}(\underline{\alpha}'-\underline{\alpha}'') = (\frac{p_1'-p_1''}{t_o},\ldots,\frac{p_n'-p_n''}{t_o})$ er et gitterpunkt $\neq \underline{0}$. ∎

Minkowsky's lenearformsætning. Lad

$$L_1(\underline{x}) = a_{11}x_1+\ldots+a_{1n}x_n$$
$$\vdots$$
$$L_n(\underline{x}) = a_{n1}x_1+\ldots+a_{nn}x_n$$

være n reelle linearformer i n variable, og antag $D = \det(a_{ij}) \neq 0$. Hvis $\lambda_1,\ldots,\lambda_n > 0$, og $\lambda_1\ldots\lambda_n \geq |D|$, da findes et gitterpunkt $\underline{h} \neq \underline{0}$ så $|L_i(\underline{h})| \leq \lambda_i$, $i = 1,\ldots,n$.

Bevis. Lad $\varepsilon > 0$, og lad $\Delta\Omega$ være mængden af de $\underline{x} \in \dot{R}^n$ for hviske $|L_1(\underline{x})| \leq \lambda_1+\varepsilon$, $|L_2(\underline{x})| \leq \lambda_2,\ldots,|L_n(\underline{x})| \leq \lambda_n$, da er $\Delta\Omega$ konveks og symmetrixk. Ved $\underline{x} \longrightarrow (L_1(\underline{x}),\ldots,L_n(\underline{x}))$ vil $\Delta\Omega$ afhildes på et parallellepipidum $[-\lambda_1-\varepsilon,\lambda_1+\varepsilon]\times[-\lambda_2,\lambda_2]\times\ldots\times[-\lambda_n,\lambda_n]$, så $V(\Delta\Omega)|D| = 2(\lambda_1+\varepsilon)(2\lambda_2)\ldots(2\lambda_n)$, og altså $V(\Delta\Omega) > 2^n$.
Lad nu først $\varepsilon_1 > 0$, da findes et gitterpunkt $\underline{h} \neq \underline{0}$, så at $|L_1(\underline{h})| \leq \varepsilon_1+\lambda_1$, $|L_2(\underline{h})| \leq \lambda_2,\ldots,|L_n(\underline{h})| \leq \lambda_n$, og der kan kun findes endelig mange sådanne, og det er klart (!), at der for et af disse må gælde $|L_1(\underline{h})| \leq \lambda_1$. ∎

Minkewsky's linearformsætning. Lad $L_1,\ldots,L_n$ være komplekse linearformer, så at $\overline{L_i} \in \{L_j\}$ og antag $D = \det(a_{ij}) = \det(L_i) \neq 0$. Hvis $\lambda_1,\ldots,\lambda_n > 0$, så at det for komplekse L'er gælder at $\overline{L_i} = L_j \Rightarrow \lambda_i = \lambda_j$, og $\lambda_1\ldots\lambda_n \geq |D|$, da findes et gitterpunkt $\underline{h} \neq \underline{0}$, så at $|L_i(\underline{h})| \leq \lambda_i$.

Bevis. Antag $L_1,\ldots,L_{n_1}$ er reelle, $\overline{L_{n_1+1}} = L_{n_1+2},\ldots,\overline{L_{n_1+2n_2-1}} = L_{n_1+2n_2}$ (så $n = r_1+2r_2$). Lad $L_i' = L_i$, $i = 1,\ldots,r_1$, $L_{n_1+1}' = \frac{1}{2}(L_{n_1+1}+L_{n_1+2}) = \mathcal{R}e(L_{n_1+1})$, $L_{n_1+2}' = \frac{1}{2}(L_{n_1+1}-L_{n_1+2}) = \mathcal{I}m(L_{n_1+1})$, o.s.v. og $\lambda_i' = \lambda_i$, $i = 1,\ldots,r_1$, $\lambda_i' = \lambda_i/\sqrt{2}$, $i = r_1+1,\ldots,n$. Vi har nu

$$\begin{pmatrix} L_1' \\ \vdots \\ L_{n_1} \\ L_{n_1+1}' \\ L_{n_1+2}' \\ \\ L_n' \end{pmatrix} = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & \begin{matrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} \end{matrix} & \\ & & & & \ddots \\ & & & & & \boxed{\quad} \end{pmatrix} \begin{pmatrix} L_1 \\ \vdots \\ \\ \\ \\ L_n \end{pmatrix}$$

og altså $|\det L_i'| = (\frac{1}{2})^{n_2}|D| \prod_i\lambda_i' = (\frac{1}{\sqrt{2}})^{2n_2}\prod_i\lambda_i = (\frac{1}{2})^{n_2}\prod_i\lambda_i \geq |\det L_i'|$. Følgelig findes $\underline{h} \neq \underline{0}$, så $|L_i'(\underline{h})| \leq \lambda_i'$, altså $|L_i(\underline{h})| \leq \lambda_i$ $i = 1,\ldots,r$, $|L_{n_1+1}(\underline{h})| = |L_{n_1+2}(\underline{h})| = \sqrt{L_{n_1+1}'(\underline{h})^2+L_{n_1+2}'(\underline{h})^2} \leq \sqrt{\lambda_{n_1+1}'^2+\lambda_{n_1+2}'^2} = \lambda_{n_1+1} = \lambda_{n_1+2}$ o.s.v. ∎

En additiv vektorgruppe $\Lambda \subseteq \dot{R}^m$ kaldes et gitter, hvis der findes r ufafhængige (over $\dot{R}$, altså $r \leq n$) vektorer, $\underline{A}_1,\ldots,\underline{A}_r$, så $\Lambda = \{h_1\underline{A}_1+\ldots h_r\underline{A}_r \mid h_i \in \dot{Z}\}$.

