Matematik 211, 1974

Anders Thorup

Algebraiske elementer

Håndskrevne noter fra algebranoterne

ALGEBRAISKE ELEMENTER

ALGEBRAISKE ELEMENTER

I det følgende betegner L et legeme.

1. Algebraiske elementer.

1.1. Vi minder om, at en L-algebra (også kaldet en algebra over L) er en ring A, i hvilken der er givet en ringhomomorfi $\varphi: L \to A$, således at

$$\varphi(\lambda)a = a\varphi(\lambda), \quad \lambda \in L, \ a \in A.$$

Algebraen kan betegnes (A, φ) eller blot A.

Er (A, φ) en L-algebra, sætter vi

$$\lambda a = \varphi(\lambda)a, \quad \lambda \in L, \ a \in A$$

Afbildningen $(\lambda, a) \mapsto \lambda a$ er en ydre komposition $L \times A \to A$, og det er let at se, at A med denne ydre komposition som multiplikation med skalar og med den givne addition (i ringen A) er organiseret som et vektorrum over L. Det ses, at vi har

$$(\lambda a)b = a(\lambda b) = \lambda(ab), \quad \lambda \in L, \ a, b \in A,$$

og homomorfien $\varphi: L \to A$ er afbildningen $\lambda \mapsto \lambda 1$, hvor 1 er et-elementet i ringen A.

Er der omvendt givet en mængde A forsynet med kompositioner

$A \times A \to A$ betegnet $(a, b) \mapsto a + b$

$A \times A \to A$ betegnet $(a, b) \mapsto a \cdot b$

$L \times A \to A$ betegnet $(\lambda, a) \mapsto \lambda a$,

således at

1) $(A, +, \cdot)$ er en ring
2) $(A, +, L)$ er et vektorrum
3) $(\lambda a) \cdot b = a(\lambda b) = \lambda(a \cdot b)$ for $\lambda \in L$, $a, b \in A$,

så organiseres ringen A ved afbildningen $\lambda \mapsto \lambda 1$ til en algebra over L.

. DEFINITION. Lad A være en L-algebra. Dimensionen af A som vektorrum over L, kaldes da A's dimension, og betegnes $|A:L|$. En endeligdimensional algebra kaldes også en endelig algebra.

1.2 Algebraen $Mat_n(L)$ af $(n\times n)$-matricer med koefficienter i L har dimensionen n^2 over L, idet en basis udgøres af matricerne ε_{ij}, $i,j = 1,\dots,n$, hvor ε_{ij} har 1 på plads (i,j) og 0 på de øvrige pladser. Er V et n-dimensionalt vektorrum over L, har vi også

$$|End_L(V) : L| = n^2,$$

idet vi efter et valg af basis i V får en isomorfi $End_L(V) \simeq Mat_n(L)$.

Algebraen $L[X]$ af polynomier med koefficienter i L er ikke endelig. Polynomierne $1, X, X^2, \dots$ er en L-basis for $L[X]$. For en kvotient $L[X]/(f)$, hvor $f \neq 0$ er et polynomium af grad n, finder vi

$$|L[X]/(f) : L| = \deg f = n,$$

idet elementerne $\textcircled{1}, \textcircled{X}, \textcircled{X}^2, \dots, \textcircled{X}^{n-1}$ er en L-basis for kvotienten.

$\mathbb{R}$, $\mathbb{C}$ og $\mathbb{H}$ ($\mathbb{H}$ er kvaternionskerlegemet) er endelige $\mathbb{R}$-algebraer. Vi har

$$|\mathbb{R}:\mathbb{R}| = 1, \quad |\mathbb{C}:\mathbb{R}| = 2, \quad |\mathbb{H}:\mathbb{R}| = 4.$$

1.3. Vi minder om at vi svarende til et element α i L-algebraen A har en homomorfi $L[X] \to A$ givet ved $p \mapsto p(\alpha)$, hvor vi for et polynomium

$$p = \lambda_0 + \lambda_1 X + \cdots + \lambda_n X^n \in L[X]$$

har sat

$$p(a) = \lambda_0 1 + \lambda_1 a + \cdots + \lambda_n a^n \in A.$$

Billedet, der betegnes $L[a]$, er den mindste delalgebra af A, som indeholder a, og kernen $\{p \in L[X] \mid p(a)=0\}$ består af de polynomier, der har a som rod. Ifølge isomorfisætningen har vi en L-isomorfi

$$L[X] / \text{kernen} \xrightarrow{\sim} L[a].$$

Kernen $\{p \in L[X] \mid p(a) = 0\}$ er et ideal. Da L er et legeme, er $L[X]$ en hovedidealring; så dette ideal er enten (0) eller af formen (f), med en entydigt bestemt normeret frembringer f.

DEFINITION. Elementet a i L-algebraen A kaldes <u>transcendent (over L)</u>, hvis der for hvert polynomium $p \in L[X]$, $p \neq 0$, gælder $p(a) \neq 0$. Elementet a i A kaldes <u>algebraisk (over L)</u>, hvis der findes polynomier $p \neq 0$ i $L[X]$, så at $p(a) = 0$. Den normerede frembringer for idealet $\{p \in L[X] \mid p(a) = 0\} \subseteq L[X]$ kaldes da <u>a's minimale polynomium</u> og betegnes $f_{a/L}$. Har $f_{a/L}$ graden n, siger vi, at a er <u>algebraisk af grad n</u>

Det minimale polynomium $f_{a/L}$ har altså a som rod, og ethvert polynomium i $L[X]$, der har a som rod, er et multiplum af $f_{a/L}$.

1.4. Hvis $a \in A$ er transcendent, så er homomorfien $p \mapsto p(a)$ en isomorfi : $L[X] \to L[a]$. Elementerne $1, a, a^2, \ldots$ er derfor en L-basis for $L[a]$; specielt er $|L[a] : L| = \infty$.

Hvis $a \in A$ derimod er algebraisk, så inducerer homomorfien $p \mapsto p(a)$ en isomorfi : $L[X]/(f_{a/L}) \xrightarrow{\sim} L[a]$.

Er α algebraisk af grad n, altså $n = \deg f_{\alpha/L}$, så er elementerne $1, \alpha, \dots, \alpha^{n-1}$ derfor en L-basis for $L[\alpha]$. Vi har altså

$$|L[\alpha] : L| = n$$

Specielt er altså $|L[\alpha] : L| < \infty$ i dette tilfælde, så vi slutter:

SÆTNING. *Elementet α i L-algebraen A er algebraisk, hvis og kun hvis delalgebraen $L[\alpha]$ er endelig.*

KOROLLAR. *Hvis A er en endelig L-algebra, så er hvert element α i A algebraisk over L af grad $\leq |A:L|$.*
thi $L[\alpha]$ er specielt et underrum i A.

1.5. Er V et n-dimensionalt vektorrum over L, har vi $|\mathrm{End}_L(V) : L| = n^2$. Enhver endomorfi $u \in \mathrm{End}_L(V)$ er altså algebraisk over L af grad $\leq n^2$. Her gælder som bekendt, at enhver endomorfi $u \in \mathrm{End}_L(V)$ er rod i sit karakteristiske polynomium $\chi_u(X) = \det(u - X1)$. Det minimale polynomium $f_{u/L}$ er derfor divisor i det karakteristiske polynomium χ_u. Specielt er altså $\deg f_{u/L} \leq n$. Eksempel: Matricerne

$$\begin{pmatrix} 0&0&0\\0&0&0\\0&0&0 \end{pmatrix}, \begin{pmatrix} 1&0&0\\0&1&0\\0&0&1 \end{pmatrix}, \begin{pmatrix} \lambda&1&0\\0&\lambda&0\\0&0&\mu \end{pmatrix}, \begin{pmatrix} \lambda&0&0\\0&\lambda&0\\0&0&\mu \end{pmatrix}, \begin{pmatrix} \lambda&0&0\\0&\mu&0\\0&0&\nu \end{pmatrix}, \begin{pmatrix} 0&1\\-1&0 \end{pmatrix},$$

hvor $\lambda, \mu, \nu \in L$ er forskellige, har som minimale polynomier

$$X,\ X-1,\ (X-\lambda)^2(X-\mu),\ (X-\lambda)(X-\mu),\ (X-\lambda)(X-\mu)(X-\nu),\ X^2+1.$$

Elementet $i \in \mathbb{C}$ har det minimale polynomium $f_{i/\mathbb{R}} = X^2+1$. Hvert element i $\mathbb{C}$ er algebraisk over $\mathbb{R}$ af grad ≤ 2.

For en kvaternion $\xi = \lambda_0 + \lambda_1 i + \lambda_2 j + \lambda_3 k \in \mathbb{H}$, $\lambda_0, \lambda_1, \lambda_2, \lambda_3 \in \mathbb{R}$ sættes $\overline{\xi} = \lambda_0 - \lambda_1 i - \lambda_2 j - \lambda_3 k$. Ved udregning finder vi $\xi + \overline{\xi} = 2\lambda_0 \in \mathbb{R}$, $\overline{\xi}\xi = \lambda_0^2 + \lambda_1^2 + \lambda_2^2 + \lambda_3^2 \in \mathbb{R}$.

