H10 Eindige en Algebraïsche uitbreidingen.

Def Zij $L \supset K$ lichaamsuitbreiding. We zeggen dat L eindige uitbreiding over K is als $\dim_K(L) < \infty$

— de graad van L over K, notatie $[L:K]$ is deze dimensie.

Def We noemen L algebraïsch over K als elke $\alpha \in L$ algebraïsch over K is.

St. 10.3 Zij $L \subset K$ uitbreiding en $\alpha \in L$. TFAE:

(i) α is algebraïsch over K
(ii) $[K(\alpha):K]$ is eindig.

Bew (i) $\Rightarrow$ (ii): We passen 9.8(d) toe op het unieke minimumpolyn. $f_K^\alpha \in K[X]$
en concluderen $\dim_K(L) = gr(f_K^\alpha) < \infty$ want een polynoom heeft eindige graad.

(ii) $\Rightarrow$ nu nemen we $[K(\alpha):K] = n \in \mathbb{N}_1$.
Dan volgt, omdat in een n-dim v.r elke $(n+1)$-tal vectoren lineair afh. is, dat $\{1, .. \alpha^n\} \subset L$ een lin afh. verzameling zijn. Er zijn dus $a_0 .. a_n \in K$ met $a_0 + a_1\alpha + .. + a_n\alpha^n = 0$. Dan volgt voor $f = a_0 + a_1X + .. + a_nX^n \in K[X]$ dat $f(\alpha) = 0$ dus α is algebraïsch over K.

St. 10.4 Als L een eindige lichaamsuitbreiding over K is, dan is L algebraïsch over K (dus elke $\alpha \in L$ is algebraïsch over K).

Bew Zij $\alpha \in L$. Omdat $K \subset K(\alpha) \subset L$ is $K(\alpha)$ een over K deelvectorruimte van L en dus $\dim_K(K(\alpha)) \leq \dim_K(L) < \infty$
dus ook $K(\alpha)$ is eindig over K. Wegens 10.3 volgt dat α algebraïsch is over K. □

— Omdat, wanneer $\alpha \in L \supset K$ algebraïsch over K is, $[K(\alpha):K] < \infty$ wegens 10.3, en wegens 10.4 volgt dan dat $K(\alpha)$ algebraïsch over K is, volgt uit 10.3 en 10.4 samen dat als $\alpha \in L$ algebraïsch is over K, dan is $K(\alpha)$ algebraïsch over K. $\square$

— De omkering van 10.4 geldt niet: er is een algebraïsche uitbreiding die niet eindig is. Zie opgave 10.1:

opg. Beschouw $\bigcup_{n=1}^{\infty} \mathbb{Q}(\sqrt[n]{2}) = L \supset \mathbb{Q} = K$

(i) L is een lichaam, want voor $n, m \geq 1$ is $\mathbb{Q}(\sqrt[n]{2}) \cup \mathbb{Q}(\sqrt[m]{2})$ als volgt:

$(\sqrt[n]{2})^n - 2 = 0$, $(\sqrt[m]{2})^m - 2 = 0$ dus $\sqrt[n]{2}$, $\sqrt[m]{2}$ zijn algebraïsch over $\mathbb{Q}$. Bovendien is $X^k - 2 \in \mathbb{Q}[X]$ voor $k \geq 1$ irreducibel (en monisch, duh), want $X^k - 2 \in \mathbb{Z}[X]$ met $\mathbb{Z}$ ufd en $\mathbb{Q} = Q(\mathbb{Z})$ en $2 \in \mathbb{Z}$ is irreducibel en $X^k - 2$ is een eisenstein polynoom bij 2. Het is dus irred. in $\mathbb{Q}[X]$ (wegens primitiviteit ook in $\mathbb{Z}[X]$) dus $X^k - 2 = f^{\sqrt[k]{2}}_{\mathbb{Q}}$ en er volgt

$[\mathbb{Q}(\sqrt[k]{2}) : \mathbb{Q}] = k$ voor $k \geq 1$ en

$\{1, \alpha, \ldots \alpha^{k-1}\}$ is basis $(\alpha = \sqrt[k]{2})$.

