# Tentamen Ringen en Lichamen op 2 april 2020 (kans A)

*Door deel te nemen aan dit tentamen verklaart de student zich te onthouden van het plegen van fraude. Indien de docent het vermoeden heeft dat er is gefraudeerd, zal er contact worden opgenomen met de student. Zo nodig zal de zaak worden doorverwezen naar de examencommissie.*

**Vergeet niet je bladeren vóór het uploaden met je naam te voorzien en duidelijk te nummeren zo dat het ingeleverde werk in een zinvolle volgorde gebracht kan worden.**

**Opgave 1.** *(8 punten)*
Zij $R$ een commutatieve ring. Voor een ideaal $I$ van $R$ definiëren we de verzameling $\sqrt{I}$ door

$$\sqrt{I} := \{a \in R \mid a^n \in I \text{ voor een } n \in \mathbb{N}_{>0}\}.$$

(i) Toon aan dat $\sqrt{I}$ een ideaal van $R$ is en dat $I \subset \sqrt{I}$.

(ii) Bewijs dat voor idealen $I, J$ van $R$ geldt dat $\sqrt{I \cdot J} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

(iii) Laat zien dat $\sqrt{P} = P$ als $P$ een priemideaal van $R$ is.

**Oplossing:**

(i) Voor $a \in I$ is $a^1 = a \in I$, dus is $I \subset \sqrt{I}$.

Zij $a \in \sqrt{I}$ met $a^n \in I$ en $r \in R$. Dan is $(ra)^n = r^n a^n \in I$ omdat $a^n \in I$, $r^n \in R$ en $I$ een ideaal is, en dus is $ra \in \sqrt{I}$.

Stel nu dat $a, b \in \sqrt{I}$ met $a^n \in I$ en $b^m \in I$. Dan is $(a+b)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} a^k b^{n+m-k}$. Voor $k < n$ is $n + m - k > m$ en dus $b^{n+m-k} \in I$ en dus ook $\binom{n+m}{k} a^k b^{n+m-k} \in I$. Voor $k \geq n$ is $a^k \in I$ en dus ook $\binom{n+m}{k} a^k b^{n+m-k} \in I$. Dus is $(a+b)^{n+m} \in I$ en dus $a+b \in \sqrt{I}$. Met $a$ is natuurlijk ook $-a \in \sqrt{I}$ omdat $(-a)^n = (-1)^n a^n \in I$.

(ii) Er geldt altijd dat $I \cdot J \subset I \cap J \subset I, J$. Zij $a \in \sqrt{I \cdot J}$, dan is $a^n \in I \cdot J$ voor een $n \in \mathbb{N}$ en dan is $a^n \in I \cap J$ en $a^n \in I$ en $a^n \in J$. Dit betekent dat $a \in \sqrt{I \cap J}$ en $a \in \sqrt{I} \cap \sqrt{J}$. Dit argument laat ook zien dat voor $a \in \sqrt{I \cap J}$ geldt dat $a \in \sqrt{I} \cap \sqrt{J}$.

Zij nu omgekeerd $a \in \sqrt{I} \cap \sqrt{J}$, dan is $a^n \in I$ en $a^m \in J$ en zonder verlies van algemeenheid nemen we aan dat $n \geq m$ zo dat $a^n \in I$ en $a^n \in J$. Dan is $a^n \in I \cap J$ en dus $a \in \sqrt{I \cap J}$. Ook is $a^{n+m} = a^n \cdot a^m \in I \cdot J$, dus is $a \in \sqrt{I \cdot J}$. Met hetzelfde argument geldt voor $a \in \sqrt{I \cap J}$ dat $a^n \in I$ en $a^n \in J$ en dus $a^{2n} \in I \cdot J$, zo dat $a \in \sqrt{I \cdot J}$.

(iii) Zij $a \in \sqrt{P}$ en neem aan dat $a^n \in P$ met $n$ minimaal. Dan is $a \cdot a^{n-1} \in P$ en omdat $P$ een priemideaal is, is dan $a \in P$ of $a^{n-1} \in P$. Wegens de minimaliteit van $n$ is niet $a^{n-1} \in P$, dus is $a \in P$ en dus $n = 1$.

**Opgave 2.** *(10 punten)*
Zij $R := \mathbb{Z}[\sqrt{-19}] = \{a + b\sqrt{-19} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$. Laten $I := (2, 1+\sqrt{-19})$, $J_1 := (5, 1+\sqrt{-19})$ en $J_2 := (5, 1-\sqrt{-19})$ idealen zijn in $R$.