Polynomiet $\chi_\xi(X) = X^2 - (\xi + \bar{\xi})X + \bar{\xi}\xi$ har således reelle koefficienter, og da det øjensynlig har ξ som rod, slutter vi, at ξ er algebraisk over $\mathbb{R}$ af grad ≤ 2. Vi ser, at det minimale polynomium $f_{\xi/\mathbb{R}}$ er divisor i χ_ξ, og dermed af grad 1 eller 2. Hvis $\xi \notin \mathbb{R}$, er grad 1 udelukket, således at vi i dette tilfælde har $f_{\xi/\mathbb{R}} = \chi_\xi$. Er derimod $\xi \in \mathbb{R}$, finder vi $f_{\xi/\mathbb{R}} = X - \xi$, $\chi_\xi = (X-\xi)^2$.

2. Udvidelser.

2.1. DEFINITION. Ved en udvidelse af legemet L vil vi her forstå et legeme K i hvilket der er givet en homomorfi: $L \to K$. Vi siger også, at K/L er en udvidelse. Den givne homomorfi: $L \to K$ kaldes indlejringen. Den er nødvendigvis injektiv (idet dens kerne er et ideal i L, som ikke kan være hele L (!), og som derfor må være (0)). Ofte identificerer vi elementerne i L med deres billeder i K ved indlejringen, og tænker altså på L som et dellegeme af K. Vi skriver da $L \hookrightarrow K$.

2.2. DEFINITION. Er K/L en udvidelse, kan vi specielt opfatte K som L-algebra. Dimensionen $|K:L|$ kaldes udvidelsens grad. Er $|K:L| < \infty$, kaldes K/L en endelig udvidelse. Er hvert element i K algebraisk over L, siger vi, at K/L er en algebraisk udvidelse.

2.3. SÆTNING. Enhver endelig udvidelse K/L er algebraisk

Bevis. Følger umiddelbart af korollar 1.4 ▨

2.4. Eksempel. $\mathbb{C}/\mathbb{R}$ er en endelig udvidelse. $\mathbb{C}/\mathbb{Q}$ og $\mathbb{R}/\mathbb{Q}$ er uendelige udvidelser.

2.5. Det er klart, at en fællesmængde af dellegemer (resp. delringe) af et legeme K igen er et dellegeme (resp. en delring) af K.

Er der givet en udvidelse $L \hookrightarrow K$, og en

vilkårlig delmængde $S \subseteq K$, kan vi betragte det mindste dellegeme (resp. den mindste delring) af K, som indeholder L og S. Herfor bruges betegnelsen $L(S)$ (resp. $L[S]$). Vi kan opfatte $L(S)$ som en udvidelse: $L \hookrightarrow L(S)$, udvidelsen frembragt af S. Det ses let, at delringen $L[S] \subseteq K$ består af alle endelige L-linearkombinationer af elementer af formen

$$s_1 \cdots s_p, \quad \text{hvor } s_1, \ldots, s_p \in S, \ p \geq 0,$$

og at $L(S)$ er (isomorft med) brøklegemet for $L[S]$.

Er $S = \{s_1, \ldots, s_n\} \subseteq K$ en endelig delmængde, bruges også betegnelserne $L(s_1, \ldots, s_n)$ (resp. $L[s_1, \ldots, s_n]$). Det er klart, at vi i dette tilfælde har

$$L(s_1, \ldots, s_n) = L(s_1, \ldots, s_{n-1})(s_n).$$

Vi siger også, at udvidelsen $L \hookrightarrow L(S)$ fremkommer ved at adjungere elementerne i S til L.

2.6. SÆTNING. *Lad der være givet en udvidelse $L \hookrightarrow K$ og et element $\alpha \in K$. Hvis α er transcendent over L, har vi en isomorfi*

$$L[X] \xrightarrow{\sim} L[\alpha],$$

og dermed en isomorfi mellem brøklegemerne

$$L(X) \xrightarrow{\sim} L(\alpha)$$

Specielt er altså $L \hookrightarrow L(\alpha)$ en uendelig udvidelse.

Hvis α derimod er algebraisk over L, så er det minimale polynomium $f_{\alpha/L}$ et irreducibelt polynomium, ringen $L[\alpha]$ er et legeme, og vi har en isomorfi

$$L[X]/(f_{\alpha/L}) \xrightarrow{\sim} L[\alpha] = L(\alpha)$$

Specielt er $L \hookrightarrow L(\alpha)$ en endelig udvidelse med $|L(\alpha) : L| = \deg f_{\alpha/L}$.

Bevis. Til tilfældet, hvor α er transcendent, følger umiddelbart af overvejelserne i 1.4.

Er α algebraisk, har vi en isomorfi

$$L[X]/(f_{\alpha/L}) \xrightarrow{\sim} L[\alpha].$$

Kvotienten $L[X]/(f_{\alpha/L})$ er således isomorf med en delring af et legeme, og er derfor et integritetsområde. Dit følger, at idealet $(f_{\alpha/L})$ er et primideal. Polynomiet $f_{\alpha/L} \neq 0$ er derfor et primelement i $L[X]$, og specielt irreducibelt. Da $L[X]$ er en hovedidealring, kan vi slutte, at idealet $(f_{\alpha/L})$ endda er et maksimalidеal, og dermed, at kvotienten $L[X]/(f_{\alpha/L}) \xrightarrow{\sim} L[\alpha]$ er et legeme. Vi har derfor $L[\alpha] = L(\alpha)$. Den sidste påstand følger nu klart af 1.4 ▨

2.7. Lad der være givet en udvidelse $L \hookrightarrow K$, og i K et element α, der er algebraisk over L med det minimale polynomium

$$f_{\alpha/L} = X^n + p_{n-1}X^{n-1} + \cdots + p_1 X + p_0 \in L[X].$$

Elementerne ξ i $L[\alpha]$ har da en fremstilling

$$\xi = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1},$$

hvor koefficienterne $a_0, \ldots, a_{n-1} \in L$ er entydigt bestemte. For et produkt $\xi\eta$ finder vi den tilhørende fremstilling ved at bruge $\alpha^n = -p_0 - p_1\alpha - \cdots - p_{n-1}\alpha^{n-1}$. Elementerne i brøklegemet $L(\alpha)$ er af formen

$$\xi/\eta = \frac{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}}{b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}}$$

hvor $(b_0, \ldots, b_{n-1}) \neq (0, \ldots, 0)$. Ifølge sætningen har

vi $L(\alpha) = L[\alpha]$. Brøken ξ/η kan altså entydigt skrives

$$\xi/\eta = z_0 + z_1\alpha + \cdots + z_{n-1}\alpha^{n-1}, \quad z_0, \ldots, z_{n-1} \in L.$$

For at bestemme koefficienterne $z_0, \ldots, z_{n-1}$ udregner vi $\eta(z_0 + \cdots + z_{n-1}\alpha^{n-1}) = (b_0 + \cdots + b_{n-1}\alpha^{n-1})(z_0 + \cdots + z_{n-1}\alpha^{n-1})$ under brug af $\alpha^n = -p_0 - \cdots - p_{n-1}\alpha^{n-1}$, og sammenligner med $\xi = a_0 + \cdots + a_{n-1}\alpha^{n-1}$. Herved fremkommer et lineært ligningssystem til bestemmelse af $z_0, \ldots, z_{n-1}$.

2.8 Eksempel. Elementet $\alpha = \sqrt[3]{2} \in \mathbb{R}$ er algebraisk over $\mathbb{Q}$, idet det er rod i polynomiet $X^3 - 2$. Det minimale polynomium $f_{\sqrt[3]{2}/\mathbb{Q}}$ er altså divisor i $X^3 - 2$; og da $X^3 - 2 \in \mathbb{Q}[X]$ er et irreducibelt polynomium, må vi have $f_{\sqrt[3]{2}/\mathbb{Q}} = X^3 - 2$.
Udvidelsen $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ har altså grad 3: En basis er $1, \sqrt[3]{2}, (\sqrt[3]{2})^2$. F.eks. finder vi

$$\frac{1 + \sqrt[3]{2}}{1 + 2\sqrt[3]{2}} = \frac{-5}{3} - \frac{1}{3}\sqrt[3]{2} + \frac{2}{3}(\sqrt[3]{2})^2$$

2.9. SÆTNING. *Lad $L \subset K$ være en endelig udvidelse, og lad V være et endeligdimensionalt vektorrum over K. Da er V også et endeligdimensionalt vektorrum over L, og*

$$\dim_L V = (\dim_K V)\,|K : L|.$$

Bevis. Lad $v_1, \ldots, v_n \in V$ være en K-basis for V, og lad $\alpha_1, \ldots, \alpha_p \in K$ være en L-basis for K. Vi viser, at de np elementer $\alpha_i v_j \in V$, $i = 1, \ldots, p$; $j = 1, \ldots, n$ er en L-basis for V:

De er et frembringersystem, thi hver vektor $v \in V$ kan skrives som K-linearkombination af vektorerne $v_1, \ldots, v_m$, og her kan hver af koefficienterne skrives som L-linearkombination af elementerne $\alpha_1, \ldots, \alpha_p$. Indsættes får vi v skrevet som L-linearkombination af vektorerne $\alpha_i v_j$.

De er uafhængige, thi en linear relation

$$\sum a_{ij} (\alpha_i v_j) = 0, \qquad a_{ij} = 0,$$

kan skrives $\sum_j \left(\sum_i a_{ij} \alpha_i \right) v_j = 0.$

For hvert j er $\sum_i a_{ij} \alpha_i \in K$, og da v_j'erne er K-uafhængige kan vi slutte, at $\sum_i a_{ij} \alpha_i = 0$, og da α_i'erne er L-uafhængige, kan vi heraf slutte $a_{ij} = 0$ for hvert i. ∎

2.10. SÆTNING. *Lad der være givet udvidelsen $L \hookrightarrow K$ og $K \hookrightarrow M$. Udvidelsen $L \hookrightarrow M$ er da endelig, hvis og kun hvis begge udvidelserne $L \hookrightarrow K$ og $K \hookrightarrow M$ er endelige. Hvis det er tilfældet, har vi*

$$|M : L| = |M : K| \, |K : V|.$$

Bevis. "hvis" fås ved at anvende sætning 2.9 på M opfattet som vektorrum over K.

