Ringen en Lichamen

Luc Veldhuis

20 November 2017

Polynoom ringen

Stelling

Als R een ontbindingsring is, $F = Frac(R)$ dan is $R[x]$ dat ook, met irreducibele factoren:

- $\pi \in R$, π irreducibel in R
- $f(x) \in R(x)$, $\deg(f(x)) \geq 1$, $ggd(\text{coefficienten}) = 1$, $f(x)$ is irreducibel in $R[x]$

Polynoom ringen

Bewijs existentie

Elk elementen $\neq 0 \notin \mathbb{R}[x]^* = R^*$ is een product van elementen van type (i) en (ii).
Als dat elementen in R is, dan kan het met type (i).
Dus neem $f(x) \in R[x]$, $\deg(f(x)) \geq 1$. Schrijf
$f(x) = q_1(x) \dots q_m(x)$ met alle $q_i(x)$ irreducibel in $F[x]$.
Gauß lemma, aannemen dat alle $q_j(x) \in R[x]$, nog steeds irreducibel in $F[x]$.

Schrijf $q_j(x) = \begin{cases} \widetilde{q_j}(x) & \text{als } ggd(coeff) = 1 \\ d_j \widetilde{q_j}(x) & \text{als } ggd(coeff) = d_j \notin R^* \end{cases}$.

$f(x) = d\widetilde{q_1}(x) \dots \widetilde{q_m}(x)$ met $d = \pi d_j$.
Alle $\widetilde{q_j}(x)$ zijn nu van type (ii). Schrijf d als product van type (i). (Als $d \neq 1$, laat d weg als $d = 1$.) Dus elk element $\neq 0 \notin R[x]^*$ is een product van type (i), (ii). Ook het volgt dat er geen andere irreducibele elementen zijn in $R[x]$.

Bewijs uniciteit

Al bekend voor element in $R \neq 0 \notin R^*$.
Dus stel $\deg(f(x)) \geq 1$ en
$f(x) = \pi_1\pi_2 \dots \pi_r p_1(x) \dots p_m(x) = \xi_1\xi_2 \dots \xi_s q_1(x) \dots q_n(x)$ met π_i, ξ_j type (i), $p_i(x)$, $q_j(x)$ type (ii), $s, r \geq 0$, $m, n \geq 1$.
De factorizatie in $F[x]$ is dan $(\pi_1 \dots \pi_r p_1(x))p_2(x) \dots p_m(x)$ en $(\xi_1 \dots \xi_r q_1(x))q_2(x) \dots q_n(x)$ met $m = n$ en na eventueel hernummeren $p_i(x) = \frac{a_i}{b_i} q_i(x)$ met $a_i, b_i \in R$ en $a_i, b_i \neq 0$, dus nu zijn $p_i(x)$ en $q_i(x)$ geassocieerd in $F[x]$. Dus $b_i p_i(x) = a_i q_i(x)$ in $R[x]$. Voor de linker term geldt $ggd(coeff) = b_i$, en voor de rechter term geldt $ggd(coeff) = a_i$ want $p_i(x)$, $q_i(x)$ van type (ii).
Dus $a_i = u_i b_i$ met $u_i \in R^*$ en $p_i(x) = u_i q_i(x)$ met $u_i \in R^*$ dus $p_i(x)$, $q_i(x)$ geassocieerd in $R[x]$.
$\pi_1\pi_2 \dots \pi_r = u\xi_1 \dots \xi_s$ met $u \in R^*$.
Nu volgt $r = s$ en na eventueel hernummeren is π_i geassocieerd met ξ_i in R.

Polynoom ringen

Voorbeeld

- $\mathbb{Z}[x]$ is een ontbindingsring dus $\mathbb{Z}[x][y] = \mathbb{Z}[x, y]$ ook een ontbindingsring
- Als k een lichaam is, dan is $k[x]$ een Euclidische ring, dus een ontbindingsring en dus ook $k[x][y] = k[x, y]$ dus ook $k[x, y][z] = k[x, y, z]$, enzovoort.

Voorbeeld

In $\mathbb{Q}[x, y] = \mathbb{Q}[y][x]$ is
$(y^2 + y)x^2 + (y^3 + y^2 + y + 1)x + (y^2 + y) =$
$(y + 1)(yx^2 + (y^2 + 1)x + y) = (y + 1)(x + \frac{1}{y})(xy + y^2)$. Deel $yx^2 + (y^2 + 1)x + y$ door $x + \frac{1}{y}$ in $\mathbb{Q}[y][x]$.
$= (y + 1)(yx + 1)(x + y)$ met $y + 1$ type (i), de rest van type (ii) met $ggd(coeff) = 1$ in $\mathbb{Q}[z]$ en $\deg_x(...) = 1$

Irreducibiliteits criteria

Definitie

Zij R een commutatieve ring, $f(x) \in R[x]$, dan heet $a \in R$ een **nulpunt** (Engels: zero point) of wortel van $f(x)$ als $f(x) = 0$.

Voorbeeld

in $\mathbb{Z}/8\mathbb{Z}[x]$ heeft $x^2 - 1$ de nulpunten $\overline{1}, \overline{3}, \overline{5}, \overline{7}$.

Stelling

Zij F een lichaam, $p(x)$ in $F[x]$, $\deg(p(x)) \geq 1$.
Dan heeft $p(x)$ een nulpunt in $F \Leftrightarrow p(x)$ heeft een lineaire factorizatie in $F[x]$.

