Ringen en Lichamen

Luc Veldhuis

2 Oktober 2017

Herhaling

Vorige keer

Maximale idealen

Idealen van een lichaam F:

$\{0\}, F$

Als $\phi : F \to R$ een ringhomomorfisme is, dan is $\ker(\phi)$ een ideaal van F.

Als $\ker(\phi) = \{0\} \Rightarrow \phi$ injectief

Als $\ker(\phi) = F \Rightarrow \phi$ het nulhomomorfisme $\phi(a) = 0 \ \forall a \in F$.

Maximaal ideaal

$M \subseteq R$ maximaal ideaal als:

- M is een ideaal van R
- $M \neq R$
- Als N ideaal met $M \subseteq N \subseteq R$ dan geldt $N = M$ of $N = R$.

Quotient ringen

Stelling

Als R commutatief is met 1 en $M \subseteq R$ een ideaal van R, dan geldt: M is een maximaal ideaal van $R \Leftrightarrow R/M$ is een lichaam.

Bewijs

'$\Rightarrow$': R/M is commutatief, $\overline{1} \neq \overline{0}$ en elke $\overline{x} \neq \overline{0}$ heeft een inverse.

- R commutatief $\Rightarrow$ R/M commutatief
- R/M heeft identiteit $\overline{1} = 1 + M$.
  Als $\overline{0} = \overline{1}$, dan geldt $1 - 0 \in M$, dus $1 \in M$, dan $M = R$. Kan niet, M is een maximaal ideaal. $\Rightarrow \overline{1} \neq \overline{0}$.
- Neem $\overline{x} \neq \overline{0}$ in R/M, dus we hebben een $x \notin M$. Dan is $N = M + (x) = \{m + rx | m \in M, r \in R\}$ een ideaal van R dat M bevat en $x \Rightarrow M \subsetneq N$. M is een maximaal ideaal, dus $N = R$. Dus er bestaan $y \in R$, $m \in N$ met $m + y = 1$ in R $\Rightarrow \overline{yx} = \overline{1}$ in $R/M \Rightarrow \overline{x}$ heeft multiplicatieve inverse $\overline{y}$.

Quotient ringen

Opgave

'$\Leftarrow$': Doe zelf.
Hint: als V een ideaal is van R met $M \subsetneq N \subseteq R$, dan is er $x \in N$ met $\overline{x} \neq \overline{0}$ in R/M.

Voorbeeld

- Gezien: in $R = \mathbb{Z}$ zijn de maximale idealen (p) met p priem. Dus $\mathbb{Z}/(p) = \mathbb{Z}/p\mathbb{Z}$ een lichaam.
- $R = C^0(\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{C} \text{ continu}\}$ een ring met puntsgewijze optelling en vermenigvuldiging van functies.
  $\phi_a : R \to \mathbb{C}$ met $f \mapsto f(a)$ voor $a \in R$ is een surjectief ring homomorfisme. (De constante functie a beeld af op a
  Conclusie 1e isomorfie-stelling: $R/\ker(\phi_a) \cong \mathbb{R}$ en $\ker(\phi_a) = \{f \in C^0(\mathbb{R}) \text{ met } f(a) = 0\}$ is een maximaal ideaal van R

Definitie

Zij R een commutatieve ring met $1 \neq 0$. $P \subseteq R$ heet een priemideaal van R als:

- P is een ideaal van R
- $P \neq R$
- Als $a, b \in \mathbb{R}$ zijn met $ab \in P$, dan geldt $a \in P$, $b \in P$. p priem in $\mathbb{Z}$. $p|ab \Rightarrow p|a$ of $p|b$.

Voorbeeld

In $\mathbb{Z}$ (met idealen (n) met $n > 0$) zijn de priemidealen (0) em (p) met p een priemgetal. (De maximale idealen van $\mathbb{Z}$.)

Stelling

Als R een commutatieve ring is, met $1 \neq 0$, $P \subseteq R$ een ideaal van R, dan geldt:
P is een priem ideaal van $R \Leftrightarrow R/P$ is een IIG

Quotient ringen

Bewijs

Opgave.

Gevolg

In een commutatieve ring met $1 \neq 0$ is een maximaal ideaal een priemideaal.

Bewijs

Als P het ideaal in een Rde ring, dan geldt P is maximaal ideaal $\Leftrightarrow R/P$ is een lichaam $\Rightarrow R/P$ is een IIG $\Leftrightarrow P$ is een priemideaal.

Quotient ringen

Voorbeeld

$R = \mathbb{Z}[X]$, $I = (X) = \{a(x)x | a(x) \in \mathbb{Z}[X]\}$.
Is I een priemideaal? Maximaal ideaal?
$R/I \cong \mathbb{Z}$ (met 1e isomorfie stelling, beginnend met $\phi : \mathbb{Z}[X] \to \mathbb{Z}$, $f(x) \mapsto f(0)$.)
Uit de vorige 2 stellingen:
I is een priemideaal van $\mathbb{Z}[X]$ want $\mathbb{Z}$ is een domein.
I is geen maximaal ideaal van $\mathbb{Z}[X]$ want $\mathbb{Z}$ is geen lichaam.

Voorbeeld

$J = (2, x)$, dan geldt $I \subsetneq J \subsetneq R$, (want $2 \in J$, $2 \notin I$)

Definitie

R commutatieve ring
$\emptyset \neq D \subseteq R$ zodat:

- $0 \notin D$
- D bevat geen 0 delers
- D is gesloten onder vermenigvuldiging: als $a, b \in D$, dan $ab \in D$.