(i) Ga na welke van de idealen $I^2 = I \cdot I$ en $J_1 \cdot J_2$ hoofdidealen zijn.

(ii) Bewijs dat $R$ geen ontbindingsring is.

(iii) Licht toe dat $R/J_1$ een lichaam is.

(iv) Welke van de restklassenringen $R/(2)$, $R/(3)$ en $R/(5)$ hebben nuldelers, welke zijn integriteitsgebieden en welke zijn lichamen?

**Oplossing:** We hanteren op $R$ de norm $N(a+b\sqrt{-19}) = a^2 + 19b^2$. Deze norm is multiplicatief omdat $N(z) = |z|^2$ voor de absolute waarde op $\mathbb{C}$.

(i) $I \cdot I = (4, 2+2\sqrt{-19}, -18+2\sqrt{-19}) = (4, 2+2\sqrt{-19})$. Als dit een hoofdideaal was, zou de norm van de voortbrenger de $ggd$ van $N(4) = 16$ en $N(2+2\sqrt{-19}) = 80$ moeten delen, dus $16$, maar de enige mogelijkheid hiervoor is dat de voortbrenger $\pm 4$ of $\pm 2$ is (want $I^2 \neq R$). Omdat $2+2\sqrt{-19}$ geen veelvoud van $4$ is, is $I^2 \neq (4)$. Aan de andere kant is $2 \notin I^2$, want men gaat makkelijk na dat voor iedere $a+b\sqrt{-19} \in I^2$ geldt dat $4 \mid (a+b)$.

$J_1 \cdot J_2 = (25, 5-5\sqrt{-19}, 5+5\sqrt{-19}, 20) = (5)$, want alle voortbrengers zijn veelvouden van $5$ en $5 = 25 - 20 \in J_1 \cdot J_2$. Dit is dus een hoofdideaal.

(ii) Omdat $R$ geen elementen van norm $2$ en $5$ bevat, zijn $2$ en $5$ irreducibele elementen. Verder zijn ook $1 \pm \sqrt{-19}$ irreducibel, want deze elementen hebben norm $20$ en in een opsplitsing $1 \pm \sqrt{-19} = ab$ met $N(a), N(b) \neq 1$ zou één van $a$ en $b$ norm $2$ of norm $5$ moeten hebben, hetgeen niet het geval is. De ontbindingen $2^2 \cdot 5 = 20 = (1+\sqrt{-19})(1-\sqrt{-19})$ zijn dus twee verschillende ontbindingen in irreducibele elementen, dus is $R$ geen ontbindingsring.

(iii) $J_1$ is de kern van de afbeelding $\varphi : R \to \mathbb{Z}/5\mathbb{Z}$, $a+b\sqrt{-19} \mapsto a - b \bmod 5$. Het is duidelijk dat $J_1$ in de kern van $\varphi$ ligt, want beide voortbrengers liggen in de kern. Aan de andere kant ligt $1$ niet in de kern en is $\varphi$ dus surjectief. Omdat $R/J_1$ en $\mathbb{Z}/5\mathbb{Z}$ beide $5$ elementen hebben, is dus $J_1$ de kern van $\varphi$. Maar dan is $R/J_1 \cong \mathbb{Z}/5\mathbb{Z} = \mathbb{F}_5$ een lichaam.

(iv) $R/(2)$ heeft nuldelers, want $1+\sqrt{-19}+(2)$ is niet nul, maar $(1+\sqrt{-19})^2 = -18+2\sqrt{-19} \in (2)$, dus is de restklasse van $1+\sqrt{-19}$ een nuldeler.

Net zo heeft $R/(5)$ nuldelers, want $1 \pm \sqrt{-19} + (5)$ zijn niet nul, maar $(1+\sqrt{-19})(1-\sqrt{-19}) = 20 \in (5)$, dus zijn de restklassen van $1 \pm \sqrt{-19}$ nuldelers.

Merk op dat $R \cong \mathbb{Z}[X]/(X^2+19)$, dus is $R/(3) \cong \mathbb{F}_3[X]/(X^2+1)$ en $X^2+1$ heeft geen nulpunten in $\mathbb{F}_3$ en is dus irreducibel. Dus is $R/(3) \cong \mathbb{F}_9$ een lichaam (en dus ook een integriteitsgebied).