Lemma. En additiv vektorgruppe $\Lambda \subseteq \dot{R}^m$ er et gitter $\Leftrightarrow \Lambda$ er diskret. (ɔ: ethvert begrænset område $\subseteq \dot{R}^m$ indeholder kun endelig mange vektorer $\in \Lambda$)

Bevis. "$\Rightarrow$" oplagt. "$\Leftarrow$": Induktion efter r = dim Λ (ɔ: et maximalt antal uafh. vekt.$\in \Lambda$): r = 1: Hvis $(0) \subset \Lambda$ findes en vektor $\underline{A} \neq \underline{0}$ med mindst mulig norm $\in \Lambda$, og en velkendt slutning viser nu, at $\Lambda = \{h\underline{A} \mid h \in \dot{Z}\}$. r-1 $\rightarrow$ r: Lad Λ være en diskret vektorgruppe af dim r, og vælg et maximalt antal uafh. $\underline{A}_1,\ldots,\underline{A}_r \in \Lambda$. Sæt $U = \{x_1\underline{A}_1+\ldots+x_{r-1}\underline{A}_{r-1} \mid x_i \in \dot{R}\}$, da er $U \cap \Lambda$ en diskret vektorgruppe af dim r-1, så der findes $\underline{B}_1,\ldots,\underline{B}_{r-1} \in U \cap \Lambda$, så at $U \cap \Lambda = \{h_1\underline{B}_1+\ldots+h_{r-1}\underline{B}_{r-1} \mid h_i \in \dot{Z}\}$. Nu er $\underline{B}_1,\ldots,\underline{B}_{r-1},\underline{A}_r$ uafh., så hver vektor $\underline{L} \in \Lambda$ kan entydigt skrives $\underline{L} = x_1\underline{B}_1+\ldots+x_{r-1}\underline{B}_{r-1}+y\underline{A}_r$, $x_i,y \in \dot{R}$. Ved $\underline{L} \longrightarrow y\underline{A}_r$ bestemmes derfor en homomorfi $\varphi : \Lambda \longrightarrow \{t\underline{A}_r \mid t \in \dot{R}\}$, med kernen $\varphi^{-1}(\underline{0}) = U \cap \Lambda$. $\varphi(\Lambda)$ er en additiv vektorgruppe, og diskret, thi er $y\underline{A}_r = \varphi(\underline{L}) \in \varphi(\Lambda)$, og $|y| \leq C$, har vi $y\underline{A}_r = \varphi(x_1\underline{B}_1+\ldots+x_{r-1}\underline{B}_{r-1}+y\underline{A}_r) = \varphi((x_1-[x_1])\underline{B}_1+\ldots+(x_{r-1}-[x_{r-1}])\underline{B}_{r-1}+y\underline{A}_r) = \varphi(z_1\underline{B}_1+\ldots+z_{r-1}\underline{B}_{r-1}+y\underline{A}_r)$, hvor $z_1\underline{B}_1+\ldots+z_{r-1}\underline{B}_{r-1}+y\underline{A}_r \in \Lambda$, og $z_i \in [0,1[$, $y \in [-C,C]$, men der findes kun endelig mange elementer i Λ med denne egenskab. Og dim $\varphi(\Lambda) = 1$. Følgelig findes $\tilde{\underline{A}} = y\underline{A}_r \in \varphi(\Lambda)$, så at $\varphi(\Lambda) = \{h\tilde{\underline{A}} \mid h \in \dot{Z}\}$.

Lad $\tilde{\underline{A}} = \varphi(\underline{B})$, hvor $\underline{B} \in \Lambda$, da er $\underline{B}_1,\ldots,\underline{B}_{r-1},\underline{B}$ en Z-basis for Λ, thi for $\underline{L} \in \Lambda$ er $\varphi(\underline{L}) = h\tilde{\underline{A}} = h\varphi(\underline{B})$, så at $\underline{L}-h\underline{B} \in \mathrm{Ker}\,\varphi = U \cap \Lambda$ ɔ: $\underline{L}-h\underline{B} = h_1\underline{B}_1+\ldots+h_{r-1}\underline{B}_{r-1}$. ▨

Minkowsky's diskriminantsætning. Hvis $K/\dot{Q}$ er endelig af grad $n > 1$, da er $|d_{K/\dot{Q}}| > 1$.

Bevis. Antag først n = 2, så $K = \dot{Q}(\sqrt{m})$. Vi har set, at $d = m, 4m$ for $m \equiv 1$ og $m \equiv 2,3$ resp (mod.4), så $|d| = 1$ indtræffer kun for $m = 1$, men så er $n = 1$.

