H.11 Ontbindingslichamen

— in H10 was een uitbreiding $L \supset K$ van lichamen steeds een lichaam L waar K een deellichaam van was

— We zagen ook dat we voor irred. polynomen $f \in K[X]$ in elk geval op symbolische wijze een lichaam $L := K[X]/(f)$ konden verkrijgen waar K in zekere zin een deellichaam van was, en $L = K(\alpha)$ waar $\alpha = (X \bmod f)$

— nu zijn we geïnteresseerd in een veel specifiekere uitbreiding van K, n.l.

Def K lichaam en $f \in K[X]$ monisch. dan heet $L \supset K$ uitbr. een splijtlichaam of ontbindingslichaam als geldt:
(i) $\exists \alpha_1 \dots \alpha_n \in L$ $\quad f = \prod_{i=1}^{n} (X - \alpha_i)$
(ii) $\quad L = K(\alpha_1, \dots, \alpha_n)$

Vbd $X^4 - 2 = (X - i\sqrt[4]{2})(X + i\sqrt[4]{2})(X + \sqrt[4]{2})(X - \sqrt[4]{2})$
We hebben dus dat $\mathbb{Q}(-i\sqrt[4]{2}, i\sqrt[4]{2}, \sqrt[4]{2}, -\sqrt[4]{2})$ een splijtlichaam is, maar dit is tevens $\mathbb{Q}(i\sqrt[4]{2}, \sqrt[4]{2})$ en aangezien dit ook $(\sqrt[4]{2})^3 \cdot i\sqrt[4]{2} = i$ bevat, $\mathbb{Q}(i\sqrt[4]{2}, \sqrt[4]{2}) \supseteq \mathbb{Q}(i, \sqrt[4]{2})$ maar andersom $\sqrt[4]{2} \cdot i \in \mathbb{Q}(i, \sqrt[4]{2}) \Rightarrow$ "$\subseteq$" dus dit is $\mathbb{Q}(i, \sqrt[4]{2})$. $X^4 - 2$ is echter irreducibel over $\mathbb{Q}(i)$, dus we vinden $[\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}] = [\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}]$
$= gr(X^4 - 2) \cdot gr(X^2 + 1) = 8$ $\square$

— bestaat er altijd een splijtlichaam van f over K?
(en: is het uniek?)

— (Stelling: Existentie) Zij K lichaam en $f \in K[X]$ monisch. Dan is er een splijtlichaam van f over K.

Bew met inductie naar $n = gr(f)$
(IB) Voor $n = 1$ is K zelf een splijtlichaam.

(IH) Stel dat voor een zekere n voor alle monische polynomen $\in K[X]$ van graad $\leq n$ een spl. lichaam over K hebben:

(IS) Dan: zij $f \in K[X]$ van $gr(f) = n+1$. Twee gevallen: f irreducibel / reducibel.

- f reducibel: dan zijn er $g, h \in K[X]$, $gr(g) \leq n$, $gr(h) \leq n$ en $gh = f$ bovendien kunnen we g en h monisch kiezen

– Stelling: Existentie van ontbindingslichamen.

— opm: in H10 hebben we aangenomen dat er een groter lichaam $L \supset K$ was om mee te werken. Nu willen we met een bestaand lichaam een groter lichaam maken

Vbd $\mathbb{F}_5[X] \ni X^2 - 2$ is irreducibel, er zijn geen nulpunten.

Vbd vroeger bedachten we $\mathbb{C}$, een groter lichaam dat i bevat en wel groot genoeg is om vgl $X^2+1=0$ op te lossen.

En eigenlijk werken we gewoon in het lichaam $\mathbb{R}[X]/(X^2+1)$ waarbij $X \bmod (X^2+1) \overset{\sim}{\longmapsto} i$

— St. zij K lichaam en $f \in K[X]$ irreducibel. Dan is er een lichaamsuitbreiding $L \supset K$ met $\alpha \in L$ en $f(\alpha) = 0$

Bew symbolische adjungatie, verwarrende truc: zij $L = K[X]/(f)$ Omdat f irreducibel is, is (f) maximaal want $K[X]$ is een hoofdideaalring (want je kunt delen met rest dus $K[X]$ is zelfs Euclidisch) en elk irreducibel elem. in hir. brengt maximaal ideaal voort $\Rightarrow L$ is een lichaam (4.10) vat nu L op als een uitbreiding van K door het injectieve homomorfisme $K \hookrightarrow K[X] \twoheadrightarrow L$ (elk lich. homom is injectief!) zij nu $\alpha = (X \bmod (f)) \in L$, dan $f(\alpha) = (f \bmod (f)) = 0$ in L

