Ringen en Lichamen

Luc Veldhuis

11 December 2017

Lichaams theorie

Herhaling

- $F/\mathbb{F}_p$, $[F : \mathbb{F}_p] = d$, F is een d dimensionale $\mathbb{F}_p$ vectorruimte.
  $F \cong \mathbb{F}_p^d$.
  $|F| = |\mathbb{F}_p^d| = p^d$.
- $F[X]/(f(x)) = \{\overline{a_0 + a_1 x + \cdots + a_{d-1}x^{d-1}}\}$.
  $d = \deg(f(x))$ met alle $a_i \in F$.

Idee

Als F een lichaam is met $q = p^d$ elementen p een priemgetal en $d \geq 1$ en $a \in F^*$, dan is $a^{q-1} \equiv 1$ (Lagrange voor groep F^*).
a is nulpunt van $x^{q-1} - 1$.
F is de nulpuntsverzameling van $x^q - x$.
Vandaag: draai dit om. Maak een eindig lichaam met q elementen als de nulpuntsverzameling van $x^q - x$.

Lichaams theorie

Stelling 3.1

Als F een lichaam is en $f(x)$ een polynoom met coëfficiënten in $F[X]$ en graad ≥ 1 heeft, dan bestaat er een eindige uitbreiding E/F zodat $f(x)$ een product is van lineaire factoren in $E[X]$.
$f(x)$ splitst volledig in $E[X]$.

Bewijs

Inductie naar $\deg(f(x))$ (en alle F)
Als $\deg(f(x)) = 1$, neem $E = F$.
Als $\deg(f(x)) = d \geq 2$, neem aan dat de bewering geldt voor alle F, alle $g(x)$ in $F[x]$ met graad $1, 2, \ldots, d-1$.
Schrijf $f(x) = g(x)h(x)$ in $F[x]$ met $g(x)$ irreducibel in $F[x]$ (want ontbindingsring).
Laat y een andere variabele zijn en $F' = F[x]/g(y)$.
F' is een lichaam, want $g(y)$ is irreducibel in $F[y]$.
We hebben $F \subseteq F'$ als deellichaam en $[F' : F] = \deg(g(x))$.

Bewijs (vervolg)

Zij a de kasse van y in F'.
Dan is $g(a) = 0$ in F'.
In $F'[x]$ hebben we $g(x) = (x - a)\widetilde{g}(x)$ voor een $\widetilde{g}(x)$ in $F'[x]$.
$f(x) = (x - a)\widetilde{g}(x)h(x)$ in $F'[x]$. Hierin heeft $\widetilde{g}(x)h(x)$ graad $d - 1$ in $F'[x]$.
Volgens de inductie (voor $\widetilde{g}(x)h(x)$ en lichaam F') is er een eindige uitbreiding E/F' zodat $\widetilde{g}(x)h(x)$ volledig splitst in $E[x]$.
$a \in F' \subseteq E \Rightarrow f(x) = (x - a)\widetilde{g}(x)h(x)$ splitst volledig in $E[x]$.
E/F is eindig: $[E : F] = [E : F'][F' : F] < \infty$.

Voorbeeld

$F = \mathbb{Q}$, $f(x) = x^4 - 2$ irreducibel (Eisenstein met (2)).
$F' = \mathbb{Q}[y]/(y^4 - 2) \cong \mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R}$.
In $F'[x]$ hebben we $x^4 - 2 = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x^2 + \sqrt[4]{2})$.
$(x^2 + \sqrt[4]{2})$ heeft geen reële wortels, dus ook niet in $F \subseteq \mathbb{Q}$. Als we wel imaginaire getallen mee nemen krijgen we:
$x^4 - 2 = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - i\sqrt[4]{2})(x + i\sqrt[4]{2})$.
Dit geeft $F = \mathbb{Q} \subseteq F' = \mathbb{Q}(\sqrt[4]{2}) \subseteq E = \mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, i)$.
Het minimum polynoom van $i\sqrt[4]{2}$ over F' deelt $x^2 + \sqrt[4]{2}$.
Geen nulpunt in $F' \Rightarrow$ minimum polynoom is $x^2 + \sqrt[4]{2}$.

§4Eindige lichamen

Stelling

Als p een priemgetal is, $d \geq 1$,$q = p^d$ dan:

- Er bestaat een lichaam met q elementen.
- Elk tweetal lichamen met q is isomorf.

Bewijs

- Neem een eindige lichaamsuitbreiding $E/\mathbb{F}_p$ zodat $x^q - x$ volledig splitst in $E[x]$, dus $x^q - x = \prod_i = 1^q (x - q_i)$ in $E[x]$. Zij $F = \{a_1, \ldots, a_q\}$.
  Claim: F is een deellichaam van E. met q elementen (dat wil zeggen $a_1, \ldots, a_q$ zijn verschillend.).

