# Ringen en Lichamen

Luc Veldhuis

30 Oktober 2017

# Examen bespreking

## Vraag

$I = (2, 1 + \sqrt{-3}) \subseteq R = \mathbb{Z}[\sqrt{-3}]$.
$II = I^2 = (2)I$
Namelijk
$II = (2, 1+\sqrt{-3})(2, 1+\sqrt{-3}) = (2^2, 2(1+\sqrt{-3}), (1+\sqrt{-3})2, (1+\sqrt{-3})^2) = (4, 2+2\sqrt{-3}, -2+2\sqrt{3}) = (4, 2+2\sqrt{-3}) = (2)I$
$\text{`}\supseteq\text{'}\ 4, 2+2\sqrt{-3} \in (4, 2+2\sqrt{-3}-2+\sqrt{-3})\ \text{`}\subseteq\text{'}$
$4, 2+2\sqrt{-3}, -2+2\sqrt{-3} \in (4, 2+2\sqrt{-3})$, want
$(-1)4 + 1(2+2\sqrt{-3})$.

## Herhaling

Al gezien in §8.2: een HIR (Hoofd ideaal ring) is een domein $R$ zodat elk ideaal een hoofdideaal is. Voorbeeld: Euclidische ringen, $ggd(a, b)$ bestaat voor alle $a, b \in R$ (namelijk als $(a, b) = (d)$)
Formule van Bèzout: $ax + by = d$ met $x, y \in R$.

## Stelling

Elk priemideaal $\neq (0)$ in HIR is een maximaal ideaal

## Bewijs

Stel $(p) \neq (0)$ is een priemideaal, dus $p \neq 0$, $p \neq R^*$, want $(p) \neq R$.
Stel $I$ is een ideaal van $R$ met $(p) \subseteq I \subseteq R$.
Te bewijzen: $I = (p)$ of $I = R$.
Schrijf $I = (m)$ dus $(p) \subseteq (m)$, derhalve $p = am$ met $a \in R$.
$(p)$ is een priemideaal, $am \in (p)$, dus $a \in (p)$ of $m \in (p)$.
Als $m \in (p)$, dan $(m) \subseteq (p)$ en $(m) = (p)$.
Als $a \in (p)$ dan is $a = bp$ voor een $b \in R$ en dus $p = am - bmp$
$p \neq 0 \Rightarrow 1 = bm$. Dus $m \in R^*$ en $(m) = R$.

## Gevolg

Als $R$ een commutatieve ring is en $R[x]$ een HIR, dan is $R$ een lichaam.

## Bewijs

$R[X]$ is een HIR $\Rightarrow$ $R[X]$ is een domein $\Rightarrow$ $R$ is een domein.
Dan is $(x)$ een priemideaal van $R[X]$, want $R[X]/[X] \cong R$ is een domein.
Dus $(x)$ is een priemideaal $\neq (0)$ in de HIR $R[X]$ dus (vorige stelling) $(x)$ is maximaal ideaal, en $R \cong R[X]/[X]$ is een lichaam.

## Voorbeeld

- $\mathbb{Z}[X]$ is geen IHR
- $k[x, y] = k[x][y]$ ($k$ een lichaam) is geen HIR.

# §8.3 Ontbindingsringen (Unique factorisation domains)

## Idee

Imiteer de unieke ontbinding van alle $n \geq 2$ in $\mathbb{Z}$ in priemfactoren.

## Definitie

Zij $R$ een domein.

- Een element $r$ in $R$ heet **irreducibel** als $r \neq 0$, $r \notin R^*$ en als $r = ab$ met $a, b \in R$, dan is $a \in R^*$ of $b \in R^*$.
- Een element $r$ in $R$ heet **priemelement** als $r \neq 0$ en $(r)$ is een priemideaal van $R \Leftrightarrow r \neq 0$, $r \notin R^*$ en $r|ab$ implicieert $r|a$ of $r|b$. De priemeigenschap.
- $a$ en $b$ in $R$ heten **geassocieerd** (Assosiated) als er een $u \in R^*$ met $a = ub$. ($a$ ene $b$ zijn geassocieerd is een equivalentie relatie: het zijn banen van de werking van $R^*$ op $R$ door linksvermenigvuldiging)

# §8.3 Ontbindingsringen (Unique factorisation domains)

## Herhaling baan

$G \times A \to A$ met $(g, a) \mapsto ga$ een groepswerking met $G$ een groep.
Baan van $a = Ga = \{ga | g \in G\}$.