– Die laatste stap is verwarrend misschien:
$f = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n \in K[X] \subset L[X]$, dan
$f(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n = a_0 + a_1\overline{X} + \cdots + a_n\overline{X}^n$
$= \overline{a_0} + \overline{a_1 X} + \cdots + \overline{a_n X^n} = \overline{a_0 + a_1 X + \cdots + a_n X^n} = \overline{0}$

$\square$

Vbd $\mathbb{F}_5$, $X^2 - 2 \in \mathbb{F}_5[X]$. Dan $\mathbb{F}_5[X]/(X^2-2)$ is lichaam en $\overline{X}$ voldoet aan $\overline{X}^2 - 2 = 0$

informeel: maar gebruik deze notatie niet: $\overline{X} = \sqrt{2}$
algebraïsch is er geen verschil tussen $\sqrt{2}$ en $-\sqrt{2}$
maar we maken in de reële getallen dat de $\sqrt{2} > 0$
is (alleen dan voegen we de structuur van een ordening toe).

Je zou het "$\mathbb{F}_5[\sqrt{2}]$" kunnen noemen. Maar eigenlijk liever niet —

Dit is verwarrend omdat je bij wortels heel andere verwachtingen hebt: $2\overline{X} \in \mathbb{F}_5[\sqrt{2}]$ voldoet aan
$(2\overline{X})^2 = 4\overline{X}^2 = 4(\overline{X}^2-2)+8 = 8 = 3$, $(2\sqrt{2})^2 = 3$
wat vreemd is. Dus $\sqrt{\ }$ notatie is verwarrend.

Gevolg: $f \in K[X]$ $f \neq 0$ met kopcoëff $c \in K$. Dan bestaat er een lich. uitbreiding $K \subset L$ met $\alpha_1, \dots \alpha_n \in L$, $n = gr(f)$ zo dat $f = c(X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_n)$ in $L[X]$

Bewijs: dat is inductie naar $n = gr(f)$.
opm als $n \leq 1$ dan $K = L$ kan gewoon.
Stel de stelling is waar voor alle polynomen van graad $< n$
over alle lichamen K')

Als $f \in K[X]$ alleen irreducibele factoren van graad $1 \leq$ heeft, dan geldt de stelling direct en zijn we klaar.
Stel daarom: f heeft monische irreducibele factor $g \in K[X]$ van graad ≥ 2 : $f = g \cdot h$
Pas dan de stelling toe op g. Dan breiden we K uit tot $K_1 = K[X]/(g)$ en is er $\alpha_1 = (X \bmod (g)) \in K_1$ met $g(\alpha_1) = 0$. Dus kunnen we het nulpunt (in een „domein K_1) 'naar buiten halen' in een factor $X - \alpha_1$:
$g = g_1 \cdot (X - \alpha_1)$. Dan bekijken we $g_1 \cdot h$ met graad $n-1$

en passen we de inductiehypothese toe en vinden we een lichaam $L \supset K_1$ met $g_1 \cdot h = c(X-\alpha_2)\cdots(X-\alpha_n)$, $\alpha_2 .. \alpha_n \in L$
en $\alpha_1 \in K_1 \subset L$ dus $f = c(X-\alpha_1)(\cdots)(X-\alpha_n)$ in L.

$\square$

— maar er is nu nog weinig controle over hoe L eruit komt te zien.

Def Als $L \supset K$ voldoet aan: $\exists\, \alpha_1 .. \alpha_n \in L$ met
$f = c(X-\alpha_1)\cdots(X-\alpha_n)$ in $L[X]$,
en L is zo klein mogelijk, dus er moet gelden
$L = K(\alpha_1 \ldots \alpha_n)$, want $K(\alpha_1 .. \alpha_n) \subseteq L$
is noodzakelijk zo.

