Ringen en Lichamen

Luc Veldhuis

2 Oktober 2017

§7.6 De Chinese rest stelling (voor ringen)

Definitie

Idealen I en J van een ring R heten **relatief priem** als $I + J = R$.

Voorbeeld

Als $R = \mathbb{Z}$, $I = (m)$, $J = (n)$, dan is $I + J = (m, n) = (ggd(m, n))$ en dat is $\mathbb{Z} \Leftrightarrow ggd(m, n) = 1$.

Stelling (Chinese rest stelling)

Zij R een commutatieve ring met $1 \neq 0$ en idealen $I_1, I_2, \ldots, I_l$ voor $l \geq 2$ idealen van R.
De afbeelding $R \to R/I_1 \times R/I_2 \times R/I_2 \times \cdots \times R/I_l$ met $x \mapsto (x + I_1, x + I_2, \ldots, x + I_l)$ is een ringhomomorfisme met ker $= I_1 \cap I_2 \cap \cdots \cap I_l$.
Als elk paar I_i, I_j met $i \neq j$ relatief priem is, dan is de afbeelding surjectief en de kern is $I_1 \cdot I_2 \ldots I_3$.

§7.6 De Chinese rest stelling (voor ringen)

Gevolg

Je krijgt een afbeelding $R/(I_1 \cap \cdots \cap I_l) \to R/I_1 \times R/i_2 \times \cdots \times R/I_l$ en ook $R/(I_1 \cap \cdots \cap I_l)^* \to (R/I_1)^* \times (R/I_2)^* \times \cdots \times (R/I_l)^* = (R/I_1 \times R/i_2 \times \cdots \times R/I_l)^*$.
Als $(a_1, \ldots, a_l) \cdot (b_1, \ldots, b_l) = (a_1 b_1, \ldots, a_l b_l) = (1, \ldots, 1)$.
Als de I_i, I_j voor $i \neq j$ altijd relatief priem zijn, dan geeft dit een isomorfisme $R/(I_1 \cdot I_2 \cdot \cdots \cdot I_l) \cong R/I_1 \times R/I_2 \times \cdots \times R/I_l$ van ringen en ook een isomorfisme
$(R/(I_1 \cdot I_2 \cdot \cdots \cdot I_l))^* \cong (R/I_1)^* \times (R/I_2)^* \times \cdots \times (R/I_l)^*$ van groepen.

§7.6 De Chinese rest stelling (voor ringen)

Voorbeeld

(Al gezien) Als $m, n \in \mathbb{Z}$, $R = \mathbb{Z}$ met $ggd(m, n) = 1$, dan is $(m) \cap (n) = (mn)$, dan is:
$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ met $a \mod mn \mapsto (a \mod m, a \mod n)$ en
$(\mathbb{Z}/mn\mathbb{Z})^* \cong (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$ als groepen.
Gezien: op deze manier bereken je
$\phi(p_1^{a_1} \dots p_t^{a_t}) = (p_1 - 1)p^{a_1 - 1} \dots (p_t - 1)p^{a_t - 1}$ als
$p_1 < p_2 < \cdots < p_t$ priemgetallen en alle $a_i \geq 1$.

Bewijs van de stelling voor $l = 2$

I, J idealen van R met $I + J = R$.

- $R \to R/I \times R/J$ is een ringhomomorfisme voor $x \mapsto (x + I, x + J)$ (ga na).
- ker : $x \in ker \Leftrightarrow \begin{cases} x + I = 0 + I \in R/I \\ x + J = 0 + J \in R?J \end{cases} \Leftrightarrow \begin{cases} x \in I \\ x \in J \end{cases} \Leftrightarrow$ $x \in I \cap J$

Neem vanaf nu aan $I + J = R$. Schrijf $1 = i + j$ met $i \in I$ en $j \in J$. Als $(a + I, a + J) \in R/I \times R/J$ dan beeldt $aj + bi$ af op $(aj + bi + I, aj + bi + J) = (aj + I, bi + I) =$ $(aj + ai + I, bi + bj + J) = (a + I, b + I)$.
Dus de afbeelding is surjectief en $R/(I \cap J) \cong R/I \times R/J$ (1e isomorfie stelling).

