Tentamen Ringen en Lichamen I (WB012C)

- *Het is een* **gesloten boek** *tentamen. Gebruik van een rekenmachine of andere hulpmiddelen is* **niet** *toegestaan.*
- *Vermeld op ieder blad je naam en studentnummer.*
- *Lees eerst de opgaven voor dat je aan de slag gaat. Deel je tijd verstandig in.*
- *Schrijf leesbaar. Geef voldoende uitleg bij je oplossingen, antwoorden zonder heldere afleiding worden niet goedgekeurd.*

Opgave 1. Zij I een ideaal in een commutatieve ring R met eenheidselement 1_R. Zij I_0 de verzameling $I_0 = I \times \mathbb{Z}$ met optelling en vermenigvuldiging gegeven door

$$(r,n)+(s,m)=(r+s,n+m), \quad (r,n)\cdot(s,m)=(rs+mr+ns,nm) \quad (r,s\in I,\ n,m\in\mathbb{Z}).$$

(a) Toon aan dat I_0 met deze optelling en vermenigvuldiging een ring is.

(b) Laat zien dat $I \times \{0\}$ een priemideaal is in I_0.

Definieer nu $\varphi : I_0 \to R$ door $\varphi(r,n) = r + n \cdot 1_R$ voor alle $(r,n) \in I_0$.

(c) Laat zien dat φ een ringhomomorfisme is.

(d) Bepaal $\mathrm{Ker}(\varphi)$ voor het geval $R = \mathbb{Z}_n$, voor een $n \in \mathbb{N}\backslash\{0\}$, en $I = \{0\}$.

Opgave 2. Zij R een commutatieve ring met eenheidselement $1 \in R$ en zij I een ideaal in R. Het *wortelideaal* van I wordt gedefinieerd door

$$I^{\frac{1}{2}} = \{x \in R \mid x^n \in I \text{ voor een } n \in \mathbb{N}, n > 0\}.$$

(a) Laat zien dat $I^{\frac{1}{2}}$ een ideaal in R is.

(b) Neem aan dat I een priemideaal is. Toon aan dat dan $I^{\frac{1}{2}} = I$.

Opgave 3. Defineer $R = \{a/2^n \mid n \in \mathbb{N}, a \in \mathbb{Z}\}$.

(a) Toon aan dat R een deelring van $\mathbb{Q}$ is.

(b) Laat zien dat R isomorf is met $\mathbb{Z}[X]/I$ met $I = \langle 2x-1 \rangle$.

(c) Bepaal de eenhedengroep R^*.

Z.O.Z.

Opgave 4. Zij R een PID en $p \in R$ irreducibel. Schrijf F voor het lichaam $F = R/\langle p \rangle$. Laat $f = \sum_{k=0}^{n} a_k x^k \in R[X]$ zo dat p geen deler is van het kopcoëfficiënt a_n. Definieer $\bar{f} \in F[X]$ door $\bar{f} = \sum_{k=0}^{n} \bar{a}_k x^k$, waarbij $\bar{a}_k = \langle p \rangle + a_k \in F$. Bij onderdeel (d) moet de volgende implicatie bewezen worden:

$$\bar{f} \text{ is irreducibel in } F[X] \Longrightarrow f \text{ is irreducibel in } R[X] \tag{1}$$

Ter herinnering: Zij $g \in R[X]$. Dan is de *inhoud* van g, notatie $C(g)$, de grootste gemene deler van de coëfficiënten van g, welke uniek bepaald is op vermenigvulding met elementen van R^* na. Het polynoom g heet *primitief* als $C(g) \in R^*$.

(a) Zij $g \in R[X]$ primitief. Toon aan dat $g \in R[X]^*$ dan en slechts dan als $\deg(g) = 0$.

Stel nu dat $g, h \in R[X]$ polynomen zijn met $f = g \cdot h$. Dan geldt ook $\bar{f} = \bar{g} \cdot \bar{h}$. (Dit hoef je niet te bewijzen.)

(b) Bewijs dat g en h primitief zijn.

(c) Leid uit $p \nmid a_n$ af dat $\deg(g) = \deg(\bar{g})$ en $\deg(h) = \deg(\bar{h})$.

(d) Bewijs (1). Hint: Toon aan dat $\bar{f}$ reducibel is als f reducibel is.

(e) Gebruik het citerium (1) om aan te tonen dat $7x^3 - 51x^2 + 5x + 70$ irreducibel in $\mathbb{Z}[X]$ is.

Oplossing Opgave 1

(a)

(b)

(c)

Oplossing Opgave 2

(a) Pas de tweede deelring test toe: Zijn $a, b \in I^{\frac{1}{2}}$, zeg $a^n \in I$ en $b^m \in I$. Dan

$$(a-b)^{n+m} = \sum_{k=0}^{n+m} (-1)^k \binom{n+m}{k} b^k a^{n+m-k} \in I,$$

omdat voor $k < m$

$$(-1)^k \binom{n+m}{k} b^k a^{n+m-k} = \left((-1)^k \binom{n+m}{k} b^k a^{m-k}\right) a^n \in I$$

en voor $k \geq m$

$$(-1)^k \binom{n+m}{k} b^k a^{n+m-k} = \left((-1)^k \binom{n+m}{k-m} b^k a^{n+m-k}\right) b^m \in I.$$

Dus $a - b \in I^{\frac{1}{2}}$. Voor $c \in R$ geldt bovendien

$$(ca)^n = c^n a^n \in I,$$

dus $ca \in I^{\frac{1}{2}}$.