"kun hvis": Er M endelig dimensionalt som vektorrum over L, så er underrummet K ligeledes endelig dimensionalt over L. Er $v_1, \ldots, v_n \in M$ en L-basis for M, så kan hvert element i M skrives som en L-linearkombination. Her er koefficienterne elementer i $L \hookrightarrow K$, så $v_1, \ldots, v_n$ er også et K-frembringersystem for M.

Følgelig er M et endeligdimensionalt vektorrum over K ▨

2.11. SÆTNING.

Lad der være givet en udvidelse $L \hookrightarrow K$ og elementer $\beta_1, \dots, \beta_n \in K$, der er algebraiske over L. Da er $L[\beta_1, \dots, \beta_n] = L(\beta_1, \dots, \beta_n)$, og udvidelsen $L \hookrightarrow L(\beta_1, \dots, \beta_n)$ er en endelig udvidelse.

Bevis. Vi viser påstanden ved induktion efter n. Den er klart rigtig for $n = 0$. Er $n \geq 1$ og er påstanden rigtig for $n-1$, så er $L[\beta_1, \dots, \beta_{n-1}] = L(\beta_1, \dots, \beta_{n-1})$, og $L \hookrightarrow L(\beta_1, \dots, \beta_{n-1})$ er en endelig udvidelse. Elementet β_n er algebraisk over L, altså rod i et polynomium $\neq 0$ med koefficienter i L. Da disse koefficienter også tilhører det størrelegeme $L' = L(\beta_1, \dots, \beta_{n-1})$, er β_n algebraisk over L'. Af sætning 2.6 følger derfor, at $L'(\beta_n) = L'[\beta_n]$ og at udvidelsen $L' \hookrightarrow L'(\beta_n)$ er endelig. Nu er $L'(\beta_n) = L(\beta_1, \dots, \beta_{n-1})(\beta_n) = L(\beta_1, \dots, \beta_n)$, og vi finder

$$\begin{aligned} L[\beta_1, \dots, \beta_n] &= L[\beta_1, \dots, \beta_{n-1}][\beta_n] = L(\beta_1, \dots, \beta_{n-1})[\beta_n] \\ &= L'[\beta_n] = L'(\beta_n) \\ &= L(\beta_1, \dots, \beta_n), \end{aligned}$$

og da udvidelserne $L \hookrightarrow L'$ og $L' \hookrightarrow L'(\beta_n) = L(\beta_1, \dots, \beta_n)$ begge er endelige, slutter vi af sætning 2.10, at også udvidelsen $L \hookrightarrow L(\beta_1, \dots, \beta_n)$ er endelig ▨

2.12. SÆTNING. Lad der være givet en udvidelse $L \hookrightarrow K$. Delmængden $\bar{L} \subseteq K$ bestående af de elementer $\alpha \in K$, der er algebraiske over L, er da et delegeme (som indeholder L).

Bevis. Sætningen udsiger, at dersom elementer $\alpha, \beta \in K$ er algebraiske over L, så er også summen $\alpha+\beta$, differensen $\alpha-\beta$, produktet $\alpha\beta$ og (dersom $\beta \neq 0$) kvotienten $\frac{\alpha}{\beta}$ algebraiske over L. Disse elementer tilhører alle dellegemet $L(\alpha,\beta) \subseteq K$. Af sætning 2.11 følger, at $L \hookrightarrow L(\alpha,\beta)$ er en endelig udvidelse, og dette medfører (sætning 2.3), at alle elementer i $L(\alpha,\beta)$ er algebraiske over L ▨

2.13. DEFINITION. Er $L \hookrightarrow K$ en udvidelse, så kaldes dellegemet

$$\bar{L} = \{\alpha \in K \mid \alpha \text{ er algebraisk over } L\}$$

for L's <u>algebraiske afslutning i K</u>. Det er klart, at $L \hookrightarrow \bar{L}$ er en algebraisk udvidelse, og at $\bar{L}$ er det største dellegeme $L \hookrightarrow L' \subseteq K$, som er algebraisk over L.

2.14 SÆTNING. <u>Lad der være udvidelser $L \hookrightarrow K$ og $K \hookrightarrow M$. Udvidelsen $L \hookrightarrow M$ er da algebraisk, hvis og kun hvis begge udvidelserne $L \hookrightarrow K$ og $K \hookrightarrow M$ er algebraiske.</u>

Bevis. "hvis". Vi skal vise, at hvert $\beta \in M$ er algebraisk over L. Nu er β algebraisk over K, altså rod i et polynomium $X^n + \alpha_1 X^{n-1} + \ldots + \alpha_n$ med koefficienter $\alpha_1, \ldots, \alpha_n \in K$. Disse koefficienter tilhører naturligvis dellegemet $L(\alpha_1, \ldots, \alpha_n)$, så β er algebraisk over dette dellegeme, og $L(\alpha_1, \ldots, \alpha_n) \hookrightarrow L(\alpha_1, \ldots, \alpha_n)(\beta) = L(\alpha_1, \ldots, \alpha_n, \beta)$ er en endelig udvidelse. Elementerne $\alpha_1, \ldots, \alpha_n$ tilhører K, og er derfor algebraiske over L. Af sætning 2.11 følger derfor, at også $L \hookrightarrow L(\alpha_1, \ldots, \alpha_n)$ er en endelig udvidelse; Sætning 2.10 viser nu først, at $L \hookrightarrow L(\alpha_1, \ldots, \alpha_n)(\beta)$ er endelig, og dernæst, at den mindre udvidelse $L \hookrightarrow L(\beta)$

er endelig. Følgelig er β algebraisk over L.
"kun hvis" er trivielt ▨

2.15. Vi ser specielt, at dersom vi for en udvidelse $L \hookrightarrow K$ betragter den algebraiske afslutning $\overline{L}$ af L i K, så vil hvert element i K, der er algebraisk over $\overline{L}$, selv tilhøre $\overline{L}$.

2.16. DEFINITION. Legemet L kaldes <u>algebraisk afsluttet</u> der som det opfylder en af følgende (ækvivalente) betingelser

(i) Ethvert polynomium $f \in L[X]$ af grad ≥ 1 har en rod i L

(ii) Ethvert polynomium $f \in L[X]$ af grad $n \geq 1$ kan skrives på formen

$$f = a(X-\alpha_1)\cdots(X-\alpha_n), \quad a, \alpha_1, \ldots, \alpha_n \in L$$

(iii) De irreducible polynomier i $L[X]$ er netop 1ste grads polynomierne.

(At disse betingelser er ækvivalente følger af, at $f \in L[X]$ har roden α, hvis og kun hvis $X-\alpha$ er divisor i f. Således ser vi, at <u>(i) $\Rightarrow$ (ii)</u>, ved at skrive $f = (X-\alpha_1)f_2$, hvor α_1 er en rod i f, dernæst skrive $f_2 = (X-\alpha_2)f_3$, og fortsætte indtil vi efter n skridt har $f = (X-\alpha_1)\cdots(X-\alpha_n)f_{n+1}$, hvor f_{n+1} har grad 0, og således er konstant.
<u>(ii) $\Rightarrow$ (i)</u> er klart, <u>(ii) $\Rightarrow$ (iii)</u> er klart, idet de eneste irreducible polynomier af formen i (ii) øjensynlig er 1ste-grads polynomier, og <u>(iii) $\Rightarrow$ (ii)</u>, thi hvert $f \in L[X]$ af grad ≥ 1 kan skrives har en primopløsning $f = a p_1 \cdots p_n$, hvor $p_1, \ldots, p_n$ er normerede, irreducible polynomier (og $a \in L^*$).

Er $p_1, \ldots, p_n$ 1ste-grads polynomier, er dette netop en fremstilling som ønsket.)

2.17. Som bekendt udsiger algebraens fundamentalsætning, at legemet $\mathbb{C}$ af komplekse tal er algebraisk afsluttet.
Tal i $\mathbb{C}$, der er algebraiske over $\mathbb{Q}$, kaldes <u>algebraiske tal</u>. Disse tal udgør altså et legeme $\overline{\mathbb{Q}} \subseteq \mathbb{C}$, den algebraiske afslutning af $\mathbb{Q}$ i $\mathbb{C}$. Der gælder nu, at også <u>legemet $\overline{\mathbb{Q}}$ af algebraiske tal er et algebraisk afsluttet legeme</u>. Et polynomium $f \in \overline{\mathbb{Q}}[X]$ af grad ≥ 1 har nemlig en rod $\alpha \in \mathbb{C}$. Denne rod α er algebraisk over $\overline{\mathbb{Q}}$, og da $\overline{\mathbb{Q}}$ er algebraisk over $\mathbb{Q}$, slutter vi, at α er algebraisk over $\mathbb{Q}$, og dermed at $\alpha \in \overline{\mathbb{Q}}$.

Det er velkendt, at udvidelsen $\mathbb{Q} \hookrightarrow \mathbb{C}$ ikke er en algebraisk udvidelse. Vi har altså $\overline{\mathbb{Q}} \subset \mathbb{C}$.
[At der findes elementer i $\mathbb{C}$, der er transcendente over $\mathbb{Q}$ kan enten vises ved et kardinalitetsargument ($\mathbb{Q}$ og dermed $\mathbb{Q}[X]$ og dermed $\overline{\mathbb{Q}}$ er numerable mængder, $\mathbb{C}$ er ikke numerabel) eller ved at bevise, at visse analytisk definerede tal er transcendente. Således kan man vise, at e og π er transcendente tal].

