Ringen en Lichamen

Luc Veldhuis

30 Oktober 2017

Herhaling

Vorige keer

In een HIR (Hoofd ideaal ring) geldt 'priem element' en 'irreducibel element' zijn hetzelfde .

Definitie

Een ontbindingsring is een domein R zodat elke $x \in R$ $x \neq 0$, $x \in R^*$ geschreven kan worden als $x = p_1 p_2 \dots p_s$ met alle p_i irreducibel en als ook $x = q_1 q_2 \dots q_t$ met alle q_j irreducibel, dan geldt $s = t$ en, na eventueel hernummeren van de q_j geldt p_i en q_i zijn geassocieerd $\Leftrightarrow$ $q_i = u_i p_i$ met $u_i \in R^*$.

Hoofd ideaal ringen

Stelling

Een hoofdideaalring (in het bijzonder een Euclidische ring) is een ontbindingsring.

Bewijs

- Existentie van een factorisatie
  Als $y \neq 0$, $y \notin R^*$, zeg 'y is ' als y het product is van eindig veel irreducibele elementen.
  Te bewijzen: als $x \neq 0$, $x \notin R^*$, dan is x ok.
  Stel van niet: voor $x \neq 0$, $x \notin R^*$ dan is x niet irreducibel $\Rightarrow$ $x = x_1 y_1$ met $x_1, y_1 \neq 0$, $x_1, y_1 \notin R^*$ en x of y *niet* ok.
  We mogen aannemen dat x_1 is niet ok.
  Herhaal dit voor x_1 ipv x, $x_1 = x_2 y_2$ met $x_2, y_2 \neq 0$ en $x_2, y_2 \notin R^*$ en x_2 niet ok.

Hoofd ideaal ringen

Bewijs (vervolg)

Ga zo door voor $x_n = x_{n+1}y_{n+1}$ met $x_{n+1}, y_{n+1} \neq 0$ en $x_{n+1}, y_{n+1} \notin R^*$ en x_{n+1} niet ok. Dan krijg je $(x) \subsetneq (x_1) \subsetneq (x_2) \subsetneq \ldots$, want $(a) = (b) \Leftrightarrow b = ua$ met u een eenheid, maar $x = x_1y_1$ met $y_1 \notin R^*$.
Schrijf $I_j = (x_j)$.
Dus $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \ldots$.
Dan is $I = \bigcup_{j=1}^{\infty} I_j$ een ideaal. (Ga na)
Dus (R is HIR), $I = (z)$ voor een z in I.
Dan is $z \in I_k$ voor een $k \geq 1$.
Nu geldt $I_k \subseteq I$ en $I = (z) \subseteq I_k$, dus $I = I_k$, maar $I_{k+1} \subseteq I = I_k$.
Tegenspraak. $I_k \subsetneq I_{k+1}$.

Hoofd ideaal ringen

Bewijs

- Uniciteit.
  Stel $x \neq 0$, $x \notin R^*$ heeft 2 factorizaties.
  $x = p_1 p_2, \ldots p_s = q_1 q_2 \ldots q_t$ met alle p_i, q_j irreducibel.
  Doe inductie naar de minimale s met $x = p_1 p_2 \ldots p_s$ alle p_i irreducibel.
  $s = 1$: dan is x irreducibel. Als $x = q_1 q_2 \ldots q_t$ met $t \geq 2$ en alle q_j irreducibel.
  x irreducibel $\Rightarrow$ q_1 is een eenheid (kan niet, irreducibel) of $q_2 q_3 \ldots q_t$ is een eenheid $\Rightarrow$ dan is elk element een eenheid, kan niet, ze zijn irreducibel.
  Tegenspraak, dus $t = 1$.
  $x = p_1 = q_1$.
  Neem nu aan: als x een factorizatie heeft in $\leq s - 1$ factoren, dan is die essentieel uniek.