D staat voor denominator. Niet delen door 0.

Voorbeeld

$R = \mathbb{Z}$, $D = \mathbb{Z} \setminus \{0\}$
Neem $R \times D$ met $\sim$: $(r, d) \sim (s, e) \Leftrightarrow er = ds$.
$(\frac{r}{d} = \frac{s}{e} \Leftrightarrow er = ds)$
Dan is $\sim$ een equivalentierelatie:

- $(r, d) \sim (r, d)$
- $(r, d) \sim (s, e) \Rightarrow (s, e) \sim (r, d)$
- $(r, d) \sim (s, e)$ en $(s, e) \sim (t, f) \Rightarrow (r, d) \sim (t, f)$

  We weten $\begin{cases} er = ds \\ fs = et \end{cases} \Rightarrow erf = dsf = det = edt$. Dus $e(rf - dt) = 0$ in R. Dus $e \neq 0$ en e geen nuldeler. Dus $rf = dt$. Dus $(r, d) \sim (f, t)$.

§7.5 Breukenringen

Definitie

Schrijf $\frac{r}{d}$ voor de equivalentie klasse van (r, d). (Dus $\frac{r}{d} = \frac{s}{e} \Leftrightarrow (r, d) \sim (s, e) \Leftrightarrow er = ds$ en $D^{-1}R = \{$ equivalentie klassen $\frac{r}{d} | r \in R, d \in D\}$.
Definieer nu op $D^{-1}R$ optelling: $\frac{a}{d} + \frac{b}{e} = \frac{ae+bd}{de}$.
Vermenigvuldiging: $\frac{a}{d}\frac{b}{e} = \frac{ab}{de}$.
Ga na: die zijn welgedefinieerd.
Ga na: $S = D^{-1}R$ is met deze bewerkingen een commutatieve ring met identiteit $\frac{d}{d}$ voor elke $d \in D$.
Dan geldt $0_s = \frac{0}{d}$ voor elke $d \in D$, $-\frac{a}{d} = \frac{-a}{d}$.
Definieer $\phi : R \to S$ met $r \mapsto \frac{rd}{d}$ voor een vaste $d \in D$. ($\frac{rd}{d} = \frac{re}{e}$ $\forall e \in D$) Dan is ϕ een injectief ringhomomorfisme. (Ga na.)
Dus ϕ is injectief $\Leftrightarrow \ker(\phi) = \{0_r\}$.
$r \in \ker(\phi) \Leftrightarrow \phi(r) = \frac{rd}{d} = \frac{0}{d} = 0_s \Leftrightarrow rd^2 = 0d = 0 \Leftrightarrow r = 0$ want $0 \notin D$ bevat geen nuldeler.
In totaal: breukring $S = D^{-1}R$. $\phi : R \hookrightarrow S$ injectieve afbeelding.

Voorbeeld

- $R = \mathbb{Z}$, $D = \mathbb{Z} \setminus \{0\}$ is $S = \mathbb{Q}$, de definitie van $\mathbb{Q}$.
- Als R een domein is, $1 \in D = R \setminus \{0\}$, dan heet $D^{-1}R = \{\frac{a}{b} | a, b \in R, b \neq 0\}$ het breukenlichaam F naar R, $Frac(R)$, met $1_F = \frac{1_R}{1_R}$, $\frac{a}{b} = 0 \Leftrightarrow a = 0_R$.
  Als $\frac{a}{b} \neq 0_F$ dan $\frac{b}{a} = (\frac{a}{b})^{-1}$.
- $R = \mathbb{Z}$, $D = \{1, 2, 4, 8, \dots\}$, $D^{-1}R = \{\frac{a}{2^m} | a \in \mathbb{Z}, m \geq 0\} \subseteq \mathbb{Q}$
- $R = \mathbb{Z}[X]$, $Frac(R) = \{\frac{\alpha}{\beta} | \alpha, \beta \in \mathbb{Z}[X], \beta \neq 0\}$.
  $Frac(R) \cong \mathbb{Q}(i) = \{a + bi | a, b \in \mathbb{Q}\}$,
  $\frac{\alpha}{\beta} \mapsto \frac{\alpha\overline{\beta}}{\beta\overline{\beta}}$ in $\mathbb{Q}(i) \subseteq \mathbb{C}$

§7.5 Breukenringen

Voorbeeld

Als k een lichaam is, X een variabele, dan is $R = k[X]$ een domein. Hier is
$Frac(R) = \{\frac{a(X)}{b(X)} | a(X), b(X) \in k[X], b(X) \neq 0\} = k(X)$ (definitie)

Voorbeeld

$\frac{2-i}{1+i} \mapsto \frac{(2-i)(1-i)}{(1+i)(1-i)} = \frac{1-3i}{2} = \frac{1}{2} + \frac{-3}{2} i$ met $\frac{2-i}{1+i} \in Frac(R)$ en $\frac{1}{2} + \frac{-3}{2} i \in \mathbb{Q}(i)$.

Reststelling voor ringen

Al gezien: $m, n \geq 2$, $ggd(m, n = 1)$ dan is $\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ met $\overline{a} \mapsto (\overline{a}, \overline{a})$ is een ringhomomorfisme.
Als R een ring commutatieve ring is met 1, I en J idealen van R met $I + J = R$, dan geldt:

- $I \cdot J = I \cap J$
- $R/(I \cap J) \cong R/I \times R/J$ een ringhomomorfisme met $a + I + J \mapsto (a + I, a + J)$