2.18 Lad $c > 0$ være et reelt tal. Lad os et øjeblik sige, at en følge (r_n) af rationale tal er <u>c-konvergent</u> (mod $\xi \in \mathbb{R}$), hvis elementerne r_n er indbyrdes forskellige, og hvis de kan skrives $r_n = \frac{p_n}{q_n}$, $p_n \in \mathbb{Z}$, $q_n \in \mathbb{N}$, hvor

$$q_n^c (r_n - \xi) \text{ er begrænset.}$$

Det følger let, at vi så har $q_n \to \infty$, og at ξ er grænseværdi

for følgen (r_n). Det er klart, at en c-konvergent følge også er c'-konvergent for hvert $c' < c$. Der gælder nu følgende SÆTNING (Liouville, 1851). *Grænseværdien ξ for en c-konvergent følge (r_n) kan ikke være et algebraisk tal af grad $< c$.*

Bevis. Indirekte. Antag at ξ er rod i et polynomium $f \in \mathbb{Q}[X]$ af grad $N < c$. Vi kan antage, at f har koefficienter i $\mathbb{Z}$ (ellers kan dette opnås ved at multiplicere koefficienterne med en "fælles nævner"). Vi kan skrive

$$f(X) = (X - \xi)\, g(X),$$

hvor polynomiet g har reelle koefficienter, og vi kan skrive $r_n = \frac{p_n}{q_n}$, hvor følgen $q_n^c(r_n - \xi)$ er begrænset. Nu finder vi

$$\begin{aligned} q_n^N f(r_n) &= q_n^N (r_n - \xi)\, g(r_n) \\ &= \frac{1}{q_n^{c-N}}\, q_n^c (r_n - \xi)\, g(r_n) \end{aligned}$$

For $n \to \infty$ har vi her $\frac{1}{q_n^{c-N}} \to 0$ (da $c - N > 0$ og $q_n \to \infty$), $q_n^c(r_n - \xi)$ er begrænset, og $g(r_n) \to g(\xi)$. Følgelig har vi $q_n^N f(r_n) \to 0$. På den anden side er $q_n^N f(r_n) = q_n^N f\left(\frac{p_n}{q_n}\right)$ element i $\mathbb{Z}$, når f er et polynomium af grad N med koefficienter i $\mathbb{Z}$. Vi må derfor have $q_n^N f(r_n) = 0$, altså $f(r_n) = 0$, fra et vist trin, men dette er en modstrid, da r_n'erne er forskellige, og f kun har endelig mange rødder. ▨

Eksempel. $\xi = \sum_{i=1}^{\infty} 10^{-i!}$ er grænseværdi for følgen $r_n = \sum_{i=1}^{n} 10^{-i!}$. Det er let at vise, at (r_n) er c-konvergent for ethvert c. Grænseværdien ξ må derfor være transcendent!

Det er klart, at hvert $\xi \in \mathbb{R}$ er grænseværdi for en 1-konvergent følge (f.eks. følgen $\frac{[n\xi]+1}{n}$). Man kan vise – og det er ikke dybtliggende –, at hvert irrationalt tal er grænseværdi for en 2-konvergent følge.

Det er derimod en dybtliggende sætning (Roth, 1955), at enhver grænseværdi for en c-konvergent følge, hvor $c > 2$, er transcendent.

2.19. Lad der være givet et legeme L og et irreducibelt polynomium $p \in L[X]$. Hvis p har en rod α i en udvidelse $L \hookrightarrow K$, så er p bortset fra en konstant faktor det minimale polynomium for α over L. Polynomiet $f_{\alpha/L}$ er nemlig divisor i p, og da p er irreducibel og dermed kun har trivielle divisorer, følger påstanden. Specielt har vi altså $(p) = (f_{\alpha/L})$, og vi får en isomorfi

$$L[X]/(p) = L[X]/(f_{\alpha/L}) \xrightarrow{\sim} L[\alpha] = L(\alpha)$$

ved hvilken $\overline{X} \longmapsto \alpha$.

Udvidelsen $L \hookrightarrow L(\alpha)$ afhænger altså kun af det givne irreducible polynomium p, og vi slutter let:

SÆTNING. <u>Lad der være et legeme L. Hvis et irreducibelt polynomium $p \in L[X]$ har en rod α i en udvidelse $L \hookrightarrow K$ og en rod α' i en udvidelse $L \hookrightarrow K'$, så findes netop en L-isomorfi $: L(\alpha) \xrightarrow{\sim} L(\alpha')$, således at $\alpha \mapsto \alpha'$.</u>

Bevis.

$$\begin{array}{ccccc} & & L & & \\ & \swarrow & \downarrow & \searrow & \\ (K \supseteq) & L(\alpha) \xleftarrow{\sim} L[X]/(p) & \xrightarrow{\sim} & L(\alpha') & (\subseteq K') \\ & \alpha \longleftarrow \overline{X} & \longmapsto & \alpha' & \end{array}$$

□

2.20. Eksempel. Polynomiet $X^2+1 \in \mathbb{R}[X]$ er irreducibelt, og har i $\mathbb{C}$ rødderne i og $-i$. Vi har $\mathbb{R}(i) = \mathbb{C} = \mathbb{R}(-i)$, og $\mathbb{R}$-isomorfien $: \mathbb{C} \to \mathbb{C}$, som sender $i \mapsto -i$ er

komplekse konjugering.

2.21. SÆTNING. *Lad der være givet et irreducibelt polynomium $p \in L[X]$. Der findes da en udvidelse $L \hookrightarrow K$ således at p har en rod i K.*

Bevis. Da p er irreducibelt, er hovedidealet (p) et maksimalideal i $L[X]$, og kvotienten $K = L[X]/(p)$ er altså et legeme. Den sammensatte afbildning $a \mapsto \textcircled{a}$ af:

$$L \to L[X] \to L[X]/(p) = K$$

er altså en udvidelse, og i denne udvidelse har p roden $\textcircled{X}$. Er nemlig

$$p = a_0 + a_1 X + \cdots + a_n X^n,$$

finder vi i $L[X]/(p)$:

$$0 = \textcircled{p} = \textcircled{a_0 + a_1 X + \cdots + a_n X^n}$$
$$= \textcircled{a_0} + \textcircled{a_1}\textcircled{X} + \cdots + \textcircled{a_n}\textcircled{X}^n$$
$$= p(\textcircled{X}). \quad \blacksquare$$

2.22. Til et givet irreducibelt polynomium $p \in L[X]$ kan vi altså finde en udvidelse $L \hookrightarrow K$ og et element $\alpha \in K$ som er rod i p. I K kan vi betragte delegemet $L(\alpha)$. Dette legeme er isomorft med $L[X]/(p)$, og afhænger altså kun af det givne polynomium p. Vi siger at det fremkommer ved <u>til L at adjungere en rod i p</u>.

F. eks. kan legemet $\mathbb{C}$ af komplekse tal <u>defineres</u> som det legeme der fremkommer ved til $\mathbb{R}$ at adjungere en rod i $X^2 + 1$.

2.23. Har vi givet en udvidelse $L \hookrightarrow K$, får vi en injektiv homomorfi $L[X] \hookrightarrow K[X]$, og kan altså opfatte $L[X]$ som en delring af $K[X]$.

SÆTNING. *Til hvert polynomium*

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0 \in L[X],$$

af grad $n \geq 1$, findes en udvidelse $L \hookrightarrow K$ og elementer $\alpha_1, \ldots, \alpha_n \in K$, så at vi i $K[X]$ har

$$f = a_n (X - \alpha_1) \cdots (X - \alpha_n).$$

Bevis. Der findes et irreducibelt polynomium $p_1 \in L[X]$, som er divisor i f. Adjungeres til L en rod i dette irreducible polynomium, får vi en udvidelse $L \hookrightarrow L_1$ og et element $\alpha_1 \in L_1$, som er rod i p. Elementet α_1 er derfor også rod i f, så i $L_1[X]$ kan vi skrive

$$f = (X - \alpha_1) f_1 \quad , \quad f_1 \in L_1[X].$$

I $L_1[X]$ kan vi finde et irreducibelt polynomium, som er divisor i f_1, og adjungeres til L_1 en rod heri, får vi en udvidelse $L_1 \hookrightarrow L_2$ og et element $\alpha_2 \in L_2$ som er rod i f_2. I $L_2[X]$ har vi derfor $f_1 = (X - \alpha_2) f_2$, $f_2 \in L_2[X]$, altså

$$f = (X_1 - \alpha_1)(X_2 - \alpha_2) f_2 \,, \quad f_2 \in L_2[X].$$

I det vi fortsætter således får vi udvidelser

$$L \hookrightarrow L_1 \hookrightarrow L_2 \hookrightarrow \cdots \hookrightarrow L_n,$$ og elementer $\alpha_i \in L_i \subseteq L_n$, så at vi i $L_n[X]$ har

$$f = (X - \alpha_1) \cdots (X - \alpha_n) f_n \,, \quad f_n \in L_n[X];$$

her må imidlertid f_n have grad 0, og vi slutter, at $f_n = a_n$ ▨

3. Indskud om symmetriske polynomier

3.1. Elementerne i polynomiumsringen $R[X_1, \cdots, X_n]$ i n variable med koefficienter i en kommutativ ring R er endelige summer

$$p = \sum p_{i_1, \ldots, i_n} X_1^{i_1} \cdots X_n^{i_n}$$

Der summeres over alle multiindices $i = (i_1, \cdots, i_n) \in \mathbb{N}_0^n$. At summen er endelig betyder, at der kun for endelig mange $i = (i_1, \cdots, i_n)$ gælder, at koefficienten $p_{i_1, \ldots, i_n}$ er $\neq 0$ i R. Hvis $p_{i_1, \ldots, i_n} \neq 0$, siger vi, at $X_1^{i_1} \cdots X_n^{i_n}$ forekommer i polynomiet p, og $p_{i_1, \ldots, i_n} X_1^{i_1} \cdots X_n^{i_n}$ kaldes et led i p.