Dus elke $\alpha \in \mathbb{Q}(\sqrt[n]{2}) \cup \mathbb{Q}(\sqrt[m]{2})$ is van de vorm

$$\alpha = a_0 + a_1\sqrt[n]{2} + a_2\sqrt[n]{2^2} + \ldots + a_{n-1}\sqrt[n]{2^{n-1}}$$
$$= a_0 + a_1 \sqrt[nm]{2^m} + \ldots + a_{n-1}\sqrt[nm]{2^{m(n-1)}}$$
$$= a_0 + a_1(\sqrt[nm]{2})^m + \ldots + a_{n-1}(\sqrt[nm]{2})^{m(n-1)} \in \mathbb{Q}(\sqrt[mn]{2})$$

hetzelfde als $\alpha = a_0 + a_1\sqrt[m]{2} + \ldots + a_{m-1}\sqrt[m]{2^{m-1}} \in \mathbb{Q}(\sqrt[m]{2})$ is.

Maar $\sqrt[mn]{2}$, $mn \geq 1$ is algebraïsch over $\mathbb{Q}$ met wegens het voorgaande $f^{\sqrt[mn]{2}}_{\mathbb{Q}} = X^{mn} - 2$, dus $\alpha \in \mathbb{Q}(\sqrt[n]{2}) \cup \mathbb{Q}(\sqrt[m]{2})$ heeft een inverse $\alpha^{-1} \in \mathbb{Q}(\sqrt[nm]{2}) \subset \bigcup_{n' \geq 1} \mathbb{Q}(\sqrt[n']{2})$

dus volgt voor $\alpha, \beta \in \bigcup_{n \geq 1} \mathbb{Q}(\sqrt[n]{2})$ dat

$\alpha \in \mathbb{Q}(\sqrt[n]{2})$, $\beta \in \mathbb{Q}(\sqrt[m]{2})$, dat

$\alpha, \beta \in \mathbb{Q}(\sqrt[mn]{2})$ en dit is een lichaam dus $\alpha-\beta,\ \overset{\text{als } \beta\neq 0}{\alpha\beta^{-1}} \in \mathbb{Q}(\sqrt[mn]{2}) \subset \bigcup_{n\geq 1} \mathbb{Q}(\sqrt[n]{2})$ en $1, 0 \in \mathbb{Q} \subset \bigcup_{n\geq 1} \mathbb{Q}(\sqrt[n]{2})$

dus we zien dat $\bigcup_{n\geq 1} \mathbb{Q}(\sqrt[n]{2})$ een deellichaam van $\mathbb{R}$ is

en daarmee zelf een lichaam (immers elke $\sqrt[n]{2} \in \mathbb{R}$, $n \in \mathbb{N}_1$)

(ii) L is algebraïsch over $\mathbb{Q}$, want als $\alpha \in L$

dan $\alpha \in \mathbb{Q}(\sqrt[n]{2})$ voor een $n \in \mathbb{N}_1$ en $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$

dus (want $X^n - 2 = f^{\sqrt[n]{2}}_{\mathbb{Q}}$) volgens 10.4

volgt dat $\mathbb{Q}(\sqrt[n]{2})$ algebraïsch (want eindig) over $\mathbb{Q}$ is.

(iii) maar $[L : K]$ is niet-eindig over $\mathbb{Q}$, want voor elke $n \in \mathbb{Z}_{\geq 1} = \mathbb{N}_1$

bevat $L \supset \mathbb{Q}(\sqrt[n]{2})$ en dit is een deellichaam $\supset \mathbb{Q}$

van graad n over $\mathbb{Q}$, dus we kunnen

geen bovengrens vinden voor deze graad, terwijl als

L een eindige graad over K zou hebben, dan zou

elke $L' \subset L$ met $K \subset L' \subset L$

een lineaire deelruimte zijn waarvan de dimensie

door $[L : K]$ begrensd moet zijn. We concluderen

dat L algebraïsch is maar niet eindig over K □

— We kunnen wel nog andere dingen bewijzen

St. 10.6 K lichaam, L uitbreiding K en M uitbreiding L ($K \subset L \subset M$) Dan geldt:

M eindig over K $\Longleftrightarrow$ M eindig over L, L eindig over K

en als M eindig over K is volgt ook

$$[M : K] = [M : L] \cdot [L : K]$$

Bew "$\Rightarrow$": Stel M is eindig over K. Dan is

direct duidelijk dat vanwege L v.r. over K

met $M \subset L \subset K$ volgt dat L een

lineaire deelruimte van M is en dus zeker e.d.

want $\dim_K(L) \leq \dim_K(M)$. Wanneer we $\alpha_1, \ldots \alpha_n \in M$ nemen

en $M = \operatorname{span}\{\alpha_1, \ldots \alpha_n\}$ dan volgt

voor elke $x \in M$ dat $x \in M$ dus $x = \sum_{i=1}^{n} a_i \alpha_i$, $a_i \in K$
dus $a_i \in K \subset L$ dus M over L wordt zeker opgespannen door $\alpha_1, \ldots \alpha_n$ en is dus ook een e.d.v.r. met $\dim_L(M) \leq \dim_K(M)$. Dus hebben we M eindig over L en K eindig over K

$\Leftarrow$ Omdat $[M:L]$ en $[L:K]$ eindig zijn,
nemen we deze op $m, n \in \mathbb{N}_1$ en we nemen L-bases $\alpha_1, \ldots \alpha_m$ voor M over L en K-basis $\beta_1, \ldots \beta_n$ voor L over K. Dan volgt dat elke $y \in M$ op $\alpha_1, \ldots \alpha_m$ geschreven kan worden als

$y = a_1\alpha_1 + \ldots + a_m \alpha_m$, $a_i \in L$. En elke $a_i \in L$ kan op K geschreven worden als $a_i = \sum_{j=1}^{n} c_{ij}\beta_j$

Dus $y = \sum_{i=1}^{m}\sum_{j=1}^{n} c_{ij}(\alpha_i\beta_j)$ waarmee $\{\alpha_i\beta_j\}_{\substack{i=1,\ldots m\\ j=1,\ldots n}}$

dus M opspant over K, dus $\dim_K(M) \leq mn$.
We laten zien dat $\{\alpha_i\beta_j\}$ ook een Kbasis voor M is;
dit doen we door lineaire onafh aan te tonen:

neem $c_{ij} \in K$ voor $i = 1, \ldots m$; $j = 1, \ldots n$ zodat
$\sum_{i=1}^{m}\sum_{j=1}^{n} c_{ij}\alpha_i\beta_j = 0$. Dan volgt

$\sum_{i=1}^{m}\left(\sum_{j=1}^{n} c_{ij}\beta_j\right)\alpha_i = 0$ en $\alpha_1, \ldots \alpha_m$ is een L-basis van M over L en
$\forall i \ \sum_{j=1}^{n} c_{ij}\beta_j \in L$, dus volgt wegens L-lineaire onafh. van $\alpha_1, \ldots \alpha_m$ dat $\forall i \ \sum_{j=1}^{n} c_{ij}\beta_j = 0$

maar β_1, β_n is een K-basis van L, dus zijn ze L-lineair onafhankelijk en volgt $\forall i (\forall j \ c_{ij} = 0)$
$\Rightarrow$ we concluderen dat $\{\alpha_i\beta_j\}_{\substack{i=1,\ldots m\\ j=1,\ldots n}}$ lin. onafh. is en opspannend, dus een basis.
Omdat ze lin. onafh zijn, zijn ze ook verschillend dus
$\#\{\alpha_i\beta_j\}_{\substack{i=1..m\\ j=1..n}} = m \cdot n \Rightarrow \dim_K(M) = m \cdot n$
en dus $[M:K] = [M:L][L:K]$ $\square$

Def $L \supset K$ uitbreiding en $\alpha_1, .. \alpha_n \in L$ dan definieert men inductief $K(\alpha_1, .. \alpha_n) = K(\alpha_1, .., \alpha_{n-1})(\alpha_n)$

Gevolg 10.7 voor $L \supset K$ en $\alpha_1, .. \alpha_n \in L$, alle α_i algebraïsch over K, is $K(\alpha_1, .. \alpha_n)$ eindig over K.