§7.6 De Chinese rest stelling (voor ringen) (vervolg)

Bewijs van stelling voor $l = 2$

Nog te bewijzen: als $I + J = R$, dan is $I \cap J = IJ$. Al gezien: $IJ \subseteq I \cap J$. In te zien: $I \cap J \subseteq IJ$.
Neem $x \in I \cap J$, dan is $x = x1 = xi + xj = ix + xj$. Want $x, i \in I$, $x, j \in J$, dus $xi = ix \in I$ en $xj \in J$, dus $ix, xj \in IJ$, gesloten onder optelling dus $x = ix + xj \in IJ$ voor alle $x \in I \cap J$.
Dus $I \cap J = IJ$.
Dus $R/IJ \cong R/I \times R/J$.

Ezelsbruggetje

$a = a1 = a(i + j) = ai + \mathbf{aj}$
$b = b1 = b(i + j) = \mathbf{bi} + bj$.

Voorbeeld

$R = \mathbb{Z}[i]$, gehelen van Gauß(commutatief met $1 \neq 0$) $I = (2+i)$, $J = (4-i)$.
$I + J = R \Leftrightarrow 1 \in I + J$.
$1 = -10 \cdot 5 + 3 \cdot 17 = -50 + 51$ met $5 = (2+i)(2-i) \in I$ en $17 = (4-i)(4+i) \in J$ met $-50 \in I$ en $51 \in J$.
$\alpha = -50\alpha + \mathbf{51}\alpha$, $\beta = -\mathbf{50}\beta + 51\beta$ Dan beeldt $\alpha, \beta \in \mathbb{Z}[i]$ af op $(\alpha + I, \beta + I)$ in $(R/I, R/J)$.
De Chinese reststelling geeft
$I \cap J = IJ = ((2+i)(4-i)) = (9+2i)$.
Conclusie:
$\mathbb{Z}[i]/(9+2i) \cong \mathbb{Z}[i]/(2+i) \times \mathbb{Z}[i]/(4-i) \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z} \cong \mathbb{Z}/85\mathbb{Z}$.

Voorbeeld

$R = \mathbb{Z}[i]$, $I = (2-i)$, $J = (2+i)$, dan is $I + J = R$ en
$I \cap J = IJ = (5) = 5\mathbb{Z}[i]$.
En $\mathbb{Z}[i]/(5) \cong \mathbb{Z}[i]/(2-i) \times \mathbb{Z}[i]/(2+i) \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

§7.6 De Chinese rest stelling (voor ringen)

Voorbeeld met $l = 3$

$R = \mathbb{Z}$, $I_1 = (3)$, $I_2 = (4)$, $I_3 = (5)$.
$1 = (-1)3 + 1 \cdot 4 = 2 \cdot 3 + (-1) \cdot 5$.
$1 = 1 \cdot 4 + (-1) \cdot 3 = (-1)4 + 1 \cdot 5$.
$1 = (-1)5 + 2 \cdot 3 = 1 \cdot 5 + (-1)4$
Met $(-1)3, 1 \cdot 3 \in I_1$, $1 \cdot 4, (-1)4 \in I_2$, $(-1) \cdot 5, 1 \cdot 5 \in I_3$.
Dus $I_1 + I_2 = I_1 + I_3 = I_2 + I_3 = \mathbb{Z}$ dus
$I_1 \cap I_2 \cap I_3 = I_1 \cdot I_2 \cdot I_3 = (3 \cdot 4 \cdot 5) = (60)$.
Welke klasse in $\mathbb{Z}/60$ beeldt af op $(a + 3\mathbb{Z}, b + 4\mathbb{Z}, c + 5\mathbb{Z})$ in
$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ (*)?
Neem $1 \cdot 4 \cdot (-1) \cdot 5 = -20 \in I_2 \cap I_3$ en
$1 = ((-1)3 + 1 \cdot 4)(2 \cdot 3 + (-1)5) = -20 \mod I_1$ (want
$(-1)3, 2 \cdot 3 \in I_1$.
Dan beelt $-20a + I_1 I_2 I_3$ af op $(a + I_1, a + I_2, a + I_3)$, want $-20 \equiv 1$
mod I_i dus $-20a \equiv a \mod I_1$.