Lad $K = \dot{Q}(\vartheta)$, lad $\vartheta^{(1)},\ldots,\vartheta^{(r_1)}$ være de r_1 reelle, og lad der være r_2 par af komplext konjugerede, $r_1+2r_2 = n$, konjugerede til ϑ. Vi kan antage, at $r_1+r_2 > 1$, thi ellers var enten $r_1 = 1$, $r_2 = 0$, n = 1, eller $r_2 = 0$, $r_1 = 1$, så n = 2, som vi har behandlet.

Lad $\omega_1,\ldots,\omega_m$ være en heltalsbasis for $K/\dot{Q}$, og sæt $L_i(\underline{x}) = \omega_1^{(i)}x_1+\ldots+\omega_m^{(i)}x_m$ for $\underline{x} \in \dot{R}$, i = 1,...,n; så vi finder da $|\det L_i| = |\det(\omega_j^{(i)})| = \sqrt{|d|}$. Antag nu, at |d| = 1, da er også $|\det L_i| = 1$. Vi vælger nu $\lambda_1 > 0$, og afpasser $\lambda_2,\ldots,\lambda_n$, så at forudsætningerne

i linearformsætningen er opfyldt, og så $\lambda_1 \ldots \lambda_n = 1$ (dette kan gøres, da $r + r \geq 1$). Følgelig findes et gitterpunkt $\underline{h} \neq \underline{0}$, så $|L_i(\underline{h})| \leq \lambda_i$, $i = 1,\ldots,n$. Vi har $L_i(\underline{h}) = h_1\omega_1^{(i)} + \ldots + h_n\omega_n^{(i)} = (h\omega_1 + \ldots + h_n\omega_n)^{(i)} = \alpha^{(i)}$, hvor $\alpha = h_1\omega_1 + \ldots + h_n\omega_n \in R\setminus(0)$. Da $N(\alpha) \neq 0$, er

$$1 \leq |N(\alpha)| = \prod |\alpha^{(i)}| \leq \prod \lambda_i = 1,$$

så at $=$ gælder hele vejen, hvoraf $|\alpha^{(i)}| = \lambda_i$, $i = 1,\ldots,n$, og specielt $|\alpha^{(1)}| = \lambda_1$. Dette kan dog ikke være rigtigt for alle λ_1 thi vælger vi fx $\lambda_1 > 0$ transcendent, findes intet $\alpha^{(1)}$ helt over $\mathbb{Z}$ så $|\alpha^{(1)}| = \lambda_1$ ($|\alpha^{(1)}| = \sqrt{\alpha^{(1)}\overline{\alpha}^{(1)}}$ er jo alg. over $\mathbb{Q}$) ∎

Korollar. <u>I enhver endelig udvidelse $K/\mathbb{Q}$ af grad > 1, findes forgrenede primtal</u>
iflg. den ubeviste del af Dedekinds diskriminantsætning.

Morsomhed. Der gælder altid $|d_{K/\mathbb{Q}}| \geq 3$ iflg. Stickelberger. (Men for $K = \mathbb{Q}(\sqrt{-3})$ er $|d_{K/\mathbb{Q}}| = 3$)

IDEALKLASSER

Lad $K/\mathbb{Q}$ være endelig, lad $\mathcal{J}$ være gruppen af brudne idealer i R, og lad $\mathcal{H}$ være undergruppen bestående af hovedidealer. Faktorgruppen $\mathcal{J}/\mathcal{H}$ kaldes <u>idealklassegruppen</u>. Den til $\mathcal{H}$ hørende ækvivalensrelation er $\mathfrak{a} \sim \mathfrak{b} \Leftrightarrow \mathfrak{a}\mathfrak{b}^{-1} \in \mathcal{H} \Leftrightarrow \exists \alpha \in K^*: \mathfrak{a} = \mathfrak{b}(\alpha)$.

Enhver <u>idealklasse</u> ($=$: en $\mathcal{H}$-sideklasse) indeholder et helt ideal, thi er $\mathfrak{a} \neq (0)$ findes $d \in R$, så $d\mathfrak{a}$ er helt, og $\mathfrak{a} \sim (d)\mathfrak{a}$. For hele idealer er $\mathfrak{a} \sim \mathfrak{b} \Leftrightarrow \exists \alpha, \beta \in R\setminus(0): (\alpha)\mathfrak{a} = (\beta)\mathfrak{b}$.

Opg. $\mathfrak{a} \sim \mathfrak{b} \Leftrightarrow \mathfrak{a}, \mathfrak{b}$ er isomorfe R-moduler.

Index $(\mathcal{J}:\mathcal{H})$ kaldes <u>klassetallet</u> (og vil blive "betegnet" h).

