H9 Enkelvoudige uitbreidingen

9.1 een uitbreiding van een lich. K is een lich L met $K \subset L$. voor $L \supset K$ uitbr en $\alpha \in L$

Def heet $K[\alpha]$ de uitbreidingsring van K met α en dit is $K[\alpha] := \{ a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_n\alpha^n \; ; \; n \in \mathbb{Z}_{>0}, \; a_0, \dots a_n \in K \}$

— dit is een ring

— als $K \subset R \subset L$ een ring is met $\alpha \in R$, dan $K[\alpha] \subset R$ dus $K[\alpha]$ is de kleinste deelring van L waarin α zit.

Bew het is een deelverzameling van een lichaam L. als we dus laten zien $0 \in K[\alpha]$ (wat zo is voor $n=0$ en $a_0 = 0 \in K$) en als $x, y \in K[\alpha]$, dus $x = a_0 + a_1\alpha + \dots + a_m\alpha^m$ voor een $m \in \mathbb{Z}_{>0}$ en $y = b_0 + b_1\alpha^1 + \dots + b_n\alpha^n$ voor een $n \in \mathbb{Z}_n$ en $a_0, a_1, \dots a_m, b_0, \dots b_n \in K$ dan volgt voor $M = \max\{m, n\}$ dat $x = a_0 + a_1\alpha + \dots + a_m\alpha^m + 0\alpha^{m+1} + \dots + 0\alpha^M$ en $y = b_0 + b_1\alpha + \dots + b_n\alpha^n + 0\alpha^{n+1} + \dots + 0\alpha^M$ dus
$x - y = (-b_0 + a_0) + (-b_1 + a_1)\alpha + \dots + (-b_M + a_M)\alpha^M$ en
$a_0 - b_0, a_1 - b_1 \dots a_M - b_M \in K$ dus $x - y \in K$. evenzo
met inductie naar m volgt $xy = (x' + a_m\alpha^m)(b_0 + \dots + b_n\alpha^n)$
$= x'y + \underbrace{a_m b_0 \alpha^m + a_m b_1 \alpha^{m+1} + \dots + a_m b_n \alpha^{m+n}}$
~~dus voor~~ $x'y \in K[\alpha]$ met IH en dit ligt ook in $K[\alpha]$
dus volgt $xy \in K[\alpha]$ en voor $m = 0$ is $xy = a_0 b_0 + \dots + a_0 b_m \alpha^m \in K[\alpha]$

$\square$

$K[\alpha]$ is zelfs een domein, want $\subset L$, L heeft geen nuldelers en $0 \neq 1$

— Dan definiëren we verder $K(\alpha)$, de enkelvoudige uitbreiding van K door adjungatie van α, als $Q(K[\alpha])$

Dit is welgedefinieerd want $K[\alpha]$ is een domein, en dit is een deellichaam F van L dat α bevat en $K \subset F \subset L$

— bovendien, als $K \subset F \subset L$ en $\alpha \in F$, dan $K(\alpha) \subset F$. want dan liggen eindige K-lin. combi's van (machten van) α in F en hun inversen $\frac{1}{a_0 + a_1\alpha + \dots + a_n\alpha^n}$ ook.

dus $Q(K(\alpha)) \subset F$.

— als $L \supset K$ uitbreiding is, dan kunnen we L als v.r. over K opvatten door als scalairverm. juist als $K \times L \to L : (k, \ell) \mapsto k\ell$ vermenigvuldiging in het lichaam te nemen.

— In veel gevallen blijken inversen van $x \in K[\alpha]$ gewoon in $K[\alpha]$ te liggen, zodat $K[\alpha]$ een deel-lichaam is dat K en α bevat, dus $K(\alpha) \subset K[\alpha] \subset K(\alpha)$ want $K(\alpha)$ is het kleinste lichaam met die eigenschap $\Longrightarrow K[\alpha] = K(\alpha)$
per constructie

We zullen zien dat dit geldt precies als $\alpha \in L$ algebraïsch is over K

Def $\alpha \in L \supset K$ heet algebraïsch over K als er een polynoom $0 \neq f \in K[X]$ is met $ev_\alpha(f) = 0$, waarbij we dus homom. $K[X] \hookrightarrow L[X] \twoheadrightarrow L$ bekijken.

Def $\alpha \in L \supset K$ heet transcendent over K als het niet algebraïsch is.