Opgave

Wat beeldt af op (*)?

Typen ringen

Idee: $\mathbb{Z}$ heeft diverse eigenschappen:

- Elk ideaal is hoofdideaal
- Unieke ontbinding in priemgetallen
- Deling met rest

We gaan doen: $\{$lichamen$\} \subsetneq \{$Euclidische ringen$\} \subsetneq \{$hoofdideaal ringen$\} \subseteq \{$ontbindings ringen$\} \subseteq \{$domeinen$\}$

§8.1 Diverse typen ringen

Definitie

Een **norm** op een domein R is een afbeelding $N : R/\{0\} \to \{0, 1, 2, \dots\}$ zodat voor elke $a, b \in R$ met $b \neq 0$ er q en r in R bestaan met $a = qn + r$ met of $r = 0$ of $r \neq 0$ en $N(r) < N(b)$.

Definitie

Een Euclidische ring is een domein R zodat er een norm $N : R/\{0\} \to \{0, 1, 2, \dots\}$ bestaat zodanig dat als $a, b \in R$ met $b \neq 0$ dan zijn er $q, r \in R$ met $a = qb + r$ met $r = 0$ of $r \neq 0$ en $N(r) < N(b)$.

Voorbeeld

- $R = \mathbb{Z}$. $N(x) = |x|$.
  $a = q \cdot b + r$ met $r \in \{0, 1, 2, \ldots, |b| - 1\}$
- k een lichaam, N willekeurig, want $a = ab^{-1}b + 0$, als $b \neq 0$.
- $R = \mathbb{Z}[i]$ met $N(a + bi) = a^2 + b^2$ met $a, b \in \mathbb{Z}$. Neem $\alpha, \beta \in \mathbb{Z}[i]$ met $\beta \neq 0 \Rightarrow \frac{\alpha}{\beta} = a + bi$ met $a, b \in \mathbb{Q}$. Neem $A, B \in \mathbb{Z}$ met $|A - a| \leq \frac{1}{2}$, $|B - b| \leq \frac{1}{2}$.
  Schrijf $\alpha = (A + Bi)\beta + r$ met $r = \alpha - (A + Bi)\beta \in \mathbb{Z}[i]$. Ook $r = \alpha - (A + Bi)\beta = (a + bi)\beta - (A + Bi)\beta =$
  $((a - A) + (b - B)i)\beta \in \mathbb{Q}[i]$.
  N op $(\mathbb{Q}(i))^*$ is multiplicatief: $N(\gamma\delta) = N(\gamma)N(\delta)$.
  $N(r) = N(((a-A)+(b-B)i)\beta) = N((a-A)+(b-B)i)N(\beta) =$
  $((a - A)^2 + (b - B)^2)N(\beta) \leq \frac{1}{2}N(\beta) < N(\beta)$. Ook als $r = 0$.
  Gebruik $\beta \neq 0$.

§8.1 Diverse typen ringen

Voorbeeld

$\alpha = 4 - i$, $\beta = 2 + i$.
$\frac{4-i}{2+i} = \frac{7}{5} - \frac{6}{5}i$. $A = 1$, $B = -1$ dus $q = 1 - i$ en $r = \alpha - qB = 1$.
Dus $\alpha = (1 - i)\beta + 1$