Alternatief: $R/(3)$ is als groep isomorf met $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ en als $(3)$ geen maximaal ideaal is, moet er een ondergroep van index $3$ in $R$ zijn, die $(3)$ omvat en die een ideaal is. Maar er zijn slechts vier ondergroepen van orde $3$ in $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, deze zijn modulo $3$ voortgebracht door $1$, $1+\sqrt{-19}$, $1-\sqrt{-19}$ en $\sqrt{-19}$, maar geen van deze brengt samen met $3$ een ideaal voort dat index $3$ in $R$ heeft.

**Opgave 3.** *(6 punten)*
Zij $a, b \in \mathbb{Q}$, $a, b \neq 0$, $a \neq b$ en definieer $c := \sqrt{a} + \sqrt{b}$.

(i) Laat zien dat $\mathbb{Q}(c) = \mathbb{Q}(\sqrt{a}, \sqrt{b})$.

(ii) Wat zijn de mogelijke graden van de lichaamsuitbreiding $\mathbb{Q}(\sqrt{a},\sqrt{b}) \supset \mathbb{Q}$? Geef voor ieder van deze mogelijkheden een voorbeeld.

**Oplossing:**

(i) Het is duidelijk dat $\mathbb{Q}(c) \subset \mathbb{Q}(\sqrt{a},\sqrt{b})$.

Omgekeerd is $c^3 = a\sqrt{a} + 3a\sqrt{b} + 3b\sqrt{a} + b\sqrt{b} = (a+3b)\sqrt{a} + (b+3a)\sqrt{b}$, dus is $c^3 - (b+3a)c = ((a+3b)-(b+3a))\sqrt{a} = (2b-2a)\sqrt{a}$. Wegens $a \neq b$ is $2b-2a \neq 0$ en dus is $\sqrt{a} \in \mathbb{Q}(c)$ en dan is ook $\sqrt{b} \in \mathbb{Q}(c)$ en dus $\mathbb{Q}(\sqrt{a},\sqrt{b}) \subset \mathbb{Q}(c)$.

Alternatief: Wegens $a, b, c \in \mathbb{Q}(c)$ is $\frac{a-b}{c} = \sqrt{a} - \sqrt{b} \in \mathbb{Q}(c)$, en samen met $c = \sqrt{a} + \sqrt{b}$ levert dit $\sqrt{a}$ en $\sqrt{b}$ op.

(ii) Er geldt $[\mathbb{Q}(\sqrt{a},\sqrt{b}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{a},\sqrt{b}) : \mathbb{Q}(\sqrt{a}] \cdot [\mathbb{Q}(\sqrt{a}) : \mathbb{Q}]$. Omdat $\sqrt{b}$ een nulpunt is van $X^2 - b$ (gezien als veelterm over $\mathbb{Q}(\sqrt{a})$) en $\sqrt{a}$ een nulpunt is van $X^2 - a$ (over $\mathbb{Q}$), zijn beide graden $1$ of $2$ en is de graad $[\mathbb{Q}(\sqrt{a},\sqrt{b}) : \mathbb{Q}]$ één van $1$, $2$ of $4$.

De graad is $1$ als $a$ en $b$ kwadraten zijn in $\mathbb{Q}$, bijvoorbeeld $a = 4$ en $b = 9$, dan is $c = 5$.

De graad is $2$ als precies één van $a$ en $b$ een kwadraat is, bijvoorbeeld voor $a = 4$ en $b = 2$, dan is $c = 2 + \sqrt{2}$, of als $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{b})$, bijvoorbeeld als $a = 2$ en $b = 8$, dan is $c = \sqrt{2} + 2\sqrt{2} = 3\sqrt{2}$.

De graad is $4$ als $\mathbb{Q}(\sqrt{a})$ en $\mathbb{Q}(\sqrt{b})$ twee verschillende kwadratische uitbreidingen zijn van $\mathbb{Q}$, bijvoorbeeld als $a = 2$ en $b = 3$.

**Opgave 4.** *(10 punten)*
Zij $a := \sqrt[4]{2} \in \mathbb{R}$ en $b := \sqrt[6]{2} \in \mathbb{R}$.

(i) Bereken de minimumveeltermen van $a+1$ en $a^{-1}$ over $\mathbb{Q}$.