Hoofd ideaal ringen

Bewijs (vervolg)

Schrijf $x = p_1 p_2 \dots p_s = q_1 q_2 \dots q_t$ met alle p_i, q_j irreducibel.
Dan geldt $p_1 | q_1 \dots q_t$. In een HIR is p_i een priemelement.
Dus $p_1 | ab$ dan $p_1 | a$ of $p_1 | b$.
$p_1 | q_j$ voor een j dus $q_j = z p_1$ voor een $z \in R$, q_j irreducibel, p_1 geen eenheid $\Rightarrow$ z is een eenheid.
Hernummeren $q_1 \dots q_t$ zodat nu $q_1 = u p_1$ met $u \in R^*$.
Dus $x = p_1 \dots p_s = q_1 \dots q_t = p_1 (u q_2) q_3 \dots q_t$
$\Rightarrow p_2 \dots p_s = (u q_2) q_3 \dots q_t = q_2' q_3' \dots q_t'$ irreducibel.
Inductie hypothese: $s - 1 = t - 1 \Rightarrow s = t$ en na hernummeren van de q_j' voor $j = 2, \dots, s$ geldt p_i en q_i' zijn geassoccieerd voor $i = 2, \dots, s$ en ook q_2' is geassocieerd met q_2 voor hernummeren.

Hoofd ideaal ringen

Voorbeeld

$\mathbb{Z}[i]$, $\mathbb{Z}$, $k[x]$ met een lichaam zijn Euclidische ringen, dus HIR, dus ontbindingsringen.
In $\mathbb{Z}$ $6 = 2 \cdot 3 = 3 \cdot 2 = (-2)(-3) = (-3)(-2)$ de mogelijke factorizaties in $\mathbb{Z}$.

Stelling

In een ontbindingsring vallen de begrippen 'irreducibel' en 'priemelementen' samen.

Bewijs

Als gezien: In een domein is elk priem element irreducibel.
Nu te bewijzen: in een ontbindingsring is een irreducibel element priem. Stel x is irreducibel, dus $x \neq 0$, $x \notin R^*$.
Nog te zien: als $x|ab$ dan $x|a$ of $x|b$.
$x|ab$ betekend $ab = x$ voor een $c \in R$.

Hoofd ideaal ringen

Bewijs (vervolg)

Als $ab = 0 \Leftrightarrow a = 0$ of $b = 0$, dan geldt $x|a$ of $x|b$ want $x|0$.
Neem nu aan: $a, b \neq 0$. Als $a^* \in R^*$ dan $ab = xc$ dus $b = xca^{-1}$ en $x|b$.
Idem: als $b \in R^*$ dan $x|a$.
Neem nu ook aan $a, b \notin R^*$.
Schrijf $a = p_1 \dots p_s$, $b = q_1 \dots q_t$ alle p_i irreducibel.
Als $c \notin R^*$, $c = r_1 \dots r_k$ alle r_i irreducibel, dan zijn $p_1 \dots p_s q_1 \dots q_t = xr_1 \dots r_k$ twee factoriaties in irreducibele elementen, maar R is een ontbindingsring
$\Rightarrow x$ is geassocieerd met een p_i of een q_j
$\Rightarrow x|a$ of $x|b$, want $p_i|a$ of $q_j|b$.
Als $c \in R^*$ doe die zelf.

Hoofd ideaal ringen

Opmerking

- In $\mathbb{Z}$ heet een positief irreducibel element een priem**getal**
- In $\mathbb{Z}[i]$ of $k[x]$ met k een lichaam spreek je meestal over irreducibele elementen (ookal zijn dat priemelementen).

