Ringen en Lichamen

Luc Veldhuis

4 December 2017

Uitbreiding

F een lichaam.
Priemlichaam in F:

- char(F)$= p > 0$: $\mathbb{F}_p$
- char(F)$= 0$: $\mathbb{Q}$

Als E/F is uitbreiding, dan is E een vectorruimte van F.
$E \times E \to E$ optelling (van vectoren)
$(e, f) \mapsto e + f$
$F \times E \to E$ scalaire vermenigvuldiging
$(c, e) \mapsto ce$.
Noem $\dim_F E$ de **graad** van de uitbreiding. Notatie: $[E : F]$.
Noem E/F **eindig** als $[E : F] < \infty$ en anders oneindig.

Lichaams theorie

Voorbeeld

- - $[\mathbb{C} : \mathbb{C}] = 1$
    $[\mathbb{C} : \mathbb{R}] = 2$ ($\{1, i\}$ is een $\mathbb{R}$ basis van $\mathbb{C}$)
    $[\mathbb{C} : \mathbb{Q}] = \infty$
- Als F een eindig lichaam is met $\mathrm{char}(F) = p$ en $[F : \mathbb{F}_p] = d < \infty$ dan is $F \cong \mathbb{F}_p^d$ als $\mathbb{F}_p$ een vector ruimte. Dus $|F| = p^d$.

Opgave

Als $E/F/k$ een **toren** van lichaams uitbreidingen dan geldt $[E : k] = [E : F][F : k]$.
Zelfs als $\{a_i\}_{i \in I}$ een F basis is van E, en $\{b_i\}_{j \in J}$ een k basis is van F, dan is $\{a_i b_j\}_{i \in I, j \in J}$ een k basis van E.

Lichaams theorie

Definitie

We hebben een notatie nodig voor uitbreiding.
Als E/F een uitbreiding is:

- Als $A \subseteq E$ een deelverzameling, dan is $k(A)$ het kleinste deellichaam van E dat k en A bevat. Als $A = \{a_1, \ldots, a_n\}$ (eindig) dan schrijf je $k(a_1, \ldots, a_n)$.
  Als $F = k(a_1, \ldots, a_n)$ dan is F **eindig voorgebracht** over k en de $a_1, \ldots, a_n$ zijn **geadjungeerd** aan k.
- Als $F = k(a)$ voor $a \in E$ dan heet F/k enkelvoudig. (Engels: simple)

Opgave

$k(a_1, a_2) = k(a_1)(a_2)$.

Lichaams theorie

Voorbeeld

In $\mathbb{C}$: $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ geldt:
$\mathbb{Q}(\sqrt{2},\sqrt{3})$ graad 2.
$\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2}, a, b \in \mathbb{Q}\}$ dus $[\mathbb{Q}[\sqrt{2} : \mathbb{Q}] = 2$. Basis: $\{1, \sqrt{2}\}$.
Dus
$[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4.$

Voorbeeld

$\mathbb{Q}(\sqrt[4]{10}, -\sqrt[4]{10}, i\sqrt[4]{10}, -i\sqrt[4]{10}) = \mathbb{Q}(\sqrt[4]{10}, i)$ wortels van $x^4 - 10$ in $\mathbb{C}$.
Bewijs '$\supseteq$':
$\mathbb{Q} \subseteq$ LHS. $\sqrt[4]{10} \in$ LHS.
$i = i\sqrt[4]{10}(\sqrt[4]{10})^{-1} \in$ LHS.
$\subseteq$ Opgave.

Lichaams theorie

Opgave

In $\mathbb{C}$, als $n \geq 2$ zij $\zeta = e^{2\pi i/n}$ dus $\zeta^n = 1$.
Dan is $\mathbb{Q}(1, \zeta, \zeta^2, \ldots, \zeta^{n-1}) = \mathbb{Q}(\zeta)$.

§2 Enkelvoudige uitbreidingen

Idee

$\sqrt{2}$ in $\mathbb{R}$ is een vortel van $x^2 - 2$ in $\mathbb{Q}[x]$.
Maar π (of e) is nooit een nulpunt van een $f(x) \in \mathbb{Q}[x]$, $f(x) \neq 0$.

Definitie

E/F een uitbreiding, $a \in E$.
a heet **algebraïsch** over F als a een nulpunt is van een $f(x) \neq 0$ in $F[x]$.
Als dat niet zo is, dan heet a **transcendent** over F.

Uitleg definitie

Voor E/F en $a \in E$ definieer $s_a : F[x] \to E$ met $f(x) \to f(a)$.
s_a een ringhomomorfisme. Dus is
$Im(s_a) = F[a] = \{b_0 + b_1 a + \cdots + b_n a^n$ met $n \geq 0$, alle $b_i \in F\}$ is een deelring van E, zelfs van $F(a)$.
We zien ook $F[a] \subseteq F(a)$.
$Im(s_a)$ is commutatief, $1 \in Im(s_a)$, $Im(s_a)$ heeft geen nuldelers.
$Im(s_a)$ is een integritieits gebied.
$Ker(s_a)$ is een priemideaal van $F[x]$. De idealen zijn: (0), $(f(x))$, $f(x)$ monisch $\neq 0$.

§2 Enkelvoudige uitbreidingen

Twee gevallen

- $Ker(s_a) = \{0\}$. Hier is a transcendent over F
- $Ker(s_a) = (m_a(x))$ met $m_a(x)$ monisch irreducibel in $F[x]$. Hier is a algebraïsch over F, $m_a(x)$ heet het minimum polynoom van a over F. Voor $f(x)$ in $F[x]$ geldt: $f(a) = 0 \Leftrightarrow m_a(x)|f(x)$ in $F[x]$.