Sætning. 1) <u>Hvis $K/\mathbb{Q}$ er endelig, da er idealklassegruppen endelig.</u>
Endda: 2) <u>Enhver idealklasse indeholder et helt ideal $\mathfrak{c}$ med $\mathcal{N}(\mathfrak{c}) \leq \sqrt{|d|}$.</u>

Bevis. 2) $\Rightarrow$ 1), thi der findes kun endelig mange hele $\mathfrak{c}$, med $\mathcal{N}(\mathfrak{c}) \leq \sqrt{|d|}$, thi da $\mathfrak{c} \mid \mathcal{N}(\mathfrak{c})R$ (Vi har jo $\mathcal{N}(\mathfrak{c}) = \mathcal{N}(\mathfrak{c})\cdot 1 =$ 0 i $R/\mathfrak{c}$ $\supset$: $\mathcal{N}(\mathfrak{c}) \equiv 0$ $(\mathfrak{c})$), og ethvert fast helt ideal har kun endelig mange divisorer.

2): Lad $\mathcal{C} \in \mathcal{J}/\mathcal{H}$, og lad $\mathfrak{a} \in \mathcal{C}^{-1}$ være et helt ideal. Lad $\alpha_1, \ldots, \alpha_n$ være en $\mathbb{Z}$-basis for $\mathfrak{a}$, og sæt $L_i(\underline{x}) = x_1\alpha_1^{(i)} + \ldots + x_n\alpha_n^{(i)}$ for $x \in \mathbb{R}^n$, $i = 1,\ldots,n$. Vi har $|\det L_i| = |\det(\alpha_j^{(i)})| = |\sqrt{\Delta(\alpha_1,\ldots,\alpha_n)}| = |\sqrt{\mathcal{N}(\mathfrak{a})^2 d}| = \mathcal{N}(\mathfrak{a})\sqrt{|d|}$. Sæt $\lambda_i = \sqrt[n]{\mathcal{N}(\mathfrak{a})\sqrt{|d|}}$, da er $\prod \lambda_i = |\det L_i|$ så iflg. linearformsætningen findes et gitterpunkt $\underline{h} \neq \underline{0}$, så $|L_i(\underline{h})| \leq \lambda_i$. Sættes $\xi = h_1\alpha_1 + \ldots + h_n\alpha_n \in \mathfrak{a}$, er $\xi^{(i)} = L_i(\underline{h})$, så $|\xi^{(i)}| \leq$

$\sqrt{\mathcal{N}(\mathfrak{a})\sqrt{|d|}}$, og dermed $|N(\xi)| \leq \mathcal{N}(\mathfrak{a})\sqrt{|d|}$.
Da $(\xi) \subseteq \mathfrak{a}$, er $(\xi) = \mathfrak{a}\mathfrak{c}$; da $\mathfrak{a} \in \mathfrak{b}^{-1}$, og $(\xi) \in \mathfrak{H} = \textcircled{1}$, er $\mathfrak{c} \in \mathfrak{b}$, og af $|N(\xi)| = \mathcal{N}(\xi R) = \mathcal{N}(\mathfrak{a})\mathcal{N}(\mathfrak{c}) \leq \mathcal{N}(\mathfrak{a})\sqrt{|d|}$ følger $\mathcal{N}(\mathfrak{c}) \leq \sqrt{|d|}$. ∎

Eks. Den diofantiske ligning $x^p+y^p = z^p$. I $\dot{Q}(\xi) = \dot{Q}(e^{\frac{2\pi i}{p}})$ er $(x+y)(x+\xi y)\ldots(x+\xi^{p-1}y) = x^p+y^p = z^p$. Kummer har vist: Ingen løsning, hvis $p \nmid h$ = kl.tal $\dot{Q}(e^{\frac{2\pi i}{p}})$.

Eks. $\underline{K = \dot{Q}(\sqrt{-1})}$. $d = -4$, $\sqrt{|d|} = 2$ $\mathcal{N}(\mathfrak{c}) = 1 \Rightarrow \mathfrak{c} \sim 1$ og $\mathcal{N}(\mathfrak{c}) = 2 \Rightarrow \mathfrak{c} \mid 2R = \mathfrak{p}_2^2$, og da $N(1+\sqrt{-1}) = 2$, er $\mathfrak{p}_2 = (1+\sqrt{-1}) \sim 1$, og altså $\mathfrak{c} \sim 1$. Altså er $\underline{h = 1}$, så $R = \dot{Z}[\sqrt{-1}]$ er et P.I.D.

$\underline{K = \dot{Q}(\sqrt{-2})}$. $d = -8$, $\sqrt{|d|} = 2{,}8\ldots$. $\mathcal{N}(\mathfrak{c}) = 1 \Rightarrow \mathfrak{c} \sim 1$ og $\mathcal{N}(\mathfrak{c}) = 2 \Rightarrow$ (som for $m = -1$) $\mathfrak{c} \sim 1$, altså $\underline{h = 1}$, så $R = \dot{Z}[\sqrt{-2}]$ er P.I.D.

$\underline{K = \dot{Q}(\sqrt{-3})}$. $d = -3$, $d = 1{,}7\ldots$ $\mathcal{N}(\mathfrak{c}) = 1 \Rightarrow \mathfrak{c} \sim 1$, så $\underline{h = 1}$, og $R = \dot{Z}[\frac{1}{2}(-1+\sqrt{-3})]$ er et P.I.D.