(b) Zij I een priemideaal. Stel $a, b \in R$ zo dat $ab \in I^{\frac{1}{2}}$. Zeg $n \in \mathbb{N}, n > 0$ zo dat $(ab)^n \in I$. Dan $(a^n)(b^n) \in I$. Aangezien I een priemideaal is geldt $a^n \in I$ of $b^n \in I$, oftewel $a \in I^{\frac{1}{2}}$ of $b \in I^{\frac{1}{2}}$.

Oplossing Opgave 3

(a) Dit volgt eenvoudig met de tweede deelring test:

$$\frac{a}{2^n} - \frac{b}{2^m} = \frac{a2^m - b2^n}{2^{n+m}}, \quad \frac{a}{2^n} \cdot \frac{b}{2^m} = \frac{ab}{2^{n+m}}.$$

(b) Neem als homomorfisme $\varphi : \mathbb{Z}[X] \to \mathbb{Q}$ gegeven door$\varphi(f) = f(1/2)$ voor elke $f \in \mathbb{Z}[X]$. Dit is zeker een homomorfisme. Als $f = \sum_{k=0}^{n} a_k x^k \in \mathbb{Z}[X]$, dan

$$\varphi(f) = \sum_{k=0}^{n} a_k (1/2)^k = \frac{\sum_{k=0}^{n} a_k 2^{n-k}}{2^n} \in R.$$

En voor $a \in \mathbb{Z}$ en $n \in \mathbb{N}$ geldt $\varphi(f) = \frac{a}{2^n}$ voor het polynoom $f = ax^n$. Dus $\mathrm{Im}\varphi = R$.
Stel $f \in \mathbb{Z}[X]$ met $\varphi(f) = 0$. Dan $f(1/2) = 0$. **Nog verder uitwerken.**

(c) Een element $\frac{a}{2^n}$ zit in R^* als er een $\frac{b}{2^m}$ bestaat zo dat $\frac{a}{2^n} \cdot \frac{b}{2^m} = \frac{ab}{2^{n+m}} = 1$, oftewel, $ab = 2^{n+m}$. Dit kan alleen als $a = 2^k$ voor een $k \in \mathbb{N}$, oftewel, voor elementen van de vorm 2^n voor $n \in \mathbb{Z}$. Daarintegen geldt dat $2^n \cdot 2^{-n} = 1$ en $2^{-n} \in R$ voor elke $n \in \mathbb{Z}$. Dus $R^* = \{2^n \mid n \in \mathbb{Z}\}$.

Oplossing Opgave 4

(a) $R[X]^* = R^*$. Dus als $g \in R[X]^*$, dan zeker $\deg(g) = 0$. Stel $\deg(g) = 0$. Dan $g \in R \subset R[X]$. Dus $g = C(g) \in R^* = R[X]^*$.

(b) Er geldt $C(g)C(h) = C(gh) = C(f) \in R^*$. Zeg $a = (C(g)C(h))^{-1}$. Dit impliceert $C(g), C(h) \in R^*$, want $C(g)C(h)a = 1$, dus $(C(g))^{-1} = C(h)a$, en $aC(g)C(h) = 1$, dus $(C(h))^{-1} = aC(g)$. Maar $C(g), C(h) \in R^*$ zegt precies dat g en h primitief zijn.

(c) Aangezien $p \nmid a_n$, geldt $\deg(f) = \deg(\bar{f})$. Omdat R en F beide integriteitsgebieden zijn, volgt dat

$$\deg(g) + \deg(h) = \deg(f) = \deg(\bar{f}) = \deg(\bar{g}) + \deg(\bar{h}).$$

Uit de constructie van $\bar{g}$ en $\bar{h}$ volgt dat $\deg(\bar{g}) \leq \deg(g)$ en $\deg(\bar{h}) \leq \deg(h)$. Voor de bovenstaande gelijkheden is het dus noodzakelijk dat $\deg(\bar{g}) = \deg(g)$ en $\deg(\bar{h}) = \deg(h)$.

(d) Uit het bovenstaande volgt

$$\begin{aligned} f \text{ is reducibel in } R[X] &\implies f = gh \text{ met } g, h \in R[X] \setminus R[X]^* \\ &\implies f = gh \text{ met } g, h \in R[X], \deg(g), \deg(h) > 0 \\ &\implies \bar{f} = \bar{g}\bar{h} \text{ met } \bar{g}, \bar{h} \in F[X], \deg(\bar{g}), \deg(\bar{h}) > 0 \\ &\implies \bar{f} = \bar{g}h \text{ met } \bar{g}, h \in F[X] \setminus F[X]^* \\ &\implies \bar{f} \text{ is reducibel in } F[X] \end{aligned}$$

(e) Neem $p = 5$, dan heeft $\bar{f}$ een dubbel nulpunt te 0.