## Opmerking

In een domein $R$:

- $a|b$ en $b|a \Leftrightarrow a$ en $b$ zijn geassocieerd $\Leftrightarrow (a) = (b)$
- Als $r$ irreducibel is, $u \in R^*$, dan is $ur$ ook irreducibel.
- Als $r$ priemelement is, $u \in R^*$, dan is $ur$ ook priemelement.

# §8.3 Ontbindingsringen (Unique factorisation domains)

## Opmerking

Een priem**getal** in $\mathbb{Z}$ is gedefinieerd als een positief irreducibel element van $\mathbb{Z}$.
De irreducibele elementen van $\mathbb{Z}$ zijn $\pm p$ met $p$ een priem**getal**.
Een priemgetal in $\mathbb{Z}$ is ook een priem**element** volgens het lemma van Euclides: $p|ab \Rightarrow p|a \vee p|b$.
We zullen zien: de priemelementen van $\mathbb{Z}$ zijn $\pm p$ met $p$ priem**getal**.

# §8.3 Ontbindingsringen (Unique factorisation domains)

## Stelling

In een willekeurig domein $R$ is elk priem element irreducibel.

## Bewijs

$r \in R$ is priem betekend: $r \neq 0$, $r \notin R^*$ en $r|ab$ implicieert $r|a$ of $r|b$.
$r$ is irreducibel betekend $r \neq 0$, $r \notin R^*$ en als $r = ab$ dan is $a \in R^*$ of $b \in R^*$.
Dus te bewijzen: als $r = ab$ dan is $a \in R^*$ of $b \in R^*$.
Neem aan $r = ab$, dan geldt $r|ab$ (want $ab = 1r$) dus ($r$ priemelement) geldt $r|a$ of $r|b$.
Stel $r|a$, dan geldt $a = rc$ voor een $c \in R \Rightarrow r = ab = rbc$ met $r \neq 0$ want $R$ is een domein. Nu geldt $1 = bc$ dus $b \in R^*$. Net zo: als $r|b$ dan $a \in R^*$. Dus $r$ is irreducibel.

# §8.3 Ontbindingsringen (Unique factorisation domains)

## Voorbeeld

In $\mathbb{Z}[\sqrt{-5}]$ geldt $6 = 2 \cdot 3 = (1 + \sqrt{-3})(1 - \sqrt{-5})$.
Ga na met behulp van de norm $N(a + b\sqrt{-5}) = a^2 + 5b^2$:
$2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ zijn irreducibel en $\mathbb{Z}[\sqrt{-5}]^* = \{\pm 1\}$.
Geen van die elementen is priem: bijvoorbeeld:
$2 | (1 + \sqrt{-3})(1 - \sqrt{-5}) = 3 \cdot 2$ maar $2 \not| 1 + \sqrt{-5}$ en $2 \not| 1 - \sqrt{-5}$,
want $(a + b\sqrt{-5})2 = 2a + 2b\sqrt{-5}$, maar $a$ is niet even.

## Stelling

In een HIR (bijvoorbeeld een Euclidische ring) is een irreducibel element priem (de begrippen 'irreducibel' en 'priemelement' vallen samen).