Irreducibiliteits criteria

Bewijs

'$\Rightarrow$' stel $p(a) = 0$ voor $a \in F$. Schrijf $p(x) = q(x)(x - a) + r(x)$ met $\deg(r(x)) < 1 \Leftrightarrow r(x)$ is een constante c.
Vul $x = a$ in: $p(a) = q(a)(x - a) + c$ dus $c = 0$.
Dus $p(x) = q(x)(x - a)$.
'$\Leftarrow$' Als $p(x) = (\alpha x + \beta)g(x)$ met $\alpha, \beta \in F$ $\alpha \neq 0$, dan is $-\beta\alpha^{-1}$ een nulpunt van $p(x)$.

Irreducibiliteits criteria

Opmerking

Zij F een lichaam, x een variabele.

- Een polynoom van graad 1 is irreducibel in $F[x]$.
- Polynoom in $F[x]$ van graad 2 of 3 zijn irreducibel $\Leftrightarrow$ er is geen wortel in F.
- Polynoom van graad ≥ 4, als er een wortel is $\Rightarrow$ reducibel. Want $(x^2 + 1)$ in $R[x]$ geen wortels in R maar wel reducibel.

Irreducibiliteits criteria

Stelling

Zij R een ontbindingsring, met breuklichaam F.
Als $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ in $R[x]$ en $a_n, a_0 \neq 0$, $n \geq 1$ en $\frac{r}{s}$ in F een wortel van F met $ggd(r,s) = 1$, dana geldt $s|a_n$ en $r|a_0$ in R.
In het bijzonder als $a_n \in R^*$ dan is elke wortel in F in R en deelt a_0 in R.

Voorbeeld

Als $R = \mathbb{Z}$ dan is $F = \mathbb{Q}$.
$f(x) = x^3 - 2x - 4$.
Wortels van $f(x)$ in $\mathbb{Q}$ zijn in $\mathbb{Z}$ en delen -4 in $\mathbb{Z}$.
$\Rightarrow$ kandidaatwortels zijn $\pm 1, \pm 2, \pm 4$.
$f(2) = 0$, en $f(x) = (x-2)(x^2 + 2x + 2)$ kandidaat wortels $\pm 1, \pm 2$ geen voldoet $\Rightarrow$ $x^2 + 2x + 2$ is irreducibel in $\mathbb{Q}[x]$. $x - 2$ is irreducibel in $\mathbb{Q}[x]$, graad is 1.

Irreducibiliteits criteria

Voorbeeld

$R = \mathbb{Q}[x]$ $f(x,y) = y^3x^2 + (y^2+y)x + 1$ in $\mathbb{Q}[x,y]$.
Neem $\mathbb{Q}[x][y]$ of neem $\mathbb{Q}[y][x]$. $f(x,y) = x^2y^3 + xy^2 + xy + 1$, $n = 3$, $a_3 = x^2$, $a_0 = 1$.
Potentiele wortels: $\frac{r(x)}{s(x)}$. $ggd(r(x), s(x)) = 1$ in $\mathbb{Q}[x]$ en $r(x)|1$ en $s(x)|x^2$.
Delers van 1 in $\mathbb{Q}[x]$: $c \in \mathbb{Q}^*$. Delers van x^2 in $\mathbb{Q}[x]$:d, dx, dx^2 met $d \in \mathbb{Q}^*$.
Potentiele nulpunten zijn: $e, \frac{e}{x}, \frac{e}{x^2}$ met $e \in \mathbb{Q}^*$.
Bijvoorbeeld: $f(x, \frac{e}{x}) = \frac{e^3}{x} + \frac{e}{x^2} + e + 1 = 0 \Leftrightarrow \begin{cases} e^3 + e^2 = 0 \\ e + 1 = 0 \end{cases}$
$\Leftrightarrow e = -1$.
$\frac{-1}{x}$ is een nulpunt en
$f(x,y) = (y + \frac{1}{x})(x^2y^2 + x) = (xy+1)(xy^2+1)$ irreducibel in $\mathbb{Q}[x][y]$. Want graad $= 1$ en $ggd(x,1) = 1$.

Irreducibiliteits criteria

Stelling irreducibiliteitscriterium van Eisenheim

Zij P een *priem*ideaal van een domein R en $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ in $R[x]$ met $n \geq 1$. Als $a_{n-1}, a_{n-2}, \ldots, a_0 \in P$ en $a_0 \notin P^2$ dan is $f(x)$ irreducibel in $R[x]$.

Voorbeeld

$R = \mathbb{Z}$, $x^5 + 8x^2 + 6x + 2$ is irreducibel in $\mathbb{Z}[x]$ (Eisenheim met $P = (2)$).

Irreducibiliteits criteria

Voorbeeld

$R = \mathbb{Z}$, $P = (p)$, p een priemgetal.
$f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducibel in $\mathbb{Z}[x]$.
$f(x)$ is irreducibel, maar dan is $f(x+1)$ ook irreducibel.
Dit geeft $f(x) = \frac{x^p - 1}{x-1}$ dus
$f(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + \binom{p}{1}x^{p-2} + \cdots + \binom{p}{p-2}x + \binom{p}{p-1}$.
(Binomium van Newton).
Als p priem, dan is $\binom{p}{i} = \frac{p!}{(p-i)!i!}$ voor $i = 1, \ldots, p-1$ deelbaar door p.
Dus irreducibel in $\mathbb{Z}[x]$. Eisenstein met $p = (p)$.

Voorbeeld

$x^6 + x^5 + \cdots + x + 1$ irreducibel in $\mathbb{Z}[x]$.