$\underline{K = Q(\sqrt{-5})}$. $d = -20$, $d = 4,\ldots$ $\mathcal{N}(\mathfrak{c}) = 1 \Rightarrow \mathfrak{c} \sim 1$, $\mathcal{N}(\mathfrak{c}) = 2 \Rightarrow \mathfrak{c} \mid 2R = \mathfrak{p}_2^2$, og $\mathfrak{p}_2$ er ikke hovedideal(!), så $\mathfrak{c} \sim \{\begin{matrix}1\\ \mathfrak{p}_2\end{matrix}$. $\mathcal{N}(\mathfrak{c}) = 3 \Rightarrow \mathfrak{c} \mid 3R = \mathfrak{p}_3\bar{\mathfrak{p}}_3$. $\mathfrak{p}_3$ er ikke hovedideal, men $\mathfrak{p}_3 \sim \mathfrak{p}_2$, thi $\mathfrak{p}_2\mathfrak{p}_3 = (1+\sqrt{-5}) \sim 1$, og $\mathfrak{p}_2^2 = 2R = 2R \sim 1$, så $\mathfrak{p}_3 \sim \mathfrak{p}_2^2\mathfrak{p}_3 = \mathfrak{p}_2(\mathfrak{p}_2\mathfrak{p}_3) \sim \mathfrak{p}_2$, altså $\mathfrak{c} \sim \{\begin{matrix}1\\ \mathfrak{p}_2\end{matrix}$ $\mathcal{N}(\mathfrak{c}) = 4 \Rightarrow \mathfrak{c} \mid 4R = \mathfrak{p}_2^4 \Rightarrow \mathfrak{c} \sim \{\begin{matrix}1\\ \mathfrak{p}_2\end{matrix}$. Følgelig er $\underline{h = 2}$, og $R = \dot{Z}[\sqrt{-5}]$ er ikke P.I.D.

$\underline{K = Q(\sqrt{-6})}$ har $\underline{h = 2}$.

Det viser sig, at $\dot{Q}(\sqrt{-1}), \dot{Q}(\sqrt{-2}), \dot{Q}(\sqrt{-3}), \dot{Q}(\sqrt{-7}), \dot{Q}(\sqrt{-11}), \dot{Q}(\sqrt{-19}), \dot{Q}(\sqrt{-43}), \dot{Q}(\sqrt{-67})$ og $\dot{Q}(\sqrt{-163})$ har $h = 1$, og at der højst findes ét mere $m < 0$, så $\dot{Q}(\sqrt{m})$ har $h = 1$.

Man kan vise, at $h = h(m) \to \infty$ for $m \to -\infty$.

Sætning. $\underline{\text{Lad } K = \dot{Q}(\sqrt{m}),\ m < 0 \text{ kvadratfri, da er } h \text{ lige} \iff d \text{ indeholder mindst to forskellige primfaktorer.}}$

Bevis. "$\Leftarrow$". Vi viser, at der findes $\mathfrak{a} \neq 1$, så $\mathfrak{a}^2 \sim 1$. Vi har $d = 4m$ for $m \equiv 2,3\ (4)$, og $d = m$ for $m \equiv 1\ (4)$. Hvis $2 \mid d$, er altså $d = 4m$, så $2R = \mathfrak{p}_2^2$, og $\mathfrak{p}_2$ er ikke hovedideal, thi $2 = N(x+\sqrt{m}y) = x^2+|m|y^2$ har kun løsninger for $|m| = 1,2$ ɔ: $d = -4,-8$, som ikke indeholder to forsk. primfaktorer. Og hvis $2 \nmid d$, er $d = m$, så der findes $p \mid m$, så $p < |m|$, men så er $pR = \mathfrak{p}_p^2$, og $\mathfrak{p}_p$ er ikke hovedideal, da $p = x^2+|m|y^2$ ikke har løsninger.