Bewijs claim

- We gaan na (Exercise 1.11?) Gebruik voor $\alpha \in F$ geldt $\alpha \in F \Leftrightarrow \alpha^q = \alpha$.
  - $1 \in F$ want $1^q = 1$
  - als $a, b \in F$, dan ook $a - b_i$, $ab \in F$. Neem $a, b \in F$ dus $a^q = a, b^q = b$ dan geldt $(ab)^q = a^q b^q = ab$ dus $ab \in F$.
    Als Fr_p de Frobenius in karakteristiek p is, dus $Fr_p(\beta) = \beta^q$ en $Fr_p(\beta + \gamma) = (\beta + \gamma)^p = \beta^p + \gamma^p = Fr(\beta) + Fr(\gamma)$ want p termen vallen weg en $p^d = q$. $Fr(\beta\gamma) = Fr(\beta)Fr(\gamma)$.
    $(a-b)^q = Fr_p^d(a-b) = Fr_p^d(a) - Fr_p^d(b) = a^q - b^q = a - b \in F$.
  - Als $a \in F$, $a \neq 0$ dan a^{-1} in F.
    $(a^{-1})^q = a^{-q} = (a^q)^{-1} = a^{-1}$, dus $a \in F$.
- Stel dat niet alle a_i verschillend zijn.
  Dan is er een i met $(x - a_i)^2 | x^q = x \in E[x]$.
  Met y een andere variabele, vul $x = y + a_i$ in, dan zou $y^2 | (y + a_i)^q - (y + a_i) = y^q + a_i^q - y - a_i = y^q - y$ in $E[y]$ want $a_i^q = a_i \in F$.

Bewijs (vervolg)

- Zij K een lichaam met q elementen, volstaat te bewijzen: K is isomorf met F.
  We hebben $\mathbb{F}_p \subseteq F \subseteq E$ en $\mathbb{F}_p \subseteq \mathbb{F}_p[x]/(m_b(x)) \subseteq \mathbb{F}_p[x]$.
  $K = \mathbb{F}_p(b)$ voor een $b \in K$, bijvoorbeeld als $K^* = \langle b \rangle$. Dan is $K \cong \mathbb{F}_p[x]/(m_b(x))$ met $(m_b(x))$ in $\mathbb{F}_p[x]$ het minimumpolynoom van b over $\mathbb{F}_p$.
  Idee vind $\phi : \mathbb{F}_p[x] \to F$ met $Ker(\phi) = (m_b(x))$.
  Merk op: b is nulpunt van $x^q - x$, dus $m_b(x)$ deelt $x^q - x$ in $\mathbb{F}_p[x]$.
  Dan zijn er d elementen in F met $m_b(x) = (x - a_{i_1}) \dots (x - a_{i_d})$ in $F[x]$.
  $x^q - x = \prod_{i=1}^{q} (x - a_i)$ in E.

Bewijs (vervolg)

Laat $c = 1$ van die a_{i_j}.
Definieer $\phi : \mathbb{F}_p[x] \to \mathbb{F}_p$ met $g(x) \to g(c)$, dan geldt $(m_b(x)) \in Ker(\phi) \subsetneq \mathbb{F}_p[x]$ want $m_b(c) = 0$ en $(m_b(x))$ is maximaal (want $m_b(x)$ is irreducibel.
Dus $(m_b(x)) = Ker(\phi)$.
Dus in totaal:

$$\begin{array}{rcl} K \cong & \mathbb{F}_p[x]/(m_b(x)) & \cong Im(\phi) \\ f(b) \hookleftarrow & \overline{f(x)} & \mapsto f(c) \end{array}$$

Dus $K \cong Im(\phi) \subseteq F$, $b \mapsto c$.
$|K| = |Im(\phi)| = q = |F|$, dus $Im(\phi) = F$.

Opmerking

Als $K = \mathbb{F}_p(b)$ en $m_b(x) \in \mathbb{F}_p[x]$ minimumpolynoom van b over $\mathbb{F}_p$ en $F/\mathbb{F}_p$ met $c \in F$ en $m_b(c) = 0$ dan krijg je:

$$\begin{array}{rcl} K \cong & \mathbb{F}_p[x]/(m_b(x)) & \cong \mathbb{F}_p(c) \subseteq F \\ f(b) \hookleftarrow & \overline{f(x)} & \mapsto f(c) \end{array}$$

met $b \mapsto c$.

Voorbeeld

$F = \mathbb{F}_7[x]/(x^2+1)$, $E = \mathbb{F}_7[y]/(y^2+y+3)$.
x^2+1 irreducibel in $\mathbb{F}_7[x]$, y^3+y+3 irreducibel in $\mathbb{F}_7[y]$.
E, F zijn lichamen met 7^2 elementen.
Zij $b \in F$ de klasse van x, $c \in E$ de klasse van y.
Minimumpolynoom van b over $\mathbb{F}_7$ is x^2+1.
Voor isomorfisme $f : F \to E$ vind een element d in E met $d^2+1=0$.
Probeer $d = a_0 + a_1 c$ met $a_0, a_1 \in \mathbb{F}_7$. We zien $c^2 = 6c+4$.
$(a_0+a_1c)^2+1 = 4a_1^2 + a_0^2 + 1 + 2a_1(3a_1+a_0)$.

$$\text{Dit is } 0 \Leftrightarrow \begin{cases} 4a_1^2+a_0^2+1=0 \\ 2a_1(3a_1+a_0)=0 \end{cases} \Leftrightarrow \begin{cases} a_0=4 \\ a_1=1 \end{cases} \text{ of } \begin{cases} a_0=3 \\ a_1=6 \end{cases}.$$

Dus $c = 4+a$ of $3+6c = -(4+a)$.
Dan geeft $f : F \to E$ met $a_0 + a_1 b \mapsto a_0 + a_1 d = a_0 + a_1(3+6c) = (a_0+3a_1) + 6a_1 c$ met alle $a_i \in \mathbb{F}_7$