(ii) Bepaal de graden van de lichaamsuitbreidingen $\mathbb{Q}(a) \supset \mathbb{Q}$, $\mathbb{Q}(b) \supset \mathbb{Q}$, $\mathbb{Q}(a,b) \supset \mathbb{Q}$ en $\mathbb{Q}(a) \cap \mathbb{Q}(b) \supset \mathbb{Q}$.

(iii) Bereken de minimumveelterm van $b$ over $\mathbb{Q}(a)$.

(iv) Zij $t$ transcendent over $\mathbb{Q}$. Bewijs dat dan ook $ta$ en $t+a$ transcendent zijn over $\mathbb{Q}$.

**Oplossing:**

(i) Het is duidelijk dat $f^a_{\mathbb{Q}}$ een deler is van $X^4 - 2$, maar dit is Eisenstein (bij $p = 2$) en dus irreducibel, dus is $f^a_{\mathbb{Q}} = X^4 - 2$. Omdat $a$ en $a+1$ dezelfde lichaamsuitbreiding voortbrengen, heeft ook $f^{a+1}_{\mathbb{Q}}$ graad $4$. Er geldt $f^{a+1}_{\mathbb{Q}} = f^a_{\mathbb{Q}}(X-1)$, want $f^a_{\mathbb{Q}}((a+1)-1) = f^a_{\mathbb{Q}}(a) = 0$, dus is $f^{a+1}_{\mathbb{Q}} = (X-1)^4 - 2 = X^4 - 4X^3 + 6X^2 - 4X - 1$.

Uit $a^4 = 2$ volgt $(a^{-1})^4 = a^{-4} = \frac{1}{2}$, dus is $f^{a^{-1}}_{\mathbb{Q}} = X^4 - \frac{1}{2}$.

(ii) We hebben al gezien dat $[\mathbb{Q}(a) : \mathbb{Q}] = 4$.

Net als in deel (i) is $f^b_{\mathbb{Q}}$ een deler van $X^6 - 2$, en ook dit is Eisenstein (bij $p = 2$) en dus irreducibel, dus is $f^b_{\mathbb{Q}} = X^6 - 2$ en $[\mathbb{Q}(b) : \mathbb{Q}] = 6$.

Omdat $\mathbb{Q}(a)$ en $\mathbb{Q}(b)$ deellichamen zijn van $\mathbb{Q}(a,b)$, moeten de graden van $\mathbb{Q}(a)$ en $\mathbb{Q}(b)$ over $\mathbb{Q}$ delers zijn van de graad van $\mathbb{Q}(a,b)$ over $\mathbb{Q}$. Dit betekent dat $12 \mid [\mathbb{Q}(a,b):\mathbb{Q}]$. Aan de andere kant is duidelijk dat voor $c := \sqrt[12]{2}$ geldt dat $[\mathbb{Q}(c):\mathbb{Q}] = 12$ en dat $a = c^3$ en $b = c^2$ en dus $\mathbb{Q}(a,b) \subset \mathbb{Q}(c)$. Dit betekent dat $[\mathbb{Q}(a,b):\mathbb{Q}] = 12$.

Omdat $\mathbb{Q}(a) \cap \mathbb{Q}(b)$ een deellichaam is van $\mathbb{Q}(a)$ en van $\mathbb{Q}(b)$ is de graad van $\mathbb{Q}(a) \cap \mathbb{Q}(b)$ over $\mathbb{Q}$ een deler van $4$ en van $6$ en is dus $1$ of $2$. Maar $\sqrt{2} = a^2 = b^3$ ligt in de doorsnede, dus is $[\mathbb{Q}(a) \cap \mathbb{Q}(b):\mathbb{Q}] = 2$.

(iii) Wegens $[\mathbb{Q}(a,b):\mathbb{Q}(a)] \cdot [\mathbb{Q}(a):\mathbb{Q}] = 12$ en $[\mathbb{Q}(a):\mathbb{Q}] = 4$ is $[\mathbb{Q}(a,b):\mathbb{Q}(a)] = 3$ en heeft $f^b_{\mathbb{Q}(a)}$ dus graad 3. Er geldt $b^3 = \sqrt{2} = a^2$, dus is $f^b_{\mathbb{Q}(a)} = X^3 - a^2$.