"$\Rightarrow$". Indirekte: Antag d kun er delleligt med ét primtal. Hvis

dette er 2, er d = 4m, og m = -1,-2 i hvilket tilfælde vi har vist, at h = 1 ulige. Ellers er d = m = -p, og p ≡ 3 (4). Vi viser, at $\mathfrak{a}^2 \sim 1 \Rightarrow \mathfrak{a} \sim 1$. Nu er $\mathfrak{a}\bar{\mathfrak{a}} = \mathcal{N}(\mathfrak{a})R$ o: $\bar{\mathfrak{a}}\mathfrak{a} \sim 1$, hvoraf $\bar{\mathfrak{a}} \sim \mathfrak{a}^2\bar{\mathfrak{a}} = \mathfrak{a}(\mathfrak{a}\bar{\mathfrak{a}}) \sim \mathfrak{a}$, altså $(\alpha)\mathfrak{a} = (\beta)\bar{\mathfrak{a}}$, $\alpha,\beta \in R \setminus (0)$. Da $\mathcal{N}(\mathfrak{a}) = \mathcal{N}(\bar{\mathfrak{a}})$, er $N(\alpha) = \mathcal{N}(\alpha) = \mathcal{N}(\beta) = N(\beta)$ o: $\alpha\bar{\alpha} = \beta\bar{\beta}$. Vi kan antage, at $\alpha + \beta \neq 0$ (ti ellers kunne vi erstatte β med $-\beta$). Sæt $\mathfrak{c} = (\alpha+\beta)(\bar{\beta})\mathfrak{a}$, da er $\bar{\mathfrak{c}} = (\bar{\alpha}+\bar{\beta})(\beta)\bar{\mathfrak{a}} = (\bar{\alpha}\beta+\bar{\beta}\beta)\bar{\mathfrak{a}} = (\bar{\alpha}\beta+\alpha\bar{\alpha})\bar{\mathfrak{a}} = (\alpha+\beta)(\bar{\alpha})\bar{\mathfrak{a}} = (\alpha+\beta)(\bar{\beta})\mathfrak{a} = \mathfrak{c}$, og vi skal blot vise, at $\mathfrak{c} \sim 1$. Der findes ét forgrenet primtal, nemlig $pR = \mathfrak{p}^2$, så vi har $\mathfrak{c} = \mathfrak{p}^a \mathfrak{q}_1^{b_1}\bar{\mathfrak{q}}_1^{b_1'} \ldots \mathfrak{a}_1^{c_1} \ldots$ og dermed $\bar{\mathfrak{c}} = \mathfrak{p}^a \bar{\mathfrak{q}}_1^{b_1}\mathfrak{q}_1^{b_1'} \ldots \mathfrak{a}_1^{c} \ldots$ Af $\mathfrak{c} = \bar{\mathfrak{c}}$ (opløst / træge) følger nu, at $b_1 = b_1', \ldots$ men så er $\mathfrak{c} = \mathfrak{p}^a(\mathfrak{q}_1\bar{\mathfrak{q}}_1)^{b_1} \ldots \mathfrak{a}_1^{c_1} \ldots$ $\mathfrak{a}_1$ er trægt, og derfor hovedideal, ... $\mathfrak{q}_1\bar{\mathfrak{q}}_1 = \mathcal{N}(\mathfrak{q}_1)R$ er hovedideal, ..., og da $\sqrt{-p} \in \dot{Q}(\sqrt{-p})$, er $\mathfrak{p} = (\sqrt{-p})$ et hovedideal. ∎

ENHEDSGRUPPEN

Vi har $K = Q(\vartheta)$. De konjugerede nemmereres, så at $\vartheta^{(1)}, \ldots, \vartheta^{(r_1)}$ er de reelle, og $\vartheta^{(r_1+a)}, \vartheta^{(r_1+a)} = \vartheta^{(r_1+r_2+a)}$ $1 \leq a \leq r_2$ er de r_2 par af komplekst konjugerede; $n = r_1 + 2r_2$.

Vi stiler efter

Dirichlets enhedssætning. Enhedsgruppen er direkte produkt af den endelige cykliske gruppe bestående af enhedsrødderne i K, og r_1+r_2-1 uendelige cykliske grupper o: der fines E.R. $\zeta \in K$, og $r = r_1+r_2-1$ enheder $\varepsilon_1, \ldots, \varepsilon_r \in R$, så at enhver enhed ε entydigt kan skrives $\varepsilon = \zeta^a \varepsilon_1^{a_1} \ldots \varepsilon_r^{a_r}$, a mod. ord($\zeta$).

For $r_1 = 1$, $r_2 = 0$, er $K = \dot{Q}$, så $E = \{1,-1\}$; stemmer! For $r_1 = 0$, $r_2 = 1$, er $K = \dot{Q}(\sqrt{m})$, $m < 0$. For $m \equiv 2,3$ (4), er $(1,\sqrt{m})$ heltalsbasis, og $x+y\sqrt{m} \in E \Leftrightarrow x^2 + |m|y^2 = 1$; for $|m| = 1$ er altså $E = \{1,-1,\sqrt{-1},-\sqrt{-1}\}$, og for $|m| > 1$, er $E = \{1,-1\}$; stemmer! For $m \equiv 1$ (4), er $(1,\frac{1}{2}(1+\sqrt{m}))$ heltalsbasis, og $x+\frac{1}{2}y(1+\sqrt{m}) = \frac{1}{2}(2x+y)+\frac{1}{2}y\sqrt{m} = \frac{1}{2}(a+b\sqrt{m}) \in E$, $a+b \in 2\dot{Z} \Leftrightarrow 4 = a^2+|m|b^2$, for $|m| > 4$ er kun $(a,b) = (\pm 2,0)$, så $E = \{1,-1\}$ og for $|m| \leq 4$, er $m = -3$, $(a,b) = (\pm 2,0),(a,b) = (\pm 1,\pm 1)$, så $E = \{1,-1, \frac{1+\sqrt{-3}}{2}, \frac{-1+\sqrt{-3}}{2}, \frac{-1-\sqrt{-3}}{2}, \frac{1-\sqrt{-3}}{2}\} = \{e^{\frac{2\pi i a}{6}}\}$. stemmer!

Vi kan følgelig antage, at $r_1 + r_2 > 1$.

Lemma. Til $C > 0$ findes kun endelig mange hele $\xi \in R$, så $|\xi^{(i)}| \leq C$ for alle $i = 1, \ldots, n$.