Bew met inductie naar n: IB $n=1$: dit is omdat $K(\alpha_1)$ eindig over K is want α_1 is algebraïsch over K (directe toepassing van 10.3, α alg. over $K \Leftrightarrow K(\alpha)$ eindig over K)

IH stel dat voor een $n \geq 1$ geldt $\alpha_1, .. \alpha_n \in L$ algbr. over K, dan $K(\alpha_1, .. \alpha_n)$ eindig over K,

IS dan nemen we $\alpha_1, .. \alpha_{n+1} \in L$ alg.br. over K
dus is $K(\alpha_1, .. \alpha_n)$ wegens IH eindig over K.
Dan is $L \supset K(\alpha_1, .. \alpha_n)$ een lichaamsuitbr. en $\alpha_{n+1} \in L$ en $f(\alpha_{n+1}) = 0$ voor een $f \in K[X] \subset K(\alpha_1, .. \alpha_n)[X]$
dus α_{n+1} is algebraïsch over $K(\alpha_1, .. \alpha_n)$, dus passen we 10.3 toe om te vinden dat $K(\alpha_1, .. \alpha_n)(\alpha_{n+1})$ eindig is over $K(\alpha_1, .. \alpha_n)$. Nu hebben we 10.6 nodig:

$M = K(\alpha_1, .. \alpha_{n+1})$ is eindig over $L = K(\alpha_1, .. \alpha_n)$ en $K(\alpha_1, .. \alpha_n)$ is eindig over K, dus volgt M is eindig over K $\square$

St. 10.8 Zij L een K-uitbreiding.

(a) Als $\alpha, \beta \in K$ algebraïsch over K zijn, dan ook $\alpha+\beta$, $\alpha-\beta$, $\alpha\beta$, α/β als $\beta \neq 0$

(b) de verz. $\{\alpha \in L : \alpha \text{ is algebraïsch over } K\}$ is een deellichaam van L dat K omvat.

Bew (a) wegens 10.7 is $K(\alpha,\beta)$ eindig over K, dus wegens 10.4 is $K(\alpha,\beta)$ algebraïsch over K, en omdat $\alpha \pm \beta$, $\alpha\beta$, $\alpha\beta^{-1}$ als $\beta \neq 0$ allemaal in $K(\alpha,\beta)$ liggen zijn dit algebraïsche elementen over K.

(b) 1,0 is algebraïsch over K want $0,1 \in K$. Dus volgt $0,1 \in \{\alpha \in L : \alpha \text{ algebraïsch over } K\} =: A$.
Bovendien, als $\alpha, \beta \in A$ dan wegens (a) $\alpha - \beta \in A$ en als $\beta \neq 0$, wegens (a) ook $\alpha/\beta \in A$. Dus A en $A \subset L$ dus A is een deellichaam van L □

Def Men noemt de verzameling A (een deellichaam dus) de **algebraïsche afsluiting** van K in L.

— Als laatste stelling: we vervangen "eindig" in 10.6 door "algebraïsch".

St. 10.9 Zij K een lichaam en L uitbreiding van K en M uitbreiding van L. Dan:

M algebraïsch over K $\Longleftrightarrow$ M algebraïsch over L
L algebraïsch over K.

Bew "$\Rightarrow$": dit volgt gelijk uit de definities: als $\alpha \in M$ dan is er een $f \in K[X] \subset L[X]$ met $f(\alpha) = 0$ dus M is ook algebraïsch over L. En als $\alpha \in L$ dan $\alpha \in L \subset M$ dus er is een $f \in K[X]$ met $f(\alpha) = 0$ dus α is alg. over K en dus is $L \subset M$ algebraïsch over K.