Voorbeeld

$E = \mathbb{C}$, $F = \mathbb{Q}$, $a = \sqrt{3}$.
$s_a : \mathbb{Q}[x] \to \mathbb{C}$.
Wat is de $Ker(s_a)$?
$x^2 - 3 \in Ker(s_a)$ want $(\sqrt{3})^2 - 3 = 0$.
$(x^2 - 3) \subseteq Ker(s_a) \subsetneq \mathbb{Q}$. $x^2 - 3$ is monisch en irreducibel in $\mathbb{Q}[x]$.
(Eisenstein met $p = 3$)
Hieruit volgt dat $(x^2 - 3)$ een maximaal ideaal is van $\mathbb{Q}[x]$.
Dus $Ker(s_a) = (x^2 - 3)$ en $m_a(x) = x^2 - 3$.
Dus $\mathbb{Q}[x]/(x^2 - 3) \cong \mathbb{Q}[a] = Im(s_a)$ $\mathbb{Q}[x]/(x^2 - 3)$ is een lichaam, want $(x^2 - 3)$ is een priemideaal, dus $Im(s_a)$ is een lichaam.

Voorbeeld (vervolg)

$\mathbb{Q}[a] \subseteq \mathbb{Q}(a)$ per definitie.
$\mathbb{Q}(a) \subseteq \mathbb{Q}[a]$ omdat $\mathbb{Q}[a]$ hier een lichaam is dat $\mathbb{Q}$ en a bevat.
Dus $\mathbb{Q}(a) = \mathbb{Q}[a]$ geldt altijd als $Ker(s_a) \neq (0)$.
Ook $\mathbb{Q}[x]/(x^2-3) = \{\overline{b_0 + b_1 x} | b_0, b_1 \in \mathbb{Q}\}$ (elke klasse 1 keer).
Dus nu geldt ook $\mathbb{Q}(a) = \{\overline{b_0 + b_1 a} | b_0, b_1 \in \mathbb{Q}\}$
$\mathbb{Q}[x]/(x^2-3)$ heeft $\mathbb{Q}$ basis $\overline{1}, \overline{x}$.
Dit isomorfisme is nu een ringisomorfisme **en** van $\mathbb{Q}$ vectorruimtes.
Conclusie: $\{1, a\}$ is een $\mathbb{Q}$ basis van $\mathbb{Q}(a) = \mathbb{Q}[a]$.

§2 Enkelvoudige uitbreidingen

Propositie

Stel E/F is een uitbreiding, $a \in E$ algebraïsch over F met minimum polynoom $m_a(x)$ over F van graad $d \geq 1$.
Dan:

- $F[x]/(m_a(x)) \cong F[a]$ is een lichaams isomorfisme.
- $F(a) = F[a] = \{b_0 + b_1 a + \cdots + b_{d-1} a^{d-1} | b_i \in F\}$ (alles uniek)
- $[F(a) : F] = d$ en $\{1, a, \ldots, a^{d-1}\}$ is een F basis van $F(a)$.

Voorbeeld

$E = \mathbb{C}$, $F = \mathbb{Q}$, $a = \sqrt[3]{2}$.
$x^3 - 2 \in Ker(s_a)$ ook irreducibel in $\mathbb{Q}[x]$ (Eisenstein $p = 2$).
Er geldt $m_a(x)|x^3 - 2$ met $x \in F[x]$, want $x^3 - 2$ is irreducibel en monisch in dus $m_a(x) = x^3 - 2$.
Dus $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}[\sqrt[3]{2}] = \{b_0 + b_1 a + b_2 a^2 | b_i \in \mathbb{Q}\}$ is een lichaam met $d = 3$ en $a^3 - 2 = 0$.
Wat te doen met een term in de vorm: $a^4 - 2a = 0$
Rekenen in $\mathbb{Q}(a)$:
$(1 + a^2)(1 - 3a^2) = 1 - 2a^2 - 3a^4 = 1 - 2a^2 - 3(2a) = 1 - 6a - 2a^2$.

Voorbeeld (vervolg)

Voor inverse:
Als $m(x)$ irreducibel is in $F[x]$ met graad $d \geq 1$ en $g(x)$ in $F[x]$ heeft $\deg(g(x)) < d$ en $g(x) \neq 0$ dan is $ggd(m(x), g(x)) = 1$ want $m(x)$ is monisch, dus delers zijn $1, m(x)$, $m(x)|g(x)$ dus $g(x) = p(x)m(x)$ kan niet met graad.
Dus Bézout: $A(x)m(x) + B(x)g(x) = 1$ voor zekere $A(x)$, $B(x)$ in $F[x]$ (met het uitgebreide Euclidische algoritme). Als $m(a) = 0 \Rightarrow B(a)g(a) = 1$, dus $B(a) = g^{-1}(a)$.
Merk op: $A(x)$ speelt geen rol, hoef je niet te berekenen.

§2 Enkelvoudige uitbreidingen

Voorbeeld

Met $a = \sqrt[3]{2}$ in $\mathbb{Q}(a) = \{b_0 + b_1 a + b_2 a^2 | b_i \in \mathbb{Q}\}$ is de inverse van $2 + a$ gelijk aan $\frac{2}{5} - \frac{1}{5}a + \frac{1}{10}a^2$
$ggd(x^3 - 2, 2 + x) = 1.$