Ringen en Lichamen

Luc Veldhuis

13 November 2017

Vraag uit boek

Vraag 8.3.7a

Laat π een element in $\mathbb{Z}[i]$.
Voor $n \geq 0$ hebben we: $(\pi^{n+1}) = \pi^{n+1}\mathbb{Z}[i]$.
a) Bewijs $\mathbb{Z}[i]/(\pi) \cong (\pi^n)/(\pi^{n+1})$ door vermenigvuldiging met π^n.
$\phi : \mathbb{Z}[i] \to^{\pi^n} (\pi^n) \to (\pi^n)/(\pi^{n+1})$ door de quotient afbeelding voor optelgroepen.
ϕ is een homomorfisme van optelgroepen.
$\alpha \in ker(\pi) \Leftrightarrow \overline{\alpha\pi^n} = \overline{0}$ in $(\pi^n)/(\pi^{n+1})$
$\Leftrightarrow \alpha\pi^n \in (\pi^{n+1}) = \{\pi^{n+1}\beta | \beta \in \mathbb{Z}[i]\}$
$\Leftrightarrow \alpha = \pi\gamma$ voor een $\gamma \in \mathbb{Z}[i]$
$\Leftrightarrow \alpha \in (\pi)$.

Vraag uit boek

Vraag 8.3.7b

b) $|\mathbb{Z}[i]/(\pi^n)| = |\mathbb{Z}[i]/(\pi)|^n$.
Ooit een opdracht dat als $H_2 \subseteq H_1 \subseteq G$, dan geldt
$|G : H_2| = |G : H_1| \cdot |H_1 : H_2|$.
$\mathbb{Z}[i] \supseteq (\pi) \subseteq (\pi^2)$.
$|\mathbb{Z}[i]/(\pi^2)| = |\mathbb{Z}[i] : (\pi)| \cdot |(\pi) : (\pi^2)|$ met $|(\pi) : (\pi^2)| = |\mathbb{Z}[i]/(\pi)|$ vanwege (a).
Dus $|\mathbb{Z}[i]/(\pi^2)| = |\mathbb{Z}[i]/(\pi)|^2$.
Voor $2 \to n$ werkt dit nu voor alle n.

Vraag uit boek

Vraag 8.3.7c

c) Gebruik dat $|\mathbb{Z}[i]/(\pi^n)| = |\mathbb{Z}[i]/(\pi)|^n$.
En voor een willekeurig geval $\alpha = u\pi_1^{m_1}\pi_2^{m_2}\dots\pi_n^{m_n}$ alle π_i irreducibel, paarsgewijs geassocieerd en $u \in \mathbb{Z}[i]^*$.
Als $\beta = \pi_1^{m_1}\dots\pi_n^{m_n}$ dan is $N(\beta) = N(\alpha)$, en dus $(\alpha) = (\beta)$.
Als laatste de Chineese Rest Stelling:
$\mathbb{Z}[i]/(\beta) \cong \mathbb{Z}[i]/(\pi_1^{m_1}) \times \cdots \times \mathbb{Z}[i]/(\pi_n^{m_n}) \Rightarrow$
$|\mathbb{Z}[i]/(\beta)| = |\mathbb{Z}[i]/(\pi_1^{m_1})| \cdot \dots \cdot |\mathbb{Z}[i]/(\pi_n^{m_n})|$ en
$|\mathbb{Z}[i]/(\beta)| = N(\pi_1^{m_1}) \cdot \dots \cdot N(\pi_n^{m_n}) = N(\beta)$.

Hoofdstelling veeltermringen

Stelling

Als R een domein is, dan:

- $\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x))$ voor $p(x)$, $q(x)$ in $R[x]$.
- $R[x]^* = R$
- $R[x]$ is een domein

Stelling

R een ring, commutatief met $1 \neq 0$, $I \subseteq R$ een ideaal van R, dan is $I[x]$ een ideaal van $R[x]$ $(= (I)_{R[x]})$ en $R[x]/I[x] \cong R/I\ [x]$.
In het bijzonder is I een priem ideaal van $R \Leftrightarrow I[x]$ is een priemideaal van $R[x]$.