St 9.6 Als L uitbreiding van K is en $\alpha \in L$ transcendent over K, dan is $K[\alpha]$ isomorf met $K[X]$ en $K(\alpha)$ is isomorf met $K(X)$

Bew definieer het homomorfisme $\varphi : K[X] \hookrightarrow L[X] \xrightarrow{ev_\alpha} L$ ..
Dan zien we dat we $\varphi(K[X]) = K[\alpha]$ kunnen nemen: want als $\ell = a_0 + a_1\alpha + \cdots + a_n\alpha^n \in K[\alpha]$, voor een $n \in \mathbb{Z}_{\geq 0}$ en $a_0, \ldots a_n \in K$, dan is er ook het polynoom $f = a_0 + a_1X + \cdots + a_nX^n$ in $K[X]$ en zo krijgen we $\varphi(f) = \ell$, dus $K[\alpha] \subset \varphi(K[X])$ en de omkering is vrij triviaal: voor elke $b_0 + b_1X + \cdots + b_mX^m$ is $\varphi(b_0 + \cdots + b_mX^m) = b_0 + \cdots + b_m\alpha^m \in K[\alpha]$.

Dat dit een homom is: komt doordat het de samenstelling van de inclusie-afbeelding en evaluatiehomomorfisme is

tenslotte resteert aan te tonen dat φ injectief is.
Als dit niet zo is, is er een $0 \neq f \in \mathrm{Ker}(\varphi)$.
maar dan $ev_\alpha(f) = 0$ dus α is het nulpunt
van een $0 \neq f \in K[X]$, maar dan is α algebraïsch
niet transcendent! tegenspraak $\square$

nu breiden we φ uit tot $\varphi^\#: Q(K[X]) \to Q(K[\alpha])$
met $\varphi^\#: \frac{f}{g} \mapsto \frac{\varphi(f)}{\varphi(g)}$ We hebben in het voorgaande al eens gesproken over
de welgedefinieerdheid van zo'n uitbreiding mits een
homom. injectief is en de ringen domeinen zijn. Daaraan
is hier voldaan.

$\varphi^\#$ is als lichaamshomom. injectief. Ook surjectief, want
elke $\dfrac{a_0 + a_1\alpha + \cdots + a_n\alpha^n}{b_0 + b_1\alpha + \cdots + b_m\alpha^m} \in K(\alpha)$ is het beeld onder φ
van $(a_0 + a_1 X + \cdots + a_n X^n)/(b_0 + b_1 X + \cdots + b_m X^m) \in K(X)$
dus is er tevens het isomorfisme $\varphi^\#$

$\square$

— We zien dat transcendente $\alpha \in L$ eigenlijk
een soort "variabele" X zijn die een polynoomring
voortbrengen. Ze zijn transcendent in de zin dat ze
zich volledig als variabele kunnen gedragen zonder
aan een voorwaarde te voldoen.

— Voor algebraïsche $\alpha \in L$ voeren we wat extra begrippen in.

Def Er zijn voor een $\alpha \in L$ algebraïsch over K,
elementen $a_0, \ldots, a_n \in K$ te vinden zodat
$0 \neq f = a_0 + a_1 X + \cdots + a_n X^n \in K[X]$ en $f(\alpha) = 0$
En we kunnen nu n zo klein mogelijk kiezen
voor deze eigenschap en bovendien omdat dan
$a_n \neq 0$ (anders is er ook $n-1 < n$) geldt dat we alle
a_i met a_n^{-1} kunnen vermenigvuldigen zodat f monisch wordt.

We beweren nu dat deze monische f met kleinste graad zodat $f(\alpha) = 0$, uniek is.
Immers zij $0 \neq g = b_0 + b_1 X + \cdots + b_m X^m$ en $g(\alpha) = 0$, $a_m = 1$
Dan $m = n$ anders is g niet laag genoeg (n.l. niet minimaal) van graad of f niet minimaal. ook $a_n = b_n = 1$ dus
dan $g - f = (b_0 - a_0) + (b_1 - a_1)X + \cdots + (b_{n-1} - a_{n-1})X^{n-1}$
en $(g-f)(\alpha) = 0$, maar $gr(g-f) < n$
dus blijkbaar zijn g, f niet minimaal van graad voor de eigenschap
tenzij $g - f$ triviaal het nulpolynoom is.
dus $g - f = 0$ en $g = f$. f is dus uniek

Dit polynoom f noemen we het minimumpolynoom van α over K, genoteerd f_K^α

— opm: als $\alpha \in K$, dan is het minimumpolynoom $X - \alpha$
want graad 0 kan niet omdat $f(\alpha) = a_0 \neq 0$
omdat $f \neq 0$.

als $\alpha \notin K$ dan is de graad minstens 2
want anders is het polynoom noodzakelijk van de vorm $X - a_0$ maar dan $f(\alpha) = \alpha - a_0 = 0$
geeft $\alpha = a_0 \in K$ tegenspraak.