Bevis. Sæt $f(X) = (X-\xi^{(1)})\ldots(X-\xi^{(n)}) \in Z[X]$. Vi har $f(X) = X^n + a_1X^{n-1} + \ldots + a_n$, $a_j \in \dot{Z}$ og $|a_1| = |-\xi^{(1)}-\ldots-\xi^{(n)}| \leq nC, \ldots, |a_j| = |\sum \xi^{(\nu_1)}\ldots\xi^{(\nu_j)}| \leq \binom{n}{j}C, \ldots$ så der findes kun endelig mange $f(X) \in Z[X]$, der opfylder dette, og dermed kun endelig mange ξ. ∎

Korollar 1. Enhedsrødderne i K udgør en endelig cyklisk gruppe.
Bevis. For en E.R. $\zeta \in K$ gælder $|\zeta^{(i)}| = 1$, så der findes kun endelig mange E.R. i K, og da disse således udgør en endelig undergruppe i K^*, er denne cyklisk. ∎

Korollar 2. Hvis $\xi \in R$, og $|\xi^{(i)}| = 1$, $i = 1,\ldots,n$, da er ξ E.R.
Bevis. Da $|(\xi^t)^{(i)}| = |(\xi^{(i)})^t| = 1$, er $\{1,\xi,\ldots,\xi^t,\ldots\}$ endelig iflg lemma, hvoraf påstanden ∎

Lad $\varepsilon \in R$ være en enhed, da er $N(\varepsilon) = \pm 1$, eller $\prod_{i=1}^{n} |\varepsilon^{(i)}| = 1$. Sættes $d_i = 1$, $1 \leq i \leq r_1$, $d_i = 2$, $r_1 < i \leq r_1+r_2$ kan dette skrives $\prod_{i=1}^{r_1+r_2} |\varepsilon^{(i)}|^{d_i} = 1$ eller

$$(*) \qquad \sum_{i=1}^{r_1+r_2} d_i \log |\varepsilon^{(i)}| = 0.$$

Ved $\varepsilon \to \underline{\ell}(\varepsilon) = (\log|\varepsilon^{(1)}|,\ldots,\log|\varepsilon^{(r_1+r_2-1)}|)$ defineres nu en afbildning $\underline{\ell} : E \to \dot{R}^{r_1+r_2-1} = \dot{R}^{r}$, og $\underline{\ell}$ er en homomorfi. Endvidere er $\underline{\ell}(E)$ en diskret additiv vektorgruppe i $\dot{R}^r$, thi ethvert begrænset område i $\dot{R}^r$ indeholder kun billeder af ε'er med $|\varepsilon^{(i)}|$, $i = 1,\ldots,r_1+r_2-1$ begrænset, og dermed iflg. (*): $|\varepsilon^{(i)}|$, $i = 1,\ldots,r_1+r_2$ begrænset, og dermed også $|\varepsilon^{(i)}|$, $i = 1,\ldots,n = r_1+2r_2$ begrænset. Af lemma følger nu, at mængden af desse ε'er er begrænset.
$\underline{\ell}(E)$ er følgelig et gitter af dim $\rho \leq r = r_1+r_2-1$, så $\underline{\ell}(E) = \{h_1\underline{\ell}(\varepsilon_1)+\ldots+h_\rho\underline{\ell}(\varepsilon_\rho) \mid h_i \in \dot{Z}\}$, hvor $\varepsilon_1,\ldots,\varepsilon_\rho \in E$. Iflg. (*) og korollar 2 er $\operatorname{Ker}\underline{\ell} = \{\text{E.R.} \in K\}$, altså cyklisk iflg. korollar 1, frembragt af E.R. $\zeta \in K$. For $\varepsilon \in E$, er $\underline{\ell}(\varepsilon) = h_1\underline{\ell}(\varepsilon_1)+\ldots+h_\rho\underline{\ell}(\varepsilon_\rho) = \underline{\ell}(\varepsilon_1^{h_1}\ldots\varepsilon_\rho^{h_\rho})$, hvor $h_i \in \dot{Z}$ er entydige, og dermed $\varepsilon = \zeta^a\varepsilon_1^{h_1}\ldots\varepsilon_\rho^{a_\rho}$ og a er bestemt mod. ord ζ.
I Enhedssætningen mangler vi nu blot at vise, at $\rho = r = r_1+r_2-1$. Vi har $\rho \leq r$, så det er nok at vise, at der findes r enheder $\varepsilon_1,\ldots,\varepsilon_r \in R$, så $\underline{\ell}(\varepsilon_1),\ldots,\underline{\ell}(\varepsilon_r)$ er uafh., hvilket er ensbetydende med $\det(\log|\varepsilon_i^{(j)}|)_{i,j=1,\ldots,r} \neq 0$ eller at

$$\begin{vmatrix} d_1\log|\varepsilon_1^{(1)}| & \ldots & d_r\log|\varepsilon_1^{(r)}| \\ \vdots & & \vdots \\ d_1\log|\varepsilon_r^{(1)}| & \ldots & d_r\log|\varepsilon_r^{(r)}| \end{vmatrix} \neq 0.$$