De belangrijke stelling van H11 is dan ook:

St Gegeven een lich. K en een $f \in K[X]-\{0\}$, bestaat er een ontb. lichaam en het is op K-isomorfie na uniek

→ gevolg: we kunnen spreken van "het" ontb. lichaam van f over K en noteren het als Ω^f_K

Bew van existentie: pas toe dat er voor $f \in K[X]-\{0\}$ een uitbreiding $L \supset K$ is met $\alpha_1, .. \alpha_n \in L$ met
$f = c\cdot(X-\alpha_1)\cdots(X-\alpha_n)$
en gegeven zo'n uitbreiding kunnen $\alpha_1 .. \alpha_n$ adjungeren aan K: en $K(\alpha_1 .. \alpha_n)$ is ~~het~~ een ontb. lichaam

Bew. van uniciteit: Eerst wat begripsvorming

zij $K_1 \cong K_2$ en $\varphi: K_1 \to K_2$ een isomorfisme.
Dan induceert dit een isomorfisme van ringen $K_1[X] \xrightarrow{\sim} K_2[X]$
met $a_0 + a_1X + \cdots + a_nX^n \longmapsto \varphi(a_0) + \varphi(a_1)X + \cdots + \varphi(a_n)X^n$
noem dit Φ.

Zij dan $f_1 \in K_1[X]$, $f_2 = \Phi(f_1) \in K_2[X]$

Beide $K_1[X]$ en $K_2[X]$ zijn unieke ontbindingsringen

Stel $L_1 \supset K_1$ is een ontb. lichaam van f_1 over K_1
Stel $L_2 \supset K_2$ is een ontb. lich. van f_2 over K_2

Dan is er een isomorfisme $\psi : L_1 \xrightarrow{\sim} L_2$
met voor alle $a \in K_1$ is $\psi(a) = \varphi(a) \in K_2 \subset L_2$

We willen dus een uitbreiding ψ vinden van φ die isomorf is.

$$\begin{tikzcd}
L_1 \arrow[r, "\psi\ \sim"] \arrow[d, dash, dashed] & L_2 \arrow[d, dash, dashed] \\
\cup & \cup \\
K_1 \arrow[r, "\varphi\ \sim"] & K_2 \\
K_1[X] \arrow[r, "\Phi\ \sim"] & K_2[X]
\end{tikzcd}$$

$\longleftarrow$ hier is nog wat in te vullen $\longrightarrow$

We gaan dit straks toepassen op $K_1 = K_2 = K$, en dit is dus een veel algemenere uitspraak dan wat we nodig hebben. Maar het is makkelijker te bewijzen!

opmerking: $[L_1 : K_1] < \infty$ want $L_1 = K_1(\alpha_1 \cdots \alpha_n)$
en gevolg 10.7 geldt, want $\alpha_1 \cdots \alpha_n$ alg. over K_1.

Dus bewijs met inductie naar $[L_1 : K_1]$.
Neem zvva f monisch, want $c \in K$ is gewoon inverteerbaar.

IB Als $[L_1 : K_1] = 1$, dan $f = (X-\alpha_1)\cdots(X-\alpha_n) \in K_1[X]$
met dus $\alpha_1 \cdots \alpha_n \in K_1$
Laat dan $\beta_i := \varphi(\alpha_i)^{\in K_2}$ $\forall i = 1, \dots n$ dan

$$
\begin{aligned}
f_2 := \Phi(f_1) &= \Phi(X-\alpha_1) \cdots \Phi(X-\alpha_n) \\
&= (X - \varphi(\alpha_1)) \cdots (X - \varphi(\alpha_n)) \\
&= (X - \beta_1) \cdots (X - \beta_n) \quad \text{voor } \beta_i \in K_2
\end{aligned}
$$

en dus is $L_2 = K_2$ en dus is $\psi = \varphi$
het gezochte isomorfisme $L_1 \to L_2$

IH Neem aan $[L_1 : K_1] = m > 1$ en voor alle L_1', K_1', L_2', K_2'
met $[L_1' : K_1'] < m$ is de stelling waar.

Uit $[L_1 : K_1] > 1$ volgt dat er een monische irreducibele factor van graad > 1 in f is, anders zouden alle nulpunten van f in K_1 liggen en gold wel $[L_1 : K_1] = 1$.
Noem deze factor $g_1 \in K_1[X]$ en schrijf $f_1 = h_1 \cdot g_1$
definieer $h_2 = \Phi(h_1)$, $g_2 = \Phi(g_1)$ en omdat een niet-triviale ontb. van $\Phi(g_1)$ een niet-triviale ontb. van g_1 geeft, is g_2 ook irreducibel.
Neem zvva g_1 monisch, dan is de kopcoeff. van $\Phi(g_1)$ $\varphi(1) = 1$ dus g_2 is ook monisch (& irred.).