Vb wegens bovenstaande opmerking en de stelling dat $\sqrt{2} \in \mathbb{R}$ irrationaal is, $f_{\mathbb{Q}}^{\sqrt{2}} = X^2 - 2$, $f_{\mathbb{R}}^{\sqrt{2}}$ $X - \sqrt{2}$

— opm omdat $K[X]$ pid is, is $\mathrm{Ker}(ev_\alpha)$
met $ev_\alpha : K[X] \hookrightarrow L[X] \longrightarrow L$ een hoofdideaal
en dus is er een voortbrenger f van $\mathrm{Ker}(ev_\alpha)$
die uniek is wanneer we eisen dat
f monisch is (f is uniek op eenheid na
en a_n^{-1} is eenheid in K)
Bovendien, wanneer we bewijzen dat $K[X]$ pid is,
gebruiken we deling met rest om een element in
$K[X]f$ te vinden van laagste graad; dat is dan een
voortbrenger. hieruit $\mathrm{Ker}(ev_\alpha) = (f_K^\alpha)$

Dus $(f_K^\alpha) = \mathrm{Ker}(ev_\alpha)$ als $ev_\alpha : K[X] \hookrightarrow L[X] \to L$
want f_K^α is een polynoom van minimale graad uit dit ideaal en $K[X]$ is pid.

$\square$

St 9.8 $L \supset K$ uitbr. $\alpha \in L$ algebraïsch over K met minimumpolynoom $f_K^\alpha \in K[X]$

a) f_K^α is irreducibel in $K[X]$ en f_K^α is het enige monische irred. polynoom in $K[X]$ met $f(\alpha)=0$

b) Voor elke $g \in K[X]$: $g(\alpha) = 0 \iff f_K^\alpha \mid g$

c) $K[\alpha] = K(\alpha)$ en $K(\alpha) \cong K[X]/(f_K^\alpha)$

d) als v.r over K is $\dim_K(K(\alpha)) = gr(f_K^\alpha)$
en een basis is $B = \{1, \alpha, \dots, \alpha^{n-1}\}$ met $n = gr(f_K^\alpha)$

Bew Beschouw het homom. $\psi : K[X] \to K[\alpha]$ door $f \mapsto f(\alpha)$. Dit is een homom. want het is de samenstelling van $K[X] \hookrightarrow L[X]$ met $ev_\alpha : L[X] \to L$ en voor $f \in K[X]$ ligt $f(\alpha) \in K[\alpha]$ per definitie dus type $K[X] \to K[\alpha]$ kan hier.
Bovendien is het per definitie surjectief, $K[\alpha]$ bestaat uit alle $a_0 + a_1\alpha + \dots + a_n\alpha^n \in L$ voor $n \geq 0$, $a_i \in K$.
Tenslotte geldt dat f_K^α een voortbrenger van $\mathrm{Ker}(\psi)$ is wegens 3.4, dus isomorfiestelling:

$$K[X]/(f_K^\alpha) \cong K[\alpha]$$

nu is $K[\alpha] \subset L$ dus een domein, maar dan is (f_K^α) een priemideaal, dus omdat $K[X]$ pid is is het ook een maximaal ideaal en is f_K^α irreducibel

Dus volgt (a) & (b) als $g \in \mathrm{Ker}(\psi)$ dan $g \in (f_K^\alpha)$ dus $g = h \cdot f_K^\alpha$ voor een $h \in K[X]$ want (f_K^α) priemideaal.
$\Rightarrow$ (b)

