Ringen en Lichamen

Luc Veldhuis

11 September 2017

Herhaling

Vorige keer

R een ring

- $a \neq 0$ heet **nuldeler** als er $b \neq 0$ is met $ab = 0$ of $ba = 0$
- Als R een $1 \neq 0$ heeft dan is
  $\mathbb{R}^* = \{u \in R | v \in R \text{ met } uv = vu = 1\}$

Herhaling

Vorige keer

De verzameling van eenheden van R:

- $1 \in R^*$
- Als $u \in R^*$ met $uv = vu = 1$ dan ook $v \in R^*$, gegeven $u \in R^*$ is die v uniek (notatie u^{-1})
- R^* is groep onder vermenigvuldiging
  - $1 \in R^*$, het neutrale element voor de vermenigvuldiging
  - Als $u_1, u_2 \in R^*$ dan bestaan $v_1, v_2 \in R^*$ met $u_i v_i = 1 = v_i u_i$ voor $i = 1, 2$.
    Dan is $u_1 u_2 v_2 v_1 = 1 = v_2 v_1 u_1 u_2 = v_2 1 u_2 = v_2 u_2 = 1$
  - Elke $u \in R^*$ heeft inverse u^{-1}
  - De vermenigvuldiging in R (dus R^*) is associatief

Ringen

Opmerking

Als R een $1 \neq 0$ heeft, dan is een element nooit zowel nuldeler als eenheid.
Stel a is beide, dus er is $c \in R$ met $ac = 1 = ca$ en $b \neq 0 \in R$ met $ab = 0$ of $ba = 0$. Zeg als $ab = 0$, dan geldt $b = 1b = cab = c0 = 0$. Tegenspraak.

Voorbeeld

In een delingsring R (bijvoorbeeld een lichaam als $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$) geldt $R^* = R \setminus \{0\}$ en dus heeft een delingsring geen nuldeler.

Integriteitsgebied

Definitie

Integriteitsgebied of domein (Engels: integral domain) is een commutatieve ring met $1 \neq 0$ zonder nuldelers

Opmerking

In een ring zonder nuldelers geldt $ab = 0 \Leftrightarrow a = 0 \vee b = 0$, en dus ook $ab = ac \Leftrightarrow a(b - c) = 0 \Leftrightarrow a = 0$ of $b = c$.

Voorbeelden

- $\mathbb{Z}$ is een ITG
- Een lichaam is een ITG (Voorbeeld: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/p\mathbb{Z}$ met p priem)

Ringen

Stelling

Elk eindig ITG is een lichaam. Bewijs: zie boek
Ook: een eindige delingsring is een lichaam (Wedderbrom)

Definition

$S \subseteq R$ met R een ring heet een **deelring** als S met de $+$ en de $\cdot$ van R zelf een ring is.
Opgave $\Leftrightarrow$:

- $S \neq \emptyset$
- Als $a, b \in S$ dan zijn $a - b$ en ab ook in S

Voorbeeld

- $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C} \subseteq H$ zijn deelringen
- $s = \{\overline{0}, \overline{3}\} \subseteq \mathbb{Z}/6\mathbb{Z} = R$ een deelring, maar $1_S = \overline{3} \neq \overline{1}_R$

Ringen

Definitie

Op $\mathbb{Z}[\sqrt{D}]$ definieer je de **norm** N:
$N(a + b\sqrt{D}) = |(a + b\sqrt{D})(a - b\sqrt{D})| = |a^2 - Db^2| \in \mathbb{N}$

Voorbeeld

Als $D \in \mathbb{Z}$ en D is geen kwadraat, dan is
$\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} || a, b \in \mathbb{Z}\}$
$\mathbb{Z}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 | a, b, c \in \mathbb{Z}\}$ is een deelring van $\mathbb{C}$ ga na: $(\sqrt{D})^2 = D$.
Als $D = -1$ dan krijg je $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{C}\}$, de gehelen van Gauß
Dan geldt $N(\alpha\beta) = N(\alpha)N(\beta)$ als $\alpha, \beta \in \mathbb{Z}[\sqrt{D}]$.

Opmerking

In het algemeen geldt niet $N(\alpha + \beta) = N(\alpha) + N(\beta) = \alpha^2 + \beta^2$

Ringen

Voorbeeld

Als $D = -1$ dan is $N(a + bi) = a^2 + b^2$.
Wat is $\mathbb{Z}[i]^*$?
Stel $\alpha \in \mathbb{Z}[i]^*$, dan is er een $\beta \in \mathbb{Z}[i]$ met $\alpha\beta = 1 = \beta\alpha$
Dan geldt $N(1) = N(\alpha)N(\beta) = N(\alpha)N(\beta)$ met $N(\alpha), N(\beta) \in \mathbb{N}$
Hieruit volgt dat $N(\alpha) = N(\beta) = 1$
Als $\alpha = a + bi$, dan is $1 = N(\alpha) = a^2 + b^2$. Dus $a = \pm 1 \vee a = \pm i$.
Controleer nu of $\pm 1, \pm i$ eenheden zijn. Dus $\mathbb{Z}][i]^* = \{\pm 1, \pm i\}$

Ringen

Voorbeeld

$(a^2 + b^2)(c^2 + d^2)$ is een som van twee kwadraten:
$N(a^2 + b^2)N(c^2 + d^2) = N(a + bi)N(c + di) = N((a + bi)(c + di))$
is een som van twee kwadraten.