## Bewijs

Zie boek voor ander bewijs.
Neem $p \in R$ irreducibel. Dan geldt per definitie: $p \neq 0$ en $p \notin R^*$.
Stel $p|ab$, te bewijzen: $p|a$ of $p|b$.
Als $p|a$ dan klaar.
Als $p \not| a$ dan is $(p, a) \supsetneq (p)$ $a \in (p) \Leftrightarrow p|a$
$R$ is HIR dus $(p, a) = (d)$ voor een $d \in R$ met $p \in (d)$ dus $p = cd$ voor een $c \in R$.
$p$ is irreducibel, dus $c \in R^*$ of $d \in R^*$.
Als $c \in R^*$, dan is $(p) = (d) = (p, a)$ tegenspraak.
Dus $d \in R^*$, dan is $(p, a) = (d) = R$.
$\Rightarrow 1 = xp + ya$ voor zekere $x, y \in R$.
Dan is $b = bxp + bya$ geeft $b = p(bx + yz)$ met $ab = pz$. Dus $b$ is deelbaar door $p$.

# §8.3 Ontbindingsringen (Unique factorisation domains)

## Voorbeeld

$\mathbb{Z}[\sqrt{-5}]$ is geen HIR want het is irreducibel maar niet priem.

## Definitie

Een ontbindingsring $R$ is een domein zodat elke $r \in R$, $r \neq 0$, $r \notin R^*$ te schrijven als $r = p_1 p_2 \dots p_s$ met alle $p_i$ irreducibel, en als $r = q_1 q_2 \dots q_t$ met $q_j$ irreducibel, dan geldt $s = t$ en op het hernummeren van de $q_j$ na geldt $p_i = u_i q_i$ met $u_i \in R^*$. Dat wil zeggen $p_i$ en $q_i$ zijn geassocieerd.

# §8.3 Ontbindingsringen (Unique factorisation domains)

## Voorbeeld

- In $\mathbb{Z}[\sqrt{-11}]$ geldt $12 = 2 \cdot 2 \cdot 3 = (1 + \sqrt{-11})(1 - \sqrt{-11})$ en $2, 3, 1 + \sqrt{-11}, 1 - \sqrt{-11}$ irreducibel en $\mathbb{Z}[\sqrt{-11}]^* = \{\pm 1\}$ $\Rightarrow \mathbb{Z}[\sqrt{-11}]$ is geen ontbindingsring.
- Een lichaam heeft geen irreducibele elementen, alleen 0 en eenheden.
- Elke HIR is een ontbindingsring. (Dus euclidische ring als $\mathbb{Z}$, $\mathbb{Z}[i]$, $k[X]$ $k$ een lichaam.) later meer.
- Als $R$ een ontbindingsring is, dan is $R[X]$ dat ook. Voorbeeld: $\mathbb{Z}[X]$, $k[x, y] = k[x][y]$ met $k$ een lichaam.

## Voorbeeld

In $\mathbb{Z}[i]$: $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$
$2 = (1+i)(1-i)$
Dus elementen van norm 2 zijn mogelijke delers: $\pm 1 \pm i = u(1+i)$ met $u$ een eenheid.
$\pm 1 \pm i$ zijn irreducibel want $N(\pm 1 \pm i) = 2$ is priemgetal.
Als $\alpha = \beta\gamma$, dan geldt $N(\alpha) = N(\beta)N(\gamma)$ in $\mathbb{N} \cup \{0\}$
$\beta \in \mathbb{Z}[i]^* \Leftrightarrow N(\beta) = 1$
Dus als $N(\alpha) =$ priemgetal $\Rightarrow \alpha$ is irreducibel in $\mathbb{Z}[i]$.
$5 = (2+i)(2-i)$, $N(2 \pm i) = 5$ is priemgetal, dus $2 \pm i$ zijn irreducibel.
Als $3 = \beta\gamma$, dan is $9 = N(3) = N(\beta)N(\gamma) = 1 \cdot 9 \vee 3 \cdot 3 \vee 9 \cdot 1$.
Maar $3 \neq a^2 + b^2$ voor $a, b \in \mathbb{Z}$.
Dus of $N(\beta) = 1$ of $N(\gamma) = 1$, dus $\beta$ of $\gamma \in \mathbb{Z}[i]^*$. Dus 3 is irreducibel in $\mathbb{Z}[i]$.