$\Rightarrow$ (a)

en als g irreducibel is, dan volgt $g = u \cdot f_K^{\alpha}$ dus als g monic dan $u=1$ en $g = f_K^{\alpha}$

omdat wegens (f_K^{α}) maximaal volgt dat $K[\alpha]$ een lichaam is en $K[\alpha] \subset Q(K[\alpha]) = K(\alpha)$, maar tegelijkertijd is $K(\alpha)$ het kleinste lichaam dat $K \subset K(\alpha)$ en $\alpha \in K(\alpha)$ heeft, dus $K(\alpha) \subset K[\alpha]$,
volgt $K(\alpha) = K[\alpha] \cong K[X]/(f_K^{\alpha})$ $\Longrightarrow$ (c)

Nu nog (d): omdat elke $y = K(\alpha) = K[\alpha]$ een $y = g(\alpha)$ is met $g \in K[X]$, maar tevens kunnen we delen met rest voor willekeurige kopkermen niet-0 want K is lichaam, dus delen we met rest $g = q \cdot f_K^{\alpha} + r$ voor $gr(r) < gr(f_K^{\alpha}) =: n$ of $r = 0$ dus dan $g(\alpha) = q(\alpha) f_K^{\alpha}(\alpha) + r(\alpha) = k_0 + k_1\alpha + \cdots + k_{n-1}\alpha^{n-1}$ voor $r = k_0 + k_1 X + \cdots + k_{n-1} X^{n-1}$ ofwel alle 0 ofwel niet, maar $k_0, \dots k_{n-1} \in K$. dus $\{1, \alpha, \dots \alpha^{n-1}\}$ spant $K(\alpha)$ op. tegelijk zijn ze lineair onafhankelijk, want een $l_0 + l_1\alpha + \cdots + l_{n-1}\alpha^{n-1} = 0$ niet-triviaal levert een Polynoom $\tilde{f}$ met graad $n-1$ zodat $\tilde{f}(\alpha) = 0$, in tegenspraak met het gevonden minimumpolynoom. Dus is $\{1, \alpha, \dots, \alpha^{n-1}\}$ een basis $\square$

Uit H4 weten we al:

4.22 K lichaam en $f_1, f_2, .. f_t \in K[X_1, .., X_n]$
dan TFAE:

(i) er zijn geen $g_1, .. g_t \in K[X_1,..,X_n]$ met $g_1 f_1 + g_2 f_2 + .. + g_t f_t = 1$

(ii) er is een lichaam $L \supset K$ en er zijn $\alpha_1, .., \alpha_n \in L$
zodat $f_1(\alpha_1, .., \alpha_n) = .. = f_t(\alpha_1, .., \alpha_n) = 0$

met een bewijs dat alleen gebruikt dat $K[X_1, .., X_n]$
zoals elke commutatieve ring met $1 \neq 0$ en $I \subsetneq R$ ideaal
een maximaal ideaal bevat met $I \subset M$:

Bew. (i) $\Rightarrow$ (ii): dit betekent precies $1 \notin (f_1, f_2, .. f_t)$
dus $(f_1, .. f_t) \neq K[X_1, .., X_n]$, waaruit volgt dat
er een maximaal ideaal $M \subset K[X_1, .. X_n]$ is zodat
$I \subset M$. Bekijk dan $L := K[X_1, .. X_n]/M$: dit is een
lichaam. Bovendien, het homomorfisme $K \hookrightarrow K[X_1, .. X_n] \rightarrow L$
waarbij het eerste homom. inbedding van K in $K[X_1, .., X_n]$ is
en het tweede de canonieke afbeelding $R \rightarrow R/M$, is
injectief want K is een lichaam (2.18).
Dus we kunnen K opvatten als deelverzameling van L,
n.l. alle $(k \bmod M) \in L$ voor $k \in K \subset K[X_1, .. X_n]$.
en we zien f_j als $f_j = \underline{\sum_i a_i X_1^{i_1} X_2^{i_2} .. X_n^{i_n}}$
Nu resteert nog aan te tonen dat L^n inderdaad gemeensch. nulpunt
bevat voor $f_1, .. f_t$. Zij $\alpha_i = (X_i \bmod M) \in L$

dan $f_i(X_1 \bmod M, .., X_n \bmod M) =$ hierin zijn $X_1 .. X_n$
$f_i \in I \subset M$ dus $= \underline{0 \bmod M \in L}$ variabelen in
$L[X_1, .. X_n]$,
oftewel $\forall i \; f_i(\alpha_1, .. \alpha_n) = 0$ terwijl we anders $(X_i \bmod M) \in L$
schrijven!