Idet vi for et multiindex $i = (i_1, \ldots, i_n)$ sætter

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

kan vi skrive

$$p = \sum p_i X^i$$

3.2. Ringen $R[X_1, \cdots, X_n]$ kan opfattes som en R-algebra, idet homomorfien $R \hookrightarrow R[X_1, \cdots, X_n]$ er givet ved

$$r \longmapsto \text{konstante polynomium } r$$

Er der givet en kommutativ R-algebra A, og et sæt $(\alpha_1, \ldots, \alpha_n)$ af elementer i A, kan vi indsætte $(\alpha_1, \ldots, \alpha_n)$ i et polynomium $p \in R[X_1, \cdots, X_n]$, idet vi sætter

$$p(\alpha_1, \ldots, \alpha_n) = \sum p_{i_1 \ldots i_n} \alpha_1^{i_1} \cdots \alpha_n^{i_n} \in A$$

Ved $p \longmapsto p(\alpha_1, \ldots, \alpha_n)$ definerus åbenbart en R-algebrahomomorfi

$$R[X_1, \ldots, X_n] \longrightarrow A;$$

Billedet ved denne afbildning er den mindste delalgebra af A, som indeholder $\alpha_1, \dots, \alpha_n$. Den betegnes $R[\alpha_1, \dots, \alpha_n]$. Hvis afbildningen $p \mapsto p(\alpha_1, \dots, \alpha_n)$ er injektiv, siger vi, at $(\alpha_1, \dots, \alpha_n)$ er <u>algebraisk uafhængige</u> over R. I dette tilfælde har vi altså en isomorfi

$$R[X_1, \dots, X_n] \xrightarrow{\sim} R[\alpha_1, \dots, \alpha_n] \quad (\subseteq A).$$

Indsættes $(X_1, \dots, X_n)$ i et polynomium p, får vi åbenbart $p(X_1, \dots, X_n) = p$.

3.3. For et <u>monomium</u> $X_1^{i_1} \dots X_n^{i_n}$ defineres <u>graden</u>, betegnet $\deg(X_1^{i_1} \dots X_n^{i_n})$ ved $i_1 + \dots + i_n \in \mathbb{N}_0$. Idet vi for et multiindex $i = (i_1, \dots, i_n)$ sætter

$$|i| = i_1 + \dots + i_n,$$

har vi altså

$$\deg(X^i) = |i|.$$

For et polynomium $p = \sum p_i X^i \neq 0$ i $R[X_1, \dots, X_n]$ defineres <u>graden</u>, betegnet $\deg(p)$, som den største grad af de monomier X^i, der forekommer i p, altså

$$\deg(p) = \max\{|i| \mid p_i \neq 0\}.$$

3.4 Multiindices kan <u>adderes</u> (komponentvis addition), idet vi for multiindices $i = (i_1, \dots, i_n)$, $j = (j_1, \dots, j_n)$ sætter

$$i + j = (i_1 + j_1, \dots, i_n + j_n)$$

For produktet af monomier X^i og X^j i $R[X_1, \dots, X_n]$ har vi

$$X^i X^j = X^{i+j}$$

Bemærk, at $|i+j| = |i| + |j|$.

Videre kan disse multiindices <u>ordnes</u>, idet

vi for multiindices $i = (i_1, \cdots, i_n)$ og $j = (j_1, \cdots, j_n)$ skriver

$$i < j,$$

hvis

$$|i| < |j|$$

eller $|i| = |j|$ og der findes $\nu \in \{1, \cdots, n\}$, så at $i_1 = j_1, \cdots, i_{\nu-1} = j_{\nu-1}$, $i_\nu < j_\nu$.

Det er let at se, at mængden af multiindices $\mathbb{N}_0^n$ herved bliver totalt ordnet, og at der til et givet multiindex $j = (j_1, \cdots, j_n)$ kun findes endelig mange multiindices $< j$. Dette sikrer let, at $(\mathbb{N}_0^n, <)$ er velordnet, således at (visse) sætninger om multiindices kan vises ved induktion. (Det er for øvrigt let at se, at $(\mathbb{N}_0^n, <)$ er isomorf med $(\mathbb{N}, <)$.). Det mindste multiindex er $(0, \cdots, 0)$; vi har

$$(0,\cdots,0) < (0,\cdots,0,1) < (0,\cdots,1,0) < \cdots < (1,0,\cdots,0) < (0,\cdots,0,2) < (0,\cdots,1,1) < \cdots$$

Bemærk, at vi for multiindices i, j, k har

$$i < j \Rightarrow i + k < j + k.$$

3.5. For et polynomium $p = \sum p_i X^i \neq 0$ i $R[X_1, \cdots, X_n]$ defineres <u>signaturen</u>, betegnet $\operatorname{sgt}(p)$, som det største multiindex i, for hvilket X^i forekommer i p, altså

$$\operatorname{sgt}(p) = \max \{ i \in \mathbb{N}_0^n \mid p_i \neq 0 \}.$$

Har p altså signaturen k, så kan vi skrive

$$p = p_k X + \sum_{i<k} p_i X^i, \quad p_k \neq 0.$$

Koefficienten p_k vil vi kalde <u>højestekoefficienten</u>.

Det er klart, at

$$|\operatorname{sgt}(p)| = \deg(p).$$

3.6. Har vi givet polynomier p, q med signaturer k, ℓ, så kan vi skrive

$$p = p_k X^k + \dots \quad , \quad p_k \neq 0$$

$$q = q_\ell X^\ell + \dots \quad , \quad q_\ell \neq 0$$

(hvor ... de to steder står for en sum af led af mindre signatur).
For produktet finder vi

$$pq = p_k q_\ell X^{k+\ell} + \dots .$$

Det følger, at vi i almindelighed har

$$sgt(pq) \leqslant sgt(p) + sgt(q),$$

og at vi endda har

$$sgt(pq) = sgt(p) + sgt(q), \text{ hvis } p_k q_\ell \neq 0.$$

Det sidste er f.eks. opfyldt, hvis R er et integritetsområde (eller hvis $p_k = 1$ eller $q_\ell = 1$).

Tilsvarende finder vi for summen

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

samt

$$sgt(p+q) = \max\{sgt(p), sgt(q)\}, \text{ hvis } sgt(p) \neq sgt(q).$$

Har p og q derimod samme signatur k, og samme højeste koefficient, så er $sgt(p-q) < k$.

[I ovenstående uligheder tilføjes nulpolynomiet 0 en signatur, der er $<$ ethvert multiindex].

Vi får tilsvarende uligheder (og ligheder) for graden af polynomier.

3.7. Eksempel. Ordner vi i polynomiet

$$p = 3 + 5X_1X_3^2 + X_2 + 8X_3^3 - X_1X_2X_3 \in \mathbb{Z}[X_1, X_2, X_3]$$

leddene efter (aftagende) signatur, får det udseendet

$$p = -X_1X_2X_3 + 5X_1X_3^2 + 8X_3^3 + X_2 + 3.$$

Signaturen er $(1,1,1)$, højestekoefficienten er -1 og graden er $1+1+1=3$.

3.8. For $\nu = 1, \cdots, n$ defineres polynomierne $s_\nu \in R[X_1, \cdots, X_n]$ ved

$$s_1 = \sum_{1 \le i \le n} X_i = X_1 + X_2 + \cdots + X_n$$

$$s_2 = \sum_{1 \le i_1 < i_2 \le n} X_{i_1} X_{i_2} = X_1 X_2 + X_1 X_3 + \cdots \cdots + X_{n-1} X_n$$

$$\vdots$$

$$s_\nu = \sum_{1 \le i_1 < i_2 < \cdots < i_\nu \le n} X_{i_1} X_{i_2} \cdots X_{i_\nu} = X_1 X_2 \cdots X_\nu + \cdots + X_{n-\nu+1} \cdots X_{n-1} X_n$$

$$\vdots$$

$$s_n = \sum_{1 \le i_1 < i_2 < \cdots < i_n \le n} X_{i_1} \cdots X_{i_n} = X_1 X_2 \cdots X_n$$

For et monomium $X_{i_1} \cdots X_{i_\nu}$, med $i_1 < \cdots < i_\nu$, har vi

$$\operatorname{sgt}(X_{i_1} \cdots X_{i_\nu}) = (0, \cdots, \underset{\uparrow}{1}, \cdots \underset{\uparrow}{0}, \underset{\uparrow}{1}, \cdots, 1, \cdots, 0)$$
$$i_1 \qquad i_2 \qquad i_\nu$$

så vi finder $\operatorname{sgt}(s_\nu) = (\underbrace{1, \cdots, 1}_{\nu \text{ et-taller}}, 0, \cdots, 0)$

For et potensprodukt $s_1^{l_1} \cdots s_n^{l_n}$ finder vi derfor

$$\operatorname{sgt}(s_1^{l_1} \cdots s_n^{l_n}) = (l_1 + \cdots + l_n, l_2 + \cdots + l_n, \cdots, l_{n-1} + l_n, l_n),$$

og højestekoefficienten er 1.