"$\Leftarrow$": Stel M alg. over L en L over K.
neem $\alpha \in M$, dan is er een $f = a_0 + a_1 X + \dots + a_n X^n \in L[X]$ met $f(\alpha) = 0$

omdat $a_0 + a_1\alpha + \dots + a_n\alpha^n = 0$ is kennelijk α ook algebraïsch over het deellichaam $K' = K(a_0, \dots a_n)$ maar omdat $a_0, \dots a_n \in L$ algebraïsch over K zijn per aanname is wegens 10.7 K' eindig over K.

We hebben nu $K \subset K' \subset K'(\alpha)$ en α is algebraïsch over K' dus $K'(\alpha)$ is eindig over K' wegens 10.3. En K' is wegens 10.7 dus eindig over K dus $K'(\alpha)$ is eindig over K' is eindig over K waardoor wegens 10.6 volgt dat $K'(\alpha)$ eindig is over K. Maar dan is wegens 10.4 $K'(\alpha)$ algebraïsch over K. Dus ihb is $\alpha \in K'(\alpha)$ algebraïsch over K. Dat voor alle $\alpha \in M$, dus M is algebraïsch over K.

$\square$

10.10 $L \subset K$ uitbr. eindig-dim. en $\beta \in L$, hoe dan f^{β}_{K} te bepalen? (wegens 10.4 is β algebraïsch dus bestaat het).

(a) Lineaire algebra: kies een K-basis voor L en schrijf $\beta^0, \beta^1, \dots \beta^n$ op basis (net zolang tot lineaire afhankelijkheid optreedt) over K

dan plaatsen we die β's in een lineaire afh. over K, en omdat er geen "kleinere" lin. afh. bestaat (dwz met lagere machten van β) vinden we f^{β}_{K} door deze afhankelijkheid monisch te maken.

(b) gedachten uit de Galois theorie: aangezien $f^{\sqrt{2}}_{\mathbb{Q}} = X^2 - 2$ en $f^{\sqrt{3}}_{\mathbb{Q}} = X^2 - 3$, nulpunten $\pm\sqrt{2}$ en $\pm\sqrt{3}$ hebben, ligt het mogelijk voor de hand dat $f^{1+\sqrt{2}+\sqrt{3}}_{\mathbb{Q}}$ nulpunten $1 \pm \sqrt{2} \pm \sqrt{3}$ heeft. Dus verm. lineaire factoren:

$(X - 1 + \sqrt{2} + \sqrt{3})(X - 1 - \sqrt{2} + \sqrt{3})(X - 1 - \sqrt{2} - \sqrt{3})(X - 1 + \sqrt{2} - \sqrt{3})$

en hopen dat dit een polynoom in $\mathbb{Q}[X]$ oplevert dat irreducibel is.

met de hoofdstelling over symmetrische polynomen zien we in dat deze methode wel altijd een rationaal polynoom oplevert. (ik zie dit even niet)

(c) "handig rekenen" : we zoeken naar $f_{\mathbb{Q}}^{\sqrt{2}+5}$
dan zien we $((\sqrt{2}+5)-5)^2 - 4 = 0$
dus $(X-5)^2 - 4 = X^2 - 10X + 21$ is een kanshebber. Maar is ook noodzakelijk $f_{\mathbb{Q}}^{\sqrt{2}+5}$ want als het graad 1 zou hebben dan zou $\sqrt{2}+5 \in \mathbb{Q}$, contradictie

(alternatief : $X^2 - 10X + 21$ is irreducibel over $\mathbb{Q}$ want niet-triviale factoren leveren $\mathbb{Q}$-nulpunten (tweedegraads) en deze moeten in $\mathbb{Z}$ liggen & 21 delen maar $(\pm 3)^2 - 10 \cdot \pm 3 + 21 \neq 0$
$(\pm 7)^2 - 10 \cdot \pm 7 + 21 \neq 0$).