Ringen en Lichamen

Luc Veldhuis

2 Oktober 2017

Stelling

Zij R een ring met $1 \neq 0$. Als $b(x) \in R[x]$, $b(x) \neq 0$, kopcöefficient van $b(x)$ in R^*. Als $a(x) \in R[x]$, dan bestaan er unieke $q(x)$, $r(x)$ in $R[x]$ met $\deg(r(x)) < \deg(b(x))$ en $a(x) = q(x)b(x) + r(x)$.

Bewijs existentie

Doe inductie naar $\deg(a(x))$. Als $\deg(a(x)) < \deg(b(x))$ dan $a(x) = 0b(x) + a(x)$. Als $\deg(a(x)) = n \geq \deg(b(x)) = m$, schrijf $a(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \neq 0$ en $b(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0$ met $b_m \in R^*$.
Dan is $\deg(\tilde{a}(x)) < \deg(a(x))$ voor $\tilde{a}(x) = a(x) - a_n b_m^{-1} x^{n-m} b(x)$.
Volgens de inductie bestaan $\tilde{q}(x)$, $\tilde{r}(x)$ met $\deg(\tilde{r}(x)) < \deg(\tilde{q}(x))$ en $\tilde{a}(x) = \tilde{q}(x)b(x) + \tilde{r}(x)$.

Bewijs uniciteit

Als $a(x) = q(x)b(x) + r(x) = q_1(x)b(x) + r_1(x)$ met $\deg(r(x))$, $\deg(r_1(x)) < \deg(b(x))$.
Dan $(q(x) - q_1(x))b(x) = r_1(x) - r(x)$.
$\deg((q(x) - q_1(x))b(x)) = \deg(q(x) - q_1(x)) + \deg(b(x)) = \deg(r(x) - r_1(x))$.
Maar $\deg(r(x) - r_1(x)) < \deg(b(x))$.
Dan volgt $q(x) = q_1(x)$, dus $r(x) = r_1(x)$.

Voorbeeld

In $\mathbb{F}_5[x]$. $x^5 + \overline{1} = (\overline{3}x^3 + x)(\overline{2}x^2 + \overline{1}) + (\overline{4}x + \overline{1})$.
Staart deling geeft $\overline{2}x^5 + \overline{1}/x^5 + \overline{1} \setminus \overline{3}x^3 + x$.

Vorige keer

Euclidische ring: een **domain** R met norm $N : R \setminus \{0\} \to \{1, 2, 3, \dots\}$ zodat voor $a, b \in R$ met $b \neq 0$ er $q, r \in R$ bestaan met $a = qb + r$ en of $r = 0$ of $r \neq 0$ en $N(r) < N(b)$.

Voorbeeld

- $\mathbb{Z}$ met $N(a) = |a|$
- $\mathbb{Z}[i]$ met $N(a + bi) = a^2 + b^2$
- $k[x]$, k een lichaam, met $N(f(x)) = \deg(f(x))$

Stelling

Elke ideaal in een Euclidische ring R is hoofd ideaal.
Als $I \neq (0)$ dan wordt I voortgebracht door elk element $x \neq 0$ in I met minimale norm.

Bewijs

Als $I = (0)$ dan is het duidelijk, dus stel $I \neq (0)$.
Neem $x \neq 0$ in I met $N(x) = \min\{N(y)|y \neq 0, y \in I\}$.
Dan is $x \in I$, dus $(x) \subseteq I$.
Voor de andere inclusie, neem $a \in I$. Schrijf $a = qx + r$ met $q, r \in R$ en $r = 0$ of $r \neq 0$ met $N(r) < N(x)$. Als $r \neq 0$, dan is $r = a - qx \in I$ maar dan $\min\{N(y)|y \neq 0, y \in I\} \leq N(r) < N(x)$.
Tegenspraak.
Conclusie: $r = 0$ en $a = qx \in (x)$, dus $I = (x)$.

Definitie

R commutatief, $a, b \in R$.

- b deelt a, $(b|a)$ betekend er is een $c \in R$ met $a = cb$.
- $d = ggd(a, b)$ als geldt dat:
  - $d|a$ en $d|b$
  - Als $e|a$ en $e|b$ dan ook $e|d$.

Voorbeeld

Als $1 \in R$:

- $b|a \Leftrightarrow a \in (b) \Leftrightarrow (a) \subseteq (b)$ want $a = cb$ en $(b) = \{cb|c \in R\}$
- $d|a$ en $d|b \Leftrightarrow (a, b) \subseteq (d)$
- $e|a$ en $e|b \Rightarrow e|d$ is $(a, b) \subseteq (e) \Rightarrow (d) \subseteq (e)$.