Zij $\alpha \in L_1$ een nulpunt van g_1, want alle nulpunten van g zijn nulpt. van f_1 en liggen dus in L_1.
Zij $\beta \in L_2$ een nulpt. van g_2.
Dan gaan we "tussenlichamen" "bouwen".

$$\begin{tikzcd} L_1 & L_2 \\ K_1(\alpha) \arrow[u, phantom, "\cup" description] \arrow[r, "\tilde{\varphi}", "\sim"'] & K_2(\beta) \arrow[u, phantom, "\cup" description] \\ K_1 \arrow[u, phantom, "\cup" description] \arrow[r, "\varphi", "\sim"'] & K_2 \arrow[u, phantom, "\cup" description] \end{tikzcd}$$

$$[L_1 : K_1(\alpha)] = \frac{[L_1 : K_1\ ]}{[K_1(\alpha) : K]} < [L_1 : K_1]$$

1.) we vinden een uitbreiding $\tilde{\varphi} : K_1(\alpha) \to K_2(\beta)$

2.) we merken op dat $f_1 \in K_1(\alpha)[X]$, $f_2 \in K_2(\beta)[X]$

3.) en we merken op $[L_1 : K_1(\alpha)] < [L_1 : K_1]$ en passen IH toe : er is een uitbr. ψ van $\tilde{\varphi}$ $L_1 \to L_2$

4.) We laten zien dat ψ ook een uitbr. van φ is.

1.) Deze claim volgt wegens : g_1 is $f^{\alpha}_{K_1}$ dus

$$\begin{array}{cccccc} \alpha & K_1(\alpha) & & K_2(\beta) & \beta & \\ \phi_1 \uparrow & \wr\| & & \wr\| & \uparrow & \phi_2 \\ \overline{X} & K_1[X]/(g_1) & & K_2[X]/(g_2) & \overline{X} & \end{array}$$

maar we hebben al het isomorfisme $\Phi : K_1[X] \to K_2[X]$

en omdat $\Phi((g_1)) \underset{\uparrow}{=} (\Phi(g_1)) = (g_2)$

pid en $\Phi(g_1) \in \Phi((g_1))$

dus dit induceert een isomorfisme $\overline{\Phi} : K_1[X]/(g_1) \xrightarrow{\sim} K_2[X]/(g_2)$

En daarmee is $\underbrace{\phi_2 \circ \overline{\Phi} \circ \phi_1^{-1}}$ is een isomorfisme

$K_1(\alpha) \xrightarrow{\sim} K_2(\beta)$. noem dit $\tilde{\varphi}$.

Bovendien geldt $\tilde{\varphi}(a) = \phi_2 \circ \overline{\Phi} \circ \phi_1(a) =$

$\phi_2 \circ \overline{\Phi}(\underset{\substack{\Uparrow \\ K_1[X]/(g_1)}}{a}) = \phi_2(\Phi(a) \bmod (g_2))$

$= \phi_2(\varphi(a) \bmod (g_2))$

$= \varphi(a)$. dus $\tilde{\varphi}$ breidt φ uit.

2.),3.) pas IH toe. omdat we nu een isomorfisme $\psi : L_1 \xrightarrow{\sim} L_2$ hebben met $\psi(a) = \tilde{\varphi}(a)$ $\forall a \in K_1(\alpha)$

volgt voor $a \in K_1$: $\psi(a) \underset{\substack{\uparrow \\ a \in K_1(\alpha) \\ \text{dus}}}{=} \tilde{\varphi}(a) \underset{\text{zie 1.)}}{=} \varphi(a)$. $\square$

met naïeve inductie loop je vast omdat er na de stap α, β al gelijk twee verschillende lichamen $K(\alpha)$, $K(\beta)$ staan en loop je naïef denkend algauw vast. Daarom de meer algemene aanpak.

Def Een $L_1 \supset K \subset L_2$ uitbreidingen, dan heet $f : L_1 \longrightarrow L_2$ een K-homomorfisme als $\forall a \in K \quad f(a) = a$
en een K-isomorfisme is een K-homom dat bijectief is.