Opmerking

Als $a, b \neq 0$ in een ontbindingsring R dan schrijf je
$a = up_1^{m_1} \dots p_s^{m_s}$, $b = vq_1^{n_1} \dots q_t^{n_t}$ met $u, v \in R^*$ met $p_1, \dots, p_s$ irreducibel paarsgewijs niet geassocieerd.
$a \in \mathbb{R}^* \Leftrightarrow m_1 = \dots = m_s = 0$.
$a \notin R^*$ $a = q_1 q_2 \dots q_t = u_1 p_{f(1)} u_2 p_{f(2)} \dots u_s p_{f(s)}$ met q_j irreducibel.
Kies uit elke associatie klasse van irreducibele elementen 1 representant.

Hoofd ideaal ringen

Voorbeeld

In $\mathbb{Z}[i]$ geldt $4 = (1+i)(1-i)(1+i)(1-i)$, en $1-i = -i(1+i)$.
Dus $4 = (-i)^2(1+i)^4$.
Dan is $p_1^{\min(m_1,n_1)} p_2^{\min(m_2,n_2)} \dots p_s^{\min(m_s,n_s)}$ een *ggd* van a en b. Dus $ggd(a,b)$ bestaat altijd. $(ggd(a,a) = a)$.

Voorbeeld

In $k[x]$ met k een lichaam hebben we $k[x]* = k^*$.
Normaliseer je $f(x) \neq 0$ door kopcoëfficiënt 1 te eisen (dat wil zeggen $f(x)$ is monisch).
Bijvoorbeeld $3X^6 - 3 = 3(X^6-1) = 3(X^3-1)(X^3+1) = 3(X^2+X+1)(X-1)(X^2-X+1)(X+1)$ in factoren.
$X^4 - 1 = (X^2-1)(X^2+1) = (X-1)(X+1)(X^2+1)$ irreducibel:
$\Rightarrow$ de (monische) ggd van $3X^6-3$ en X^4-1 is
$(X-1)(X+1) = X^2-1$.

Hoofd ideaal ringen

Voorbeeld

Wat zijn de irreducibele elementen in $\mathbb{Z}[i]$?
Stel $\pi \in \mathbb{Z}[i]$ is irreducibel, dus $\mathbb{Z}[i]/(\pi)$ is een domein.
Dan is $(\pi) \cap \mathbb{Z}$ is een priemideaal $\neq 0$: $\mathbb{Z} \to \mathbb{Z}[i]/(\pi)$ natuurlijke afbeelding, een ring homomorfisme met kern $\mathbb{Z} \cap (\pi)$.
Dan volgt nu uit de eerste isomorfie stelling $\Rightarrow \mathbb{Z}/(\mathbb{Z} \cap (\pi)) \cong$ beeld, een domein.
$\mathbb{Z} \cap (\pi)$ is een priemideaal van $\mathbb{Z}$, ($\neq 0$ want $\pi \cdot \overline{\pi}$ is er in.)

Voorbeeld (vervolg)

Dus als $\mathbb{Z} \cap (\pi) = (p)$ met p priemgetal in $\mathbb{Z}$ dan is $p \in (\pi)$, dus $\pi | p$ in $\mathbb{Z}[i]$.
Conclusie: we vinden alle irreducibele elementen in $\mathbb{Z}[i]$ door alle priemgetallen p te factorizeren in $\mathbb{Z}[i]$.
Stel p is een priemgetal en $p = \pi_1 \pi_2 \dots \pi_s$ is een element in $\mathbb{Z}[i]$.
$p^2 = N_m$ en $(p) = N_m(\pi_1) N_m(\pi_2) \dots N_m(\pi_s)$ met $N_m(\pi_i) \neq 1$.
Dus $s = 1$ of $s = 2$.
Je vindt:

- $p = 2$, $2 = (1+i)(1-i)$ allebei irreducibel.
- $p \equiv 1 \mod 4$: $p = \pi\overline{\pi}$ met π, $\overline{\pi}$ irreducibel met norm p.
  Voorbeeld $13 = (2+3i)(2-3i)$
- $p \equiv 3 \mod 4$: die zijn irreducibel in $\mathbb{Z}[i]$.
  Voorbeeld $p = 3, 7, 11, 19$.