Opgave

Als d, d' allebei een *ggd* zijn van a en b, dan geldt $d|d'$ en $d'|d$ (en omgekeerd): als d en d' elkaar delen en d is een ggd, dan ook d'.

Opgave

In een domein R geldt $x|y$ en $y|x \Leftrightarrow$ er bestaat $u \in R^*$ met $y = ux \Leftrightarrow (x) = (y)$.

Voorbeeld

In $\mathbb{Z}[\sqrt{-5}]$ hebben $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ en $b = 2 + 2\sqrt{-5}$ geen ggd.
Stel $d = ggd(a, b)$, dus $d|a$ en $d|b$. Dan geldt $N(d)|N(a) = 36$ en $N(d)|N(a) = 24$.
$a = cd \Rightarrow N(a) = N(c)N(d) \Rightarrow N(d)|N(a) \Rightarrow N(d)|12$.
Merk op $2|a$ en $2|b$, dus $2|d$ en daarom $4 = N(2)|N(d)$.
$1+\sqrt{-5}|a$ en $1+\sqrt{-5}|b$, dus $1+\sqrt{-5}|d$ en
$6 = N(1+\sqrt{-5})|N(d) \Rightarrow 12|N(d)$.
$N(d) = \pm 12$, dus $N(d) = 12$.
Als $d = x + y\sqrt{-5}$ dan is dus $12 = x^2 + 5y^2$. Dat heeft geen oplossingen met $x, y \in \mathbb{Z}$, dus d bestaat niet.

Voorbeeld

In $\mathbb{Z}[\sqrt{-5}]$ hebben 2 en $1+\sqrt{-5}$ $ggd1$ maar $(2, 1+\sqrt{-5}) \neq (1)$. Stel $d|2$ en $d|1+\sqrt{-5} \Rightarrow N(d)|N(2) = 4$ en $N(d)|N(1+\sqrt{-5}) = 6$. Dus $N(d) = 1$ of $N(d) = 2$, komt niet voor als norm. Dus $d = \pm 1$. Dan is $ggd(2, 1+\sqrt{-5}) = 1$ (of -1) want 1 deelt alles.

Opgave

In $\mathbb{Z}[x]$ is $ggd(2, x) = 1$ maar $(2, x) \neq (1)$.

Stelling

Zij R een Euclidische ring. Dan:

- Elke 2 elementen a, b hebben een $ggd : (a, b) = (d)$ met $d = ggd(a, b)$.
- $d = xa + yb$ met $x, y \in R$ en d, a, b zijn te berekenen met behulp van het uitgebreide Euclidische algoritme: $(a, b) = (a - qb, b)$.

Voorbeeld

In $\mathbb{Q}[x]$ bereken $ggd(x^5+1, x^3+1) = x+1$.

Tabel : Uitwerking

	x_i	y_i	q_i	berekening
x^5+1	1	0		
x^3+1	0	1		
$-x^2+1$	1	$-x^2$	x^2	$x^5+1 = x^2(x^3+1) - x^2 + 1$
$x+1$	x	$1-x^3$	$-x$	$x^3+1 = (-x)(-x^2+1) + x + 1$
				$-x^2+1 = (-x+1)(x+1) + 0$

en $x+1 = x(x^5+1) + (1-x^3)(x^3+1)$

Voorbeeld

In $\mathbb{Z}[i]$ bereken $ggd(3+4i,5) = -2-i = 1(3+4i)+(-1-i)5$.
Dus $(3+4i,5) = (-2-i) = (2+i)$.

	x_j	y_j	q_j	berekening
$3+4i$	1	0		
5	0	1		
$-2-i$	1	$-1-i$	1+i	$3+4i$
				$5 = (-2+i)(-2+i)+0$

§8.2 Hoofdideaalringen

Definitie

Een hoofdideaalring (HIR) (Engels: Princiap Ideal Domain) is een domain zodat elk ideaal een hoofdideaal is.

Voorbeeld

Euclidische ringen ($\mathbb{Z}$, $\mathbb{Z}[i]$, $k[x]$ met k een lichaam).

Stelling

Zij R een HIR, $a, b \in R$, d een voortbrenger van (a, b), dan:

- $d = ggd(a, b)$
- Er bestaan $x, y \in R$ met $d = xa + yb$

Bewijs

- Algoritme: als $(a, b) = (d) \Rightarrow d$ is $ggd(a, b)$
- $(a, b) = \{xa + yb | x, y \in R\}$

§8.2 Hoofdideaalringen

Voorbeeld

$\mathbb{Z}[\frac{1+\sqrt{-19}}{2}] = \{a + b\frac{1+\sqrt{-19}}{2}\}$ met $a, b \in \mathbb{Z}$ deelring van $\mathbb{C}$ is een HIR maar geen Euclidische ring.