Polynomierne $s_1, \cdots, s_n$ kaldes de <u>elementarsymmetriske</u> polynomier (i n variable). Ofte betragtes også polynomierne

$$a_\nu = (-1)^\nu s_\nu = s_\nu(-X_1, \cdots, -X_n).$$

3.9. For polynomiet

$$\Delta = \prod_{i_1 < i_2} (X_{i_1} - X_{i_2})$$

finder vi signaturen

$$sgt(\Delta) = (n-1, n-2, \ldots, 1, 0)$$

og graden $\deg(\Delta) = \binom{n}{2}$.

3.10. Lad der være givet en permutation $\sigma \in \mathcal{S}_n$. For et givet polynomium $p \in R[X_1, \ldots, X_n]$,

$$p = \sum p_{i_1, \ldots, i_n} X_1^{i_1} \ldots X_n^{i_n}$$

definerer polynomiet $\sigma(p) \in R[X_1, \ldots, X_n]$ ved

$$\sigma(p) = \sum p_{i_1, \ldots, i_n} X_{\sigma(1)}^{i_1} \ldots X_{\sigma(n)}^{i_n}.$$

Vi finder let for polynomier p, q, at

$$(A) \begin{cases} \sigma(p+q) = \sigma(p) + \sigma(q) \\ \sigma(pq) = \sigma(p)\sigma(q), \end{cases}$$

samt for permutationer σ, τ, at

$$(B) \quad \sigma(\tau(p)) = (\sigma\tau)(p)$$

DEFINITION. Et polynomium $p \in R[X_1, \ldots, X_n]$ kaldes <u>symmetrisk</u>, hvis $\sigma(p) = p$ for alle permutationer $\sigma \in \mathcal{S}_n$.

3.11. Polynomiet $X_1^4X_2^2 + X_1^4X_3^2 + X_1^2X_2^4 + X_1^2X_3^4 + X_2^4X_3^2 + X_2^2X_3^4$ er symmetrisk ($n=3$). De elementarsymmetriske polynomier $s_1, \ldots, s_n$ (jfr. 3.8) er symmetriske polynomier.

For polynomiet $\Delta = \prod_{i_1 < i_2} (X_{i_1} - X_{i_2})$ finder vi

$$\sigma(\Delta) = (\operatorname{sign}\sigma)\,\Delta .$$

[vi finder faktisk $\sigma(\Delta) = (-1)^{I(\sigma)}\Delta$, hvor $I(\sigma)$ er antallet af inversioner i permutationen σ = antallet af par (i_1, i_2), hvor $i_1 < i_2$ og $\sigma(i_1) > \sigma(i_2)$. Definerer fortegnet $\operatorname{sign}\sigma$ ved $\operatorname{sign}\sigma = (-1)^{I(\sigma)}$, følger det let af ligningen 3.10 (B), at vi har $\operatorname{sign}(\sigma\tau) = (\operatorname{sign}\sigma)(\operatorname{sign}\tau)$].

Vi slutter, at kvadratet $D = \Delta^2$ er et symmetrisk polynomium. Polynomiet

$$D = \Delta^2 = \prod_{i_1 < i_2} (X_{i_1} - X_{i_2})^2 = (-1)^{\binom{n}{2}} \prod_{i_1 \neq i_2} (X_{i_1} - X_{i_2})$$

kaldes <u>diskriminanten</u>.

3.12 HOVEDSÆTNING OM SYMMETRISKE POLYNOMIER.

<u>Til hvert symmetrisk polynomium $p \in R[X_1, \dots, X_n]$ findes netop et polynomium $q \in R[X_1, \dots, X_n]$, således at vi ved indsættelse af de elementarsymmetriske polynomier $s_1, \dots, s_n$ i q får polynomiet p:</u>

$$\underline{p = q(s_1, \dots, s_n).}$$

Bevis. Vi bemærker først, at der for signaturen $\operatorname{sgt}(p) = k = (k_1, \dots, k_m)$ af et symmetrisk polynomium

$$p = \sum p_i X^i = p_k X^k + \cdots$$

gælder

$$k_1 \geqslant k_2 \geqslant \cdots \geqslant k_n .$$

Fandtes nemlig et $\nu < n$, således at $k_\nu < k_{\nu+1}$, så kunne vi sætte $l = (k_1, k_2, \dots, k_{\nu+1}, k_\nu, \dots, k_{n-1}, k_n)$ og betragte transpositionen $\tau = (\nu, \nu+1)$. Vi ser, at X^l ville forekomme i polynomiet $\tau(p)$, således at vi ville have $\operatorname{sgt}(\tau(p)) \geqslant l$. Da $l > k = \operatorname{sgt}(p)$ er dette i modstrid med at $\tau(p) = p$.

Vi viser nu for et symmetrisk polynomium p eksistensen af det søgte polynomium q ved fuldstændig induktion efter signaturen af p: Er $p = 0$ kan vi bruge $q = 0$. Har $p \neq 0$ signaturen $k = (k_1, \cdots, k_n)$, og antager vi, at eksistensen er vist for alle symmetriske polynomier af signatur $< k$, så kan vi skrive

$$p = p_k X^k + \cdots \quad , \quad p_k \neq 0.$$

I følge bemærkningen har vi $k_1 \geqslant k_2 \geqslant \cdots \geqslant k_n$, og vi kan derfor skrive

$$(k_1, k_2, \cdots, k_n) = (l_1 + \cdots + l_n, l_2 + \cdots + l_n, \cdots, l_n)$$

med tal $l_\nu \geqslant 0$. Udregningen i 3.8. viser nu, at polynomiet $p_k s_1^{l_1} \cdots s_n^{l_n}$ har signatur $k = (k_1, \cdots, k_n)$ og samme højeste koefficient som p (nemlig p_k), så differensen $p - p_k s_1^{l_1} \cdots s_n^{l_n}$ har signatur $< k$. Da denne differens øjensynlig er et symmetrisk polynomium, findes et polynomium $\tilde{q}$, så at

$$p - p_k s_1^{l_1} \cdots s_n^{l_n} = \tilde{q}(s_1, \cdots, s_n),$$

men så er

$$p = q(s_1, \cdots, s_n), \text{ med } q = p_k X_1^{l_1} \cdots X_n^{l_n} + \tilde{q}(X_1, \cdots, X_n).$$

For at vise entydigheden er det nok at vise, at vi for et polynomium $q \neq 0$ har

$$q(s_1, \cdots, s_n) \neq 0.$$

Et sådant polynomium er imidlertid sum af sine led

$$q_i X^i = q_i X_1^{i_1} \cdots X_n^{i_n} \qquad q_i \neq 0$$

som har indbyrdes forskellig signatur. Ved indsættelse af $s_1, \cdots, s_n$ ser vi, at $q(s_1, \cdots, s_n)$ er sum af de tilsvarende polynomier

$$q_i s_1^{i_1} \cdots s_n^{i_n},$$

og udregningen i 3.8. viser, at disse polynomier

også har indbyrdes forskellig signatur. Deres sum må derfor være $\neq 0$ ▨

3.13. Bemærk, at entydighedsudsagnet i hovedsætningen udsiger, at polynomierne $s_1, \cdots, s_n \in R[X_1, \cdots, X_n]$ er algebraisk uafhængige, og at eksistensudsagnet udsiger, at delringen

$$R[s_1, \cdots, s_n] \subseteq R[X_1, \cdots, X_n]$$

netop består af de symmetriske polynomier.

3.14. For $n = 2$ er polynomierne $X_1^2 + X_2^2$, $X_1^3 + X_2^3$, $D = \Delta^2 = (X_1 - X_2)^2 = X_1^2 + X_2^2 - 2X_1X_2$ symmetriske. Man finder let

$$\begin{aligned} X_1^2 + X_2^2 &= s_1^2 - 2s_2 \\ X_1^3 + X_2^3 &= s_1^3 - 3s_1s_2 \\ D &= s_1^2 - 4s_2. \end{aligned}$$

For $n = 3$ er polynomierne $X_1^4X_2^2 + X_1^4X_3^2 + X_1^2X_2^4 + X_1^2X_3^4 + X_2^4X_3^2 + X_2^2X_3^4$, $D = \Delta^2 = (X_1 - X_2)^2(X_1 - X_3)^2(X_2 - X_3)^2$ symmetriske. Det er noget omstændeligt at finde

$$X_1^4X_2^2 + X_1^4X_3^2 + X_1^2X_2^4 + X_1^2X_3^4 + X_2^4X_3^2 + X_2^2X_3^4 = -2s_1^3s_3 + s_1^2s_2^2 + 4s_1s_2s_3 - 2s_2^3 - 3s_3^2$$

og

$$D = -4s_1^3s_3 + s_1^2s_2^2 + 18s_1s_2s_3 - 4s_2^3 - 27s_3^2$$

Vi bemærker, at da $a_\nu = (-1)^\nu s_\nu$, $\nu = 1, \cdots, n$, kan vi på oplagt måde udtrykke et hvert symmetrisk polynomium $p \in R[X_1, \cdots, X_n]$ som et polynomium i $a_1, \cdots, a_n$.