Hoofdstelling veeltermringen

Bewijs

Als $\phi : R \to S$ een homomorfisme is, dan is $R[x] \to S[x]$ met $f(x) \mapsto f^{\phi}(x)$, pas ϕ toe op de coefficienten van f. Dit is een ring homomorfisme (ga na).
Pas dit toe op $\phi : R \to R/I$, een surjectief ringhomomorfisme.
Je krijgt $\varphi : R[x] \to R/I[x]$ met $f(x) \mapsto \overline{f}(x)$, reduceer de coefficienten van f modulo I.
φ is surjectief.
$f(x) \in \ker(\varphi) \Leftrightarrow$ modulo I zijn alle coefficienten 0
$\Leftrightarrow$ alle coefficienten zijn in I
$\Leftrightarrow f(x) \in I[x] = \{a_0 + a_1 x + \cdots \in R[x], a_i \in I\}$.
Uit de 1e isomorfie stelling volgt nu dat $R[x]/I[x] \cong R/I\ [x]$.
$(I)_{R[x]} = I[x]$ (Opgave)

Hoofdstelling veeltermringen

Voorbeeld

$R = \mathbb{Z}$, $I = (p)$ dan is $\mathbb{Z}[x]/(p) \cong \mathbb{Z}/p\mathbb{Z}[x]$

Stelling

I is een priemideaal van R
$\Leftrightarrow$ R/I is een domein
$\Leftrightarrow$ $R/I[x]$ is een domein
$\Leftrightarrow$ $R[x]/I[x]$ is een domein (want $R[x]/I[x] \cong R/I[x] \Leftrightarrow I[x]$ is een priemideaal van $R[x]$.

Herhaling

Als k een lichaam is dan is $k[x]$ een Euclidische ring, dus een Hoofd Ideaal Ring, dus een ontbindings ring.
In $k[x]$ is een ideaal of (0) of $(f(x))$ met $f(x) \neq 0$ in $k[x]$.
$f(x)$ is uniek op vermenigvuldiging met $k[x]^* = k^*$ na.
Kies in het algemeen de unieke monische (kop coefficient 1) voortbrenger.
Ook $(f(x))$ met $f(x) \neq 0$ is een priem ideaal
$\Leftrightarrow$ $f(x)$ is priem element
$\Leftrightarrow$ $f(x)$ is irreducibel ($f(x)$ in HIR)
Ook in een HIR is elk priem ideaal $\neq 0$ een maximaal ideaal.
Dus $k[x]/(f(x))$ is een lichaam als $f(x)$ irreducibel is.

Voorbeeld

- In $\mathbb{R}[x]$ is X^2+1 irreducibel (dus $R[x]/(X^2+1)$ is een lichaam). Maar in $\mathbb{C}[x]$ is $X^2+1=(X-i)(X+i)$ reducibel
- In $\mathcal{F}_2[x]$ geldt
  $X^4+X^3+X+\overline{1}=(X-\overline{1})(X^3+\overline{1})=(X+\overline{1})^2(X^2+X+1)$
  met $(X+\overline{1})$ en (X^2+X+1) irreducibel.
  Dus $F_2[x]/(X^2+X+\overline{1})$ is een lichaam met 4 elementen.

§9.3 Polynoomringen die ontbindingsringen zijn

Stelling

Als R een ontbindingsring is dan is $R[x]$ dat ook.

Idee

Gebruik $F = Frac(R)$ en $R[x] \subseteq F[x]$ (een eenvoudige ring) en 'vergelijk' $R[x]$ en $F[x]$.

Voorbereiding

Gaußlemma: Zij R een ontbindingsring, F het brekenlichaam van F, zij $p(x) \in R[x] (\subseteq F[x])$.
Als $p(x)$ reducibel is in $F[x]$ dan is $p(x)$ reducibel in $R[x]$.
Preciezer: als $p(x) = A(x)B(x)$ in $F(x)$
$(\deg(A(x)), \deg(B(x)) \geq 1$, dan bestaan a, b in F^* met $ab = 1$ en $aA(x), bB(x) \in R[x]$
$\Rightarrow p(x) = (aA(x))(bB(x))$ in $R[x]$