(ii) $\Rightarrow$ (i): stel dat er een L is en $\alpha_1, .., \alpha_n \in L$ met
$f_1(\alpha_1 .. \alpha_n) = .. = f_t(\alpha_1, .., \alpha_n)$. Stel dat er toch

$g_1, .. g_t \in K[X_1 .. X_n]$ zijn met $g_1 f_1 + + g_t f_t = 1$
Dan volgt, wanneer we $g_1, .. g_t$ en $f_1, .. f_t$ als elementen van $L[X_1 .. X_n]$ zien en evalueren in $\alpha_1 .. \alpha_n$, dat

$$1 = (g_1 f_1 + \cdots + g_t f_t)(\alpha_1, \ldots, \alpha_n) =$$
$$g_1(\alpha_1 .. \alpha_n) f_1(\alpha_1, .. \alpha_n) + \cdots + g_t(\alpha_1 .. \alpha_n) f_t(\alpha_1, .. \alpha_n) =$$
$$g_1(\alpha_1, .. \alpha_n) \cdot 0 + \cdots + g_t(\alpha_1, .. \alpha_n) \cdot 0 = 0$$

dus $1 = 0$ tegenspraak. $\square$

Met deze stelling is de existentie van een uitbreidingslichaam L van K aangetoond waarin in L^n alle f_t een gemeensch. nulpunt $(\alpha_1, .. \alpha_n)$ hebben.

Uit deze stelling 4.22 volgt direct dat als $f \in K[X]$ monisch, irreducibel is, er een uitbreiding $L \supset K$ is met $\alpha \in L$ zodat $f(\alpha) = 0$
(immers als f irred. is in $K[X]$ volgt dat, omdat $K[X]$ pid is, dat $(f) \neq K[X]$ (en (f) is maximaalideaal,)
dus $1 \notin (f)$ dus er is geen $g \in K[X]$: $gf = 1$.
Dus er is een $L \supset K$ met $\alpha \in L$ en $f(\alpha) = 0$.

Bovendien is $f_K^\alpha = f$ wegens 9.8 (a): f is namelijk dan uniek voor " irreducibel en $f(\alpha) = 0$ "

— De volgende constructie van zo'n uitbreiding is echter veel explicieter

9.12 K lichaam en $f \in K[X]$ monisch en irreducibel.
Dan is er een uitbreiding $K \subset L$ met $\alpha \in L$ zodat $f(\alpha) = 0$ en $f = f_K^\alpha$ (ihb is α algebraïsch over K).

Bew f is irreducibel. Omdat $K[X]$ pid is, volgt dat $K[X]/(f) =: L$ een lichaam is.
Bovendien is het inbeddingshomom. vóór het canonieke homom, dwz $K \hookrightarrow K[X] \xrightarrow[\varphi]{} K[X]/(f)$, een homom dat wegens 2.18 injectief is.
We kunnen K dus opvatten als deellichaam $\{(k \bmod (f)) : k \in K\} \subset L$ en daarmee
$f = a_0 + a_1 X + \dots + a_n X^n \in K[X]$ als
$f = (a_0 \bmod (f)) + (a_1 \bmod (f)) X'^1 + \dots + (a_n \bmod (f)) X'^n \in L[X']$

dus volgt voor $\alpha = X \bmod (f) \in L$ dat
$$f(\alpha) = (a_0 \bmod (f)) + (a_1 \bmod (f))(X \bmod (f)) \dots + (a_n \bmod (f))(X^n \bmod (f))$$
$$= (a_0 \bmod (f)) + (a_1 X \bmod (f)) + \dots + (a_n X^n \bmod (f))$$
$$= (a_0 + a_1 X + \dots + a_n X \bmod (f))$$
$$= f \bmod (f) = 0 \bmod (f) \in L$$

dus α is algebraïsch over $K := \{k \bmod (f) : k \in K\}$
en f is irreducibel over K en monisch en $f(\alpha) = 0$
dus f is het unieke minimumpolynoom □

— De constructie uit 9.12 is bekend als de **Symbolische Adjungatie** van een nulpunt van f.

(Gevolg 9.13) Voor elke irreducibele $f \in K[X]$ is er een uitbreiding $L \supset K$ met $\alpha \in L$ en $f(\alpha) = 0$.

dit volgt doordat we f eerst monisch maken door verm met a_n^{-1}. Vervolgens passen we 9.12 toe.