3.15 Hovedsætningen anvendes ofte i følgende situation: Der er givet en kommutativ R-algebra A, og et normeret n-te grads polynomium (i én variabel)

$$(1)\quad f = X^n + \tilde{a}_1 X^{n-1} + \cdots + \tilde{a}_{n-1} X + \tilde{a}_n \in A[X],$$

som har en fremstilling

$$(2)\quad f = (X-\alpha_1)\cdots(X-\alpha_n),$$

hvor $\alpha_1, \ldots, \alpha_n \in A$. Udregnes produktet i (2) og sammenlignes med koefficienterne i (1), ser vi, at

$$\tilde{a}_\nu = (-1)^\nu \sum_{1 \le i_1 < \cdots < i_\nu \le n} \alpha_{i_1} \cdots \alpha_{i_\nu}.$$

Vi har altså

$$\tilde{a}_\nu = a_\nu(\alpha_1, \ldots, \alpha_n), \quad \nu = 1, \ldots, n,$$

hvor $a_\nu \in R[X_1, \ldots, X_n]$ er de elementarsymmetriske polynomier.

Er $p \in R[X_1, \ldots, X_n]$ et polynomium, så kan vi indsætte $\alpha_1, \ldots, \alpha_n$ i p, og får elementet $p(\alpha_1, \ldots, \alpha_n) \in A$. Hvis p er symmetrisk, ser vi, at $p(\alpha_1, \ldots, \alpha_n)$ ikke afhænger af rækkefølgen af faktorerne i (2).

Ifølge hovedsætningen kan det symmetriske polynomium p skrives

$$p = q(a_1, \ldots, a_n)$$

med et passende polynomium q. Ved indsættelse får vi derfor

$$p(\alpha_1, \ldots, \alpha_n) = q(a_1(\alpha_1, \ldots, \alpha_n), \ldots, a_n(\alpha_1, \ldots, \alpha_n))$$

altså

$$p(\alpha_1, \ldots, \alpha_n) = q(\tilde{a}_1, \ldots, \tilde{a}_n)$$

For et symmetrisk polynomium $p \in R[X_1, \ldots, X_n]$, kan $p(\alpha_1, \ldots, \alpha_n)$ altså udtrykkes som et polynomium i koefficienterne $\tilde{a}_1, \ldots, \tilde{a}_n$. Specielt ser vi, at

$$p(\alpha_1, \ldots, \alpha_n) \in R[\tilde{a}_1, \ldots, \tilde{a}_n]$$

3.16. Eksempel. Polynomiet $f = X^3 + 2X + 5 \in \mathbb{Z}[X]$ har i $\mathbb{C}$ tre rødder $\alpha_1, \alpha_2, \alpha_3$ og altså en fremstilling

$$f = (X-\alpha_1)(X-\alpha_2)(X-\alpha_3).$$

Uden at kende disse rødder finder vi (jfr. 3.14)

$$\alpha_1^4\alpha_2^2 + \alpha_1^4\alpha_3^2 + \alpha_1^2\alpha_2^4 + \alpha_1^2\alpha_3^4 + \alpha_2^4\alpha_3^2 + \alpha_2^2\alpha_3^4 = -2\cdot 2^3 - 3(-5)^2$$
$$= -91$$

$$(\alpha_1-\alpha_2)^2(\alpha_1-\alpha_3)^2(\alpha_2-\alpha_3)^2 = -4\cdot 2^3 - 27(-5)^2 = -707.$$

4. Algebraens fundamentalsætning.

4.1. ALGEBRAENS FUNDAMENTALSÆTNING. Ethvert polynomium

$$f = X^n + a_1 X^{n-1} + \cdots + a_{n-1} X + a_n \in \mathbb{C}[X],$$

af grad $n \geq 1$, har en rod i $\mathbb{C}$.

Beviset er i en række skridt:

① Sætningen er rigtig for $n = 2$. Skriver vi

$$f = X^2 + a_1 X + a_2 = \left(X + \tfrac{1}{2}a_1\right)^2 - \frac{a_1^2 - 4a_2}{4} = \left(X + \tfrac{1}{2}a_1\right)^2 - \frac{D}{4}$$

ser vi, at det er nok at vise, at hvert komplekst tal har en kvadratrod, altså at der til hvert tal $a \in \mathbb{C}$ findes et element $\alpha \in \mathbb{C}$, så at $a = \alpha^2$. Hertil bemærker vi, at hvert reelt tal ≥ 0 som bekendt har en reel kvadratrod, der er ≥ 0. Skriver vi

$$a = a' + i\,a'', \quad a', a'' \in \mathbb{R}$$

ser vi nu lit ved udregning, at af tallene

$$\sqrt{\frac{\sqrt{a'^2 + a''^2} + a'}{2}} \quad \pm i\sqrt{\frac{\sqrt{a'^2 + a''^2} - a'}{2}}$$

kan et bruges som α.

② Det er nok at vise, at hvert polynomium med reelle koefficienter af grad ≥ 1 har en rod i $\mathbb{C}$.

Er nemlig dette vist, og er

$$f = X^n + a_1 X^{n-1} + \cdots + a_n \in \mathbb{C}[X], \quad n \geq 1$$

et vilkårligt polynomium, så kan vi betragte det konjugerede polynomium

$$\bar{f} = X^n + \bar{a}_1 X^{n-1} + \cdots + \bar{a}_n.$$

Produktet $f\bar{f}$ har da reelle koefficienter og grad ≥ 2, og det har derfor en rod $\alpha \in \mathbb{C}$. Vi har nu $f(\alpha)\bar{f}(\alpha) = 0$, og altså $f(\alpha) = 0$ eller $\bar{f}(\alpha) = 0$. Hvis $f(\alpha) = 0$, så er α rod i f, og hvis $\bar{f}(\alpha) = 0$,

så er også $f(\bar{\alpha}) = \overline{f(\alpha)} = 0$, og altså $\bar{\alpha}$ rod i f.

③ Et tal $n \geq 1$ kan entydigt skrives

$$n = 2^k u, \quad k \geq 0, \quad u \text{ ulige}.$$

Vi viser nu udsagnet i ② for polynomier af grad $n = 2^k u$, $k \geq 0$, u ulige, ved <u>induktion efter k</u>.

For $k = 0$ er påstanden, at ethvert reelt polynomium af ulige grad har en rod i $\mathbb{C}$. Dette følger af et velkendt sammenhængsargument: Et sådant polynomium definerer en kontinuert funktion

$$f : \mathbb{R} \to \mathbb{R},$$

og billedmængden $f(\mathbb{R})$ er derfor et interval. Da graden er ulige, ser vi, at dette interval hverken kan være opad eller nedad begrænset, så vi må have $f(\mathbb{R}) = \mathbb{R}$. Specielt er altså

$$0 \in f(\mathbb{R}),$$

så f har endda en rod i $\mathbb{R}$.

④ Induktionsskridtet: Vi betragter et polynomium

$$f = X^n + a_1 X^{n-1} + \cdots + a_n$$

med reelle koefficienter $a_1, \ldots, a_n$ af grad $n = 2^k u$, $k > 0$, u ulige, og antager, at påstanden i ② er vist for alle polynomier af grad $2^{k-1} u'$, u' ulige.

Betragter vi f som et polynomium i $\mathbb{C}[X]$ følger det af sætning 2.23, at vi kan finde en udvidelse $\mathbb{C} \subset K$ og elementer $\alpha_1, \ldots, \alpha_n \in K$, så at vi i $K[X]$ har en fremstilling

$$f = (X - \alpha_1) \cdots (X - \alpha_n).$$

Vi har nu

$$\mathbb{R} \subseteq \mathbb{C} \subseteq K,$$

og vi ønsker at vise, at et af α_i'erne tilhører $\mathbb{C}$.

For et tal $t \in \mathbb{R}$ betragter vi nu polynomiet

$$g_t = \prod_{1 \le i < j \le n} \left(X - (\alpha_i + \alpha_j + t\alpha_i\alpha_j)\right)$$

Dette er et polynomium i $K[X]$, det har grad $\binom{n}{2}$ og i K rødderne $\alpha_i + \alpha_j + t\alpha_i\alpha_j$, $i < j$. Ved udregning af produktet, ser vi, at hver koefficient i g_t kan udtrykkes som et symmetrisk polynomium i $\alpha_1, \dots, \alpha_n$ med koefficienter (der afhænger af t) i $\mathbb{R}$. I følge hovedsætningen om symmetriske polynomier kan vi derfor slutte, at g_t's koefficienter tilhører $\mathbb{R}[a_1, \dots, a_n] = \mathbb{R}$. Da endvidere g_t's grad $\binom{n}{2} = \frac{n}{2}(n-1) = 2^{k-1}u(2^k u - 1)$ er af formen $2^{k-1}u'$, u' ulige, kan vi af induktionsforudsætningen slutte, at g_t har en rod i $\mathbb{C}$. Denne rod må være af formen $\alpha_i + \alpha_j + t\alpha_i\alpha_j$, så til det givne $t \in \mathbb{R}$ findes altså (i,j) med $1 \le i < j \le n$, således at

$$\alpha_i + \alpha_j + t\alpha_i\alpha_j \in \mathbb{C}.$$

For hvert $t \in \mathbb{R}$ findes altså et par (i,j), $1 \le i < j \le n$ således at $\alpha_i + \alpha_j + t\alpha_i\alpha_j \in \mathbb{C}$. Der er uendelig mange t'er, men kun endelig mange par (i,j). Det følger, at der må findes elementer $s \neq t$ i $\mathbb{R}$ og et par (i,j) så at

$$\alpha_i + \alpha_j + t\alpha_i\alpha_j \in \mathbb{C}$$
$$\alpha_i + \alpha_j + s\alpha_i\alpha_j \in \mathbb{C}.$$