(Stelling over uniciteit van "Ω^f_K")

K lichaam, $f \in K[X] - \{0\}$. Dan is er een ontb. lichaam van f over K en op K-isomorfie na is dit uniek

$$\begin{tikzcd} \Omega \arrow[rr, "\sim"] & & \Omega' \\ & K \arrow[ul] \arrow[ur] & \end{tikzcd}$$

er is dus een K-isomorfisme $\Omega \xrightarrow{\sim} \Omega'$

dus voor $x \in \Omega$ geldt $\varphi(x) = x$ als $x \in K$.

Bew Direct gevolg van voorgaande stelling toegepast op $\varphi = Id_K$ en $L_1 = \Omega$ $L_2 = \Omega'$ $\square$

H. 12 Eindige lichamen

— We gaan nadenken over lichamen met eindig veel elementen. Zij K eindig

Wat weten we: $\mathbb{Q}$ is oneindig, dus het priemlichaam $K_0 \subseteq K$ kan niet "$\cong \mathbb{Q}$" zijn

$\Longrightarrow$ karakteristiek is eindig dus een priemgetal.

— Daarmee is $K_0 \cong \mathbb{F}_p$ met p priem.
En dan $\dim_{\mathbb{F}_p}(K) = [K : \mathbb{F}_p] = n < \infty$.
en dus is er een basis $e_1 \dots e_n$ over $\mathbb{F}_p$
(preciezer: K_0, maar op isomorfie na werken we over $\mathbb{F}_p$)

Dan is elke $\alpha \in K$ eenduidig als $a_1e_1 + \dots + a_ne_n$ te schrijven en dus geeft elke keuze $a_1, \dots, a_n \in \mathbb{F}_p^n$ een uniek elem. Maw $K \underset{!}{\cong} \mathbb{F}_p^n$ als <u>lineair isomorfisme</u>.

$$\Longrightarrow |K| = p^n \quad (\text{noem } p^n = q$$

— K^* is een cyclische groep (want 3.14, R domein en G eindige o.g. van R^*, met $K^* \subseteq K^*$ eindig)

Dus $K^* = \langle \alpha \rangle$ voor een zekere $\alpha \in K - \{0\} = K^*$
En $\alpha \in K^*$ heeft orde $p^n - 1$ (noem $p^n = q$) $= q - 1$

I.h.b. $K = \{0, 1, \alpha, \alpha^2, \dots, \alpha^{q-2}\}$ (per definitie, $\langle \alpha \rangle \cup \{0\}$)
$\alpha^{q-1} = 1$ etc.

dus $K = \mathbb{F}_p(\alpha)$ want $\{1, \alpha, \dots \alpha^{q-2}\}$ spant K op over $\mathbb{F}_p$
dus wegens $g(\alpha)$ en de kennis dat K eindig is dus α wel algebraïsch moet zijn, anders is $\mathbb{F}_p(\alpha)$ oneindig, volgt dit. En bovendien

$$K \cong \mathbb{F}_p(\alpha) \cong \mathbb{F}_p[X] / (f^{\alpha}_{\mathbb{F}_p})$$

en $f^{\alpha}_{\mathbb{F}_p} \in \mathbb{F}_p[X]$ is irreducibel en monisch van graad..

$|K| = p^n$ dus $gr(f^{\alpha}_{\mathbb{F}_p}) = [K : \mathbb{F}_p] = n$

— Bovendien weten we $\beta^q = \beta \quad \forall \beta \in K$ want
$char(K) = p$ en $p | q = p^n$

Andere benadering: $\beta = \alpha^i$, $\alpha^{q-1} = 1$ dus
$\beta^q = \alpha^{qi} = (\alpha^{q-1})^i \alpha^i = 1^i \beta = \beta \quad \square$

$\Longrightarrow$ Conclusie: in $K[X]$ geldt de factorisatie

$$X^q - X = \prod_{\beta \in K} (X - \beta)$$

want elke $\beta \in K$ voldoet aan $\beta^q - \beta = 0$ en is dus nulpunt, en dat is precies de graad (n.l. q) en K is domein dus hoogstens q nulpunten.

Ihb $K = \Omega^{X^q - X}_{\mathbb{F}_p}$

(construeren we)

— En dus concluderen we: K bestaat, want het rechterlid bestaat, of er gaat is fout en K bestaat niet.

— in elk geval is er een recept waarmee we aan de gang kunnen.