Først
Minkowsky's determinantsætning. Lad $\underline{\underline{A}} = (a_{ij}) \in \mathcal{M}_n(\dot{R})$, så at $a_{ij} \leq 0$, $i \neq j$, og $\sum_{j=1}^{n} a_{Ij} > 0$, $i = 1,\ldots,n$, da er $\det \underline{\underline{A}} \neq 0$.
Bevis. Indirekte, da findes $\underline{x} \neq \underline{0}$, så at $\underline{\underline{A}}\underline{x} = \underline{0}$. Vi kan antage, at $\max_i |x_i| = 1 = x_\nu$, men så er $0 =$

$$= (\underset{\nu\text{''}}{x_1 a_{\nu 1}}+\ldots+\underset{\nu\text{''}}{x_{\nu-1}\, a_{\nu,\nu-1}})+\underset{\text{''}}{x_\nu a_\nu}+(\underset{\nu\text{''}}{x_{\nu+1}\, a_{\nu,\nu+1}}+\ldots+\underset{\nu\text{''}}{x_m a_{\nu m}})$$
$$\geq (-|a_{\nu 1}|-\ldots-|a_{\nu,\nu-1}|)+a_\nu+(-|a_{\nu,\nu+1}|-\ldots-|a_{\nu m}|)$$
$$= a_{\nu 1}+\ldots+a_{\nu,\nu-1}+a_\nu+a_{\nu,\nu+1}+\ldots+a_{\nu m} > 0, \text{ modstrid.}$$

∎

Iflg. determinantsætningen er det nu nok at vise, at der findes r_2 enheder $\varepsilon_1,\ldots,\varepsilon_{r_2}$, så $|\varepsilon_i^{(i)}| > 1$ og $|\varepsilon_i^{(j)}| < 1$, $i \neq j$, $i = 1,\ldots,r$, $j = 1,\ldots,r+1=r_1+r_2$, thi da følger påstanden v.hj.a. (*).

Lad nu $\omega_1,\ldots,\omega_m$ være en heltalsbasis, sæt $\lambda = \sqrt[m]{\sqrt{|d|}} = |d|^{\frac{1}{2m}}$, lad $\gamma_1,\ldots,\gamma_\mu \in R\setminus(0)$ være de endelig(!) mange ikke-associerede hele tal, for hvilke $\mathcal{N}(\gamma_\mu) \leq \sqrt{|d|}$ Sæt $\lambda_1 = \max_{i,\nu} \frac{\lambda}{|\gamma_\mu{}^{(i)}|}$. Til $\underline{t} \in \dot{C}^n$, så $t_1,\ldots,t_{n_1} \in \dot{R}$, $\overline{t_{n_1+a}} = t_{n_1+n_2+a}$, $1 \leq a \leq r_2$, og $\prod |t_i| = 1$ sættes $L_i(\underline{x}) = t_i\omega_1^{(i)}x_1+\ldots+t_i\omega_m^{(i)}x_m$, $i = 1,\ldots,n$, $\underline{x} \in \dot{R}^m$. Vi har $|\det L_i| = |\det(t_i\omega_j^{(i)})| = |\prod t_i\sqrt{|d|}| = \sqrt{|d|} = \prod_1^m \lambda$, så iflg linearformsætningen findes et gitterpunkt $\underline{h} \neq \underline{0}$, så at $|L_i(\underline{h})| \leq \lambda$, $i = 1,\ldots,n$, eller $|t_i\gamma^{(i)}| \leq \lambda$, hvor $\gamma = h_1\omega_1+\ldots+h_m\omega_m \in R\setminus(0)$. Nu er $|N(\gamma)| = \prod|\gamma^{(i)}| = \prod|t_i\gamma^{(i)}| \leq \lambda^m = \sqrt{|d|}$, eller $\mathcal{N}(\gamma) \leq \sqrt{|d|}$, og vi har γ associeret med γ_ν, altså $\gamma = \varepsilon\gamma_\mu$, og $|t_i\varepsilon^{(i)}\gamma_\mu^{(i)}| \leq \lambda$, og dermed $|t_i\varepsilon^{(i)}| \leq \lambda/|\gamma_\mu^{(i)}| \leq \lambda_1$. Altså til $\underline{t}$ har vi fundet en enhed ε, så at $|t_i\varepsilon^{(i)}| \leq \lambda_1$.
Lad nu $1 \leq i \leq r = r_1+r_2-1$, og vælg $\underline{t} = (t_1,\ldots,t_m)$, så $t_j = 2\lambda_1$ for $j \neq i$ (og evt. for $j \neq i+r_2$, hvis $i > r_1$), og afstem t_i (og evt. $t_{i+n_2} = \overline{t_i}$), så at $\prod_i|t_i| = 1$, da findes en enhed ε_i, så $|t_j\varepsilon_i^{(j)}| \leq \lambda_1$, eller $|\varepsilon_i^{(j)}| \leq \lambda_1/t_j = \frac{1}{2} < 1$, for $j \neq i$.

Hermed er beviset for Direchlets enhedssætning fuldført. ∎

Eks. $K = \dot{Q}(\sqrt{m})$, $m > 0$. $r_1 = 2$, $r_2 = 0$, $r = r_1+r_2-1 = 1$. Enhedsrødderne i K er ± 1, så $E = \{\pm\varepsilon^h \mid h \in \dot{Z}\}$, men $x+y\sqrt{m} \in E \iff x^2-my^2 = \pm 1$, altså Pell's ligning.