Ved "subtraktion" slutter vi, at $(t-s)\alpha_i\alpha_j \in \mathbb{C}$, og dermed, at $\alpha_i\alpha_j = (t-s)^{-1}(t-s)\alpha_i\alpha_j \in \mathbb{C}$, og heraf følger videre, at også $\alpha_i + \alpha_j \in \mathbb{C}$. Polynomiet

$$(X - \alpha_i)(X - \alpha_j) = X^2 - (\alpha_i + \alpha_j)X + \alpha_i\alpha_j$$

har således koefficienter i $\mathbb{C}$, det har grad 2 og det har rødderne α_i og α_j i K. Af ① følger, at dette polynomium har en rod i $\mathbb{C}$. Vi har derfor $\alpha_i \in \mathbb{C}$ eller $\alpha_j \in \mathbb{C}$. ▨

4.2. Algebraens fundamentalsætning medfører, at de irreducible polynomier i $\mathbb{C}[X]$ er 1ste grads polynomierne. De normerede irreducible polynomier i $\mathbb{C}[X]$ er altså polynomierne af formen

$$X - a, \quad a \in \mathbb{C}.$$

Algebraens fundamentalsætning medfører videre, at de normerede irreducible polynomier i $\mathbb{R}[X]$ er polynomierne af formen

(1) $X - a$, $a \in \mathbb{R}$

(2) $(X-a)^2 + b^2$, $a, b \in \mathbb{R}$, $b \neq 0$.

Er nemlig p et sådant polynomium, så har p en rod $\alpha = a + ib$ i $\mathbb{C}$, og vi har $p = f_{\alpha/\mathbb{R}}$, jfr. 2.19. Det minimale polynomium for $\alpha = a+ib$ er øjensynlig $X-a$, hvis $b=0$, og $(X-a)^2+b^2$, hvis $b \neq 0$.

5. Endelige, reelle divisionsalgebraer.

5.1. DEFINITION. En algebra A over legemet L kaldes en <u>divisionsalgebra</u> (resp. <u>integritetsalgebra</u>), hvis ringen A er et skevlegeme (resp. integritetsområde).

5.2. SÆTNING. <u>Enhver endelig integritetsalgebra A er en divisionsalgebra.</u>

Bevis. For et givet $\alpha \neq 0$ i A betragtes afbildningen $r_\alpha : A \to A$ givet ved

$$r_\alpha : \xi \longmapsto \xi\alpha.$$

Denne afbildning er lineær, altså en endomorfi i det endeligdimensionale vektorrum A. Da nulreglen gælder i A, ser vi, at den er injektiv. Vi slutter, at den er bijektiv. Specielt findes et element $\alpha' \in A$, så at $\alpha'\alpha = 1$. Her er nødvendigvis $\alpha' \neq 0$, så tilsvarende findes $\alpha'' \in A$, så at $\alpha''\alpha' = 1$. Men så er $\alpha'' = \alpha''(\alpha'\alpha) = (\alpha''\alpha)\alpha = \alpha$, og vi har $\alpha'\alpha = 1$ og $\alpha\alpha' = 1$. Elementet α er altså invertibelt ▨

5.3. KOROLLAR. <u>Enhver delalgebra B af en endelig divisionsalgebra A er selv en endelig divisionsalgebra.</u>

Bevis. Delalgebraen B er specielt et underrum i A, og dermed endeligdimensional. Da nulreglen gælder i delmængden, følger påstanden af sætning 5.2 ▨

5.4. Vi kan opfatte legemet L som en 1-dimensio-

nal divisionsalgebra. For enhver endelig udvidelse $L \subset K$ er K en kommutativ endelig divisionsalgebra.
Over $\mathbb{R}$ er $\mathbb{R}$, $\mathbb{C}$ og $\mathbb{H}$ endelige divisionsalgebraer. Som vi om lidt skal se findes der ikke andre.

5.5. Er A en L-algebra $\neq 0$, så er homomorfien $L \to A$ injektiv. Vi vil sædvanligvis identificere elementerne i L med deres billeder i A, altså opfatte L som en delring $L \subseteq A$. Vi har endda

$$L \subseteq \mathrm{Cent}(A).$$

Hvis A er en endelig divisionsalgebra, så er hvert element $\alpha \in A$ algebraisk over L (Korollar 1.4), og delalgebraen $L[\alpha]$ er selv en endelig divisionsalgebra. Vi har således en endelig udvidelse $L \subset L[\alpha]$ af legemer, og det minimale polynomium $f_{\alpha/L} \in L[X]$ er et irreducibelt polynomium. Vi bemærker her, at det irreducible polynomium $f_{\alpha/L}$ har grad 1, hvis og kun hvis $\alpha \in L$.

SÆTNING. Hvis legemet L er algebraisk afsluttet, så findes netop én endelig divisionsalgebra over L, nemlig L selv.

Bevis. Lad A være en sådan algebra. For et element $\alpha \in A$ er det minimale polynomium $f_{\alpha/L} \in L[X]$ irreducibelt. Da L er algebraisk afsluttet, må $f_{\alpha/L}$ være et 1ste gradspolynomium (jfr. 2.16), så vi har $\alpha \in L$ ▨

5.6. Sætning 5.5. kan anvendes på legemet $\mathbb{C}$ ifølge algebraens fundamentalsætning. For $L = \mathbb{R}$ gælder nu

FROBENIUS' SÆTNING. Over legemet $\mathbb{R}$ findes på isomorfi nær kun tre endelige divisionsalgebraer, nemlig $\mathbb{R}$, $\mathbb{C}$ og $\mathbb{H}$.

Bevis. Lad A være en sådan algebra. Vi kan antage, at $\mathbb{R} \subset A$. For et element $\alpha \in A \setminus \mathbb{R}$ er (jfr. 4.2) det minimale polynomium $f_{\alpha/\mathbb{R}}$ af formen

$$(*) \quad (X-a)^2 + b^2, \quad a, b \in \mathbb{R}, \ b \neq 0,$$

og delalgebraen $\mathbb{R}[\alpha]$ er isomorf med $\mathbb{C}$.
Da $\mathbb{R} \subset A$ findes der sådanne elementer α, og der findes følgelig i A en delalgebra $B \simeq \mathbb{C}$. I B findes et element I, så at

$$\boxed{I^2 = -1}$$

og vi har $B = \mathbb{R}[I]$.

Vi betragter nu afbildningen $p: A \to A$ givet ved

$$p: \xi \longmapsto I\xi I^{-1}!$$

Vi ser lit, at

1) p er $\mathbb{R}$-lineær
2) p er involutorisk (d: $p^2 = Id_A$)
3) p er multiplikativ.

Af 1) og 2) følger som bekendt, at vi har en direkte sum opspaltning

$$A = A_1 \oplus A_{-1}$$

i egenrummene

$$A_1 = \{\xi \in A \mid I\xi I^{-1} = \xi\}$$

$$A_{-1} = \{\xi \in A \mid I\xi I^{-1} = -\xi\}.$$

Af 3) følger, at A_1 er en delring, og det er klart, at $B \subseteq A_1$. For $\xi \in A_1$ har vi $I\xi = \xi I$, så ξ kommuterer med I. Heraf følger lit, at ξ kommuterer med alle elementer af formen $a + bI$,

altså med alle elementer i B. Dette betyder, at $B \subseteq \mathrm{Cent}(A_1)$, så vi kan betragte A_1 som en algebra over B. Det er klart en endelig divisionsalgebra, og da $B \simeq \mathbb{C}$ er algebraisk afsluttet, må vi have $B = A_1$ (sætning 5.5).
Hvis $A_1 = (0)$, har vi altså $A = A_1 = B \simeq \mathbb{C}$.
Er derimod $A_{-1} \neq (0)$, kan vi betragte et element $J \neq 0$ i A_{-1}. At $J \in A_{-1}$ betyder, at $IJI^{-1} = -J$, altså at

$$\boxed{IJ = -JI}$$

Det er klart, at $J \notin \mathbb{R}$, så dit minimale polynomium for J er af formen (*). Der findes altså en ligning

$$J^2 + a^2 + b^2 = 2aJ, \quad a, b \in \mathbb{R}, \quad b \neq 0.$$

Da $J \in A_{-1}$, slutter vi let af 3), at $J^2 \in A_1$. Da også $a^2 + b^2 \in \mathbb{R} \subseteq A_1$ har vi $J^2 + a^2 + b^2 \in A_1$. Nu er $2aJ \in A_{-1}$, og da $A_1 \cap A_{-1} = (0)$, må begge sider i ligningen være 0. Vi får først $a = 0$, og dernæst $J^2 = -b^2$. I stedet for at erstatte J med $b^{-1}J$, kan vi antage, at

$$\boxed{J^2 = -1}$$

Af 3) følger nu let, at der ved $\alpha \mapsto \alpha J$ defineres en afbildning $: A_1 \to A_{-1}$. Den er øjensynlig $\mathbb{R}$-lineær, og den er en isomorfi, idet afbildningen $\beta \mapsto \beta J^{-1} = -\beta J$ ses at være dens inverse. Vi slutter, at basen $1, I$ for A_1 afbildes på en basis for A_{-1}, altså at J, IJ er en basis for A_{-1}. Sættes altså

$$\boxed{IJ = K,}$$

ser vi, at $1, I, J, K$ er en $\mathbb{R}$-basis for A.

De øvrige ligninger for multiplikation med kvaternionenheden følger let af de indrammede. ▨