Sommige getallen zijn geen som van kwadraten

Als $a \in \mathbb{Z}$ dan is $a^2 \equiv 0, 1 \mod 4$
$a^2 + b^2 \equiv 0, 1, 2 \mod 4$ dus bijvoorbeeld 7 is geen som van twee kwadraten.

Voorbeeld

Als $D \in \mathbb{Z}$ geen kwadraat is, dan is $\mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} | a, b \in \mathbb{Q}\}$ is een lichaam en deelring van $\mathbb{C}$.
$a + b\sqrt{D} = 0 \Leftrightarrow a^2 - Db^2 = 0$ dus $(a - b\sqrt{D})(a + b\sqrt{D})$

Ringen

Wortel truuk van middelbare school

$$\frac{1}{a+b\sqrt{D}} = \frac{1}{a+b\sqrt{D}}\frac{a-b\sqrt{D}}{a-b\sqrt{D}} = \frac{a}{a^2-Db^2} + \frac{-b}{a^2-Db^2}\sqrt{D}$$

met $a \pm b\sqrt{D} \neq 0$

Definitie

R een ring, X een variabele.
$R[X] = \{$polynoom in X met coefficienten in $\mathbb{R}\} =$
$\{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n | n \in \mathbb{N}, a_i \in R \forall i \in \mathbb{N}\} =$
$\{\sum_{i=0}^{\infty} a_ix^i | a_i \in R, \text{ voor slechts eindig veel} a_i \neq 0\}$. Conventie:
$a_0x^0 = a_0$
Met optelling en vermenigvuldiging: $f(x) = \sum_{i=0}^{\infty} a_ix^i$,
$g(x) = \sum_{i=1}^{\infty} b_ix^i$ dan is
$(f+g)(x) = \sum_{i=0}^{\infty}(a_i + b_i)x^i$
$(fg)(x) = \sum_{i=0}^{\infty} c_ix^i$
met $c_i = \sum_{j=0}^{i} a_j \cdot b_{i-j}$ is een ring

Eigenschappen

- $R[X]$ is commutatief $\Leftrightarrow$ R is commutatief
- $R[X]$ heeft 1 $\Leftrightarrow$ R heeft 1 (als dat zo is $1_{R[X]} = 1_R$ als constante polynoom)
- $R \subseteq R[X]$ als de constante polynomen. Dit is een deelring.

Definitie

Als $0 \neq f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ met $a_n \neq 0$, dan heet n de **graad** van $f(x)$ (Engels: degree(f)), a_n de **kopcoëfficiënt** van $f(x)$.
Als $a_n = 1$ dan heet $f(x)$ monisch.

§7.2 Voorbeelden van ringen

Stelling

- Als $f(x) = a_m x^m + \cdots + a_1 x + a_0$, $a_m \neq 0$
  $g(x) = b_n x^n + \cdots + b_1 x + b_0$, $b_n \neq 0$
  en a_m, b_n zijn geen nuldelers, dan geldt
  $deg(fg) = deg(f) + deg(g)$
- Als $1 \in R$ en R heeft geen nuldelers dan geldt $R[X]^* = R^*$
- Als R een ITG is dan is $R[X]$ dat ook

Bewijs

- $f(x)g(x) = a_m b_n x^{m+n} + (a_m b_{n-1} + a_{m-1} b_n)x^{m+n-1} + \cdots + (a_1 b_0 + a_0 b_1)x + a_0 b_0$
  Dus $deg(fg) \leq deg(f) + deg(g)$.
  Hierbij is $a_n b_m \neq 0$ omdat a_m, b_n beide geen nuldeler zijn.
  $deg(fg) = m + n = deg(f) + deg(g)$.
- Stel $f(x) \in R[X]^*$ dus er is een $g(x)$ met
  $f(x)g(x) = 1 = g(x)f(x)$
  $f, g \neq 0$ en $0 = deg(1) = deg(fg) = deg(f) + deg(g)$ volgens 1.
  $deg(f) = deg(g) = 0$, dus $f, g \in R \setminus \{0\}$.
  Doe verder zelf
- Zie boek/doe zelf

§7.2 Voorbeelden van ringen

Voorbeeld

Als K een lichaam is (en dus ITG), dan is $K[X]$ een ITG, maar geen lichaam, want $K[X]^* = K^* = K \setminus \{0\}$ volgens de stelling.

Voorbeeld

In $R = \mathbb{Z}/4\mathbb{Z}[X]$ is elk element $\overline{1} + \overline{2}f(x)$ met $f(x)$ in R een eenheid want $(\overline{1} + \overline{2}f(x))^2 = \overline{1}$

Voorbeeld

Als R een ring is, $n \geq 1$, dan is $M_n(R) = \{n \times n \text{ matrices met coefficienten in } R\}$ met de gebruikelijke matrix optelling en vermenigvuldiging een ring. (Zie boek)