Uitwerkingen Ringen en Galoistheorie, 7 april 2020

1. (a) (**5 pt**) Ontbind $X^8 - X^4 - 6$ in irreducibele factoren in $\mathbb{Z}[X]$.

   (b) (**5 pt**) Bepaal of het ideaal (X^3+2X-1, X^3+2X+2) in $\mathbb{Z}[X]$ een priemideaal is en of het een maximaal ideaal is.

   (c) (**5 pt**) Bepaal of het ideaal $(X^2 + 4XY + 5Y^2)$ in $\mathbb{Q}[X, Y]$ een priemideaal is en of het een maximaal ideaal is.

   Uitwerking.

   (a) Schrijf $f(X) = X^8 - X^4 - 6$, dan $f(X) = g(X^4)$ met $g(Y) = Y^2 - Y - 6$. We zien (eventueel via de abc-formule) dat $g(Y) = (Y - 3)(Y + 2)$, dus $f(X) = (X^4 - 3)(X^4 + 2)$. Nu is $X^4 - 3 \in \mathbb{Z}[X]$ Eisenstein bij 3 in $\mathbb{Z}$, dus irreducibel in $\mathbb{Q}[X]$. Ook is het primitief, dus irreducibel in $\mathbb{Z}[X]$. Net zo is $X^4 + 2$ Eisenstein bij 2 en primitief, dus irreducibel in $\mathbb{Z}[X]$. Dus $(X^4 - 3)(X^4 + 2)$ is de ontbinding in irreducibele factoren in $\mathbb{Z}[X]$ van $X^8 - X^4 - 6$.

   (b) Merk op dat $X^3+2X+2-(X^3+2X-1) = 3$, waaruit volgt dat $(X^3+2X-1, X^3 + 2X + 2) = (3, X^3 + 2X - 1)$. Noem dit ideaal I, dan is $\mathbb{Z}[X]/I \cong \mathbb{F}_3[X]/(X^3 + 2X - 1)$. (Dit is een toepassing van de derde isomorfiestelling; we delen eerst uit naar het ideaal (3). Zie opgave 2.4.18.) Het polynoom $X^3 + 2X - 1 = (X^3 - X) - 1$ in $\mathbb{F}_3[X]$ heeft geen nulpunten in $\mathbb{F}_3$ en is van graad 3, dus het is irreducibel in $\mathbb{F}_3[X]$. Maar $\mathbb{F}_3[X]$ is een hoofdideaaldomein (P.I.D.), want $\mathbb{F}_3$ is een lichaam. Het ideaal $(X^3 + 2X - 1)$ is dan een maximaal ideaal (en dus een priemideaal) in $\mathbb{F}_3[X]$; zie St. 5.2.3. Het quotiënt $\mathbb{F}_3[X]/(X^3 + 2X - 1)$ is dus een lichaam (met 27 elementen, maar dit terzijde), dus $\mathbb{Z}[X]/I$ is een lichaam, dus I is een maximaal ideaal in $\mathbb{Z}[X]$, dus ook een priemideaal.

   (c) Merk op dat $X^2 + 4XY + 5Y^2 = (X^2 + 4XY + Y^2) + Y^2 = (X + 2Y)^2 + Y^2$; in $\mathbb{C}