§9.3 Polynoomringen die ontbindingsringen zijn

Voorbeeld

$6x^2 + 7x + 2 \in \mathbb{Q}[x] = (x + \frac{1}{2})(6x + 4) \in \mathbb{Q}[x] = (2x + 2)(3x + 2)$

Bewijs

Er zijn a, b in $R \setminus \{0\}$ met $a_1A(x), b_1B(x)$ in $R[x]$ met $d_1 = a_1b_1$, geldt $d_1p(x) = (a_1A(x))(b_1B(x)) \in R[x]$.
Als $d_1 \in R^*$ dan is $p(x) = (d_1^{-1}a_1A(x))(b_1B(x)) \in R[x]$.
Als $d_1 \notin R^*$, schrijf $d_1 = \pi_1\pi_2 \dots \pi_n$ met π_i irreducieerbaar in R.
Reduceer $d_1p(x) = (a_1A(x))(b_1B(x))$ modulo (π_1) (dat wil zeggen, gebruik $R[x] \to R/(\pi_1)[x]$.
$\Rightarrow \overline{0}\overline{p}(x) = \overline{a_1A(x)b_1B(x)} \in R/(\pi_1)[x]$.
π_1 irreducibel $\Rightarrow \pi_1$ is priem in een ontbindings ring.
$\Rightarrow (\pi_1)$ priemideaal van R
$\Rightarrow R/(\pi_1)$ is een domein
$\Rightarrow R/(\pi_1)[x]$ is een domein.

Bewijs (vervolg)

Dus $\overline{a_1 A(x)} = \overline{0}$ of $\overline{b_1 B(x)} = \overline{0}$.
Als $\overline{a_1 A(x)} = \overline{0}$ dan is $a_1 A(x) = \pi_1 a_2 A(x)$ met $a_2 A(x) \in R[x]$.
Nog steeds geldt dat $a_2 b_2 = d_2$.
$\Rightarrow d_2 p(x) = (a_2 A(x))(b_2 B(x))$ met $a_1 = \pi_1 a_2$ en $b_1 = b_2$ met $d_1 = \pi_1 d_2$. Nu geldt $d_2 = \pi_2 \pi_3 \dots \pi_n$.
Idem als $\overline{b_1 B(x)} = \overline{0}$, dan geldt $a_1 = a_2$ en $b_1 = \pi_1 b_2$.
Herhaal dit totdat $d_{n+1} = 1$,
$d_{n+1} p(x) = (a_{n+1} A(x))(b_{n+1} B(x)) \in R[x]$.
Dan zien we $a_{n+1} b_{n+1} = d_{n+1} = 1$.

§9.3 Polynoomringen die ontbindingsringen zijn

Gevolg

Zij R een ontbindingsring, $F = Frac(R)$, $p(x) \in R[x]$ met $ggd(coefficientp(x)) = 1$.
Dan os $p(x)$ reducibel in $R[x] \Leftrightarrow p(x)$ is reducibel in $F[x]$.

Voorbeeld

$R = \mathbb{Z}$, $F = \mathbb{Q}$, $p(x) = 6x + 4$ $ggd(coeff) = 2$, $p(x) = 2(3x + 1)$ reducibel in $\mathbb{Z}[x]$.
$p(x)$ is irreducibel in $\mathbb{Q}[x]$ want het is graad 1 en $\mathbb{Q}$ is een lichaam.

Bewijs

Zie boek (gebruikt Gaußlemma)

§9.3 Polynoomringen die ontbindingsringen zijn

Opmerking

Volgens het gevolg geldt ook: als $p(x)$ in $R[x]$ en $ggd(coeff) = 1$ dan geldt $p(x)$ irreducibel in $R[x] \Leftrightarrow p(x)$ irreducibel in $F[x]$.

Conclusie

In $R[x]$ zijn de volgende elementen irreducibel:

- $\pi \in R$ met π irreducibel in R
- $p(x)$ in $R[x]$ met $ggd(coeff) = 1$ en $p(x)$ irreducibel in $F[x]$.

Voorbeeld

$3x^2 + 7 \in \mathbb{Z}[x]$, $ggd(coeff) = 1$, $3x^2 + 7 \in \mathbb{Q}[x]$ graad 2, geen wortel in $\mathbb{Q}$.