(iv) Zij $c = ta$ of $c = t + a$ en stel dat $c$ algebraïsch is over $\mathbb{Q}$. Omdat $a$ algebraïsch is over $\mathbb{Q}$ is dan ook $\mathbb{Q}(a,c)$ algebraïsch over $\mathbb{Q}$. Maar voor $c = ta$ is $t = \frac{c}{a}$ en voor $c = t + a$ is $t = c - a$ en in beide gevallen ligt $t$ in $\mathbb{Q}(a,c)$ en zou dus algebraïsch zijn over $\mathbb{Q}$. Dit is een tegenspraak, dus kan $c$ niet algebraïsch zijn over $\mathbb{Q}$.

**Opgave 5.** *(8 punten)*
Zij $\mathbb{F}_q$ het eindige lichaam met $q$ elementen, zij $\mathbb{F}_{q^2}$ de lichaamsuitbreiding van graad 2 van $\mathbb{F}_q$ en zij $n \in \mathbb{N}_{>0}$.

(i) Toon aan: De vergelijking $x^n = b$ heeft voor iedere $b \in \mathbb{F}_q$ een oplossing in $\mathbb{F}_q$ dan en slechts dan als $\gcd(n, q-1) = 1$. Laat ook zien dat in dit geval de oplossing eenduidig is.

(ii) Zij $\gcd(n, q-1) > 1$ en $0 \neq b \in \mathbb{F}_q$.

Bewijs dat het aantal elementen $a \in \mathbb{F}_q$ waarvoor $a^n = b^n$ geldt, gelijk is aan $\gcd(n, q-1)$.

(iii) Stel dat $q$ oneven is. Er zijn drie typen van elementen in $\mathbb{F}_{q^2}$:

(a) elementen $a$ met $a \in \mathbb{F}_q$;

(b) elementen $b$ met $b \notin \mathbb{F}_q$ maar $b^2 \in \mathbb{F}_q$;

(c) elementen $c$ met $c \notin \mathbb{F}_q$ en $c^2 \notin \mathbb{F}_q$.

Bepaal het aantal elementen van type (a), (b) en (c) in $\mathbb{F}_{q^2}$.

**Oplossing:**

(i) Omdat $\mathbb{F}_q^*$ een cyclische groep is, is de afbeelding $\alpha : x \mapsto x^n$ een groepshomomorfisme van $\mathbb{F}_q^*$. Zij $d = \gcd(n, q-1)$, dan is de kern van $\alpha$ de (eenduidige) ondergroep van orde $d$ in $\mathbb{F}_q^*$. In het bijzonder is $\alpha$ bijectief dan en slechts dan als $\gcd(n, q-1) = 1$ en in dit geval heeft $x^n = b$ voor iedere $b \in \mathbb{F}_q^*$ een eenduidige oplossing, namelijk $x = \alpha^{-1}(b)$. Als $\alpha$ niet bijectief is, is hij niet surjectief en is er dus niet voor iedere $b \in \mathbb{F}_q^*$ een oplossing van $x^n = b$.

(ii) Zij $d = \gcd(n, q-1)$ en schrijf $n = dm$ met $\gcd(m, q-1) = 1$. Volgens deel (i) is er een eenduidige $a \in \mathbb{F}_q$ met $a^m = b^m$ en dan geldt $a^n = (a^m)^d = (b^m)^d = b^n$.

Stel nu dat $a^n = b^n = (a')^n$, dan ligt $a'a^{-1}$ in de kern $K$ van $x \mapsto x^n$ en omgekeerd geldt voor iedere $a' = ak$ met $k \in K$ dat $(a')^n = a^n k^n = a^n = b^n$. We hadden in deel (i) al gezien dat $K$ de ondergroep van orde $d$ in $\mathbb{F}_q^*$ is, daarom zijn de verschillende oplossingen van $x^n = b^n$ juist de restklasse $aK$ en deze bevat $d$ elementen.

(iii) Natuurlijk zijn er $q$ elementen van type (a).

Omdat $q$ oneven is, is $q-1$ even en de kwadraten in $\mathbb{F}_q^*$ zijn juist de even machten van een primitief element $a \in \mathbb{F}_q$. Voor de oneven machten $n$ is dus $X^2 - a^n$ irreducibel over $\mathbb{F}_q$ en heeft in $\mathbb{F}_{q^2}$ twee nulpunten. Omdat er $\frac{q-1}{2}$ oneven getallen $1 \leq n \leq q-1$ zijn, geeft dit $q-1$ elementen van type (b).

De resterende $q^2 - 2q + 1 = (q-1)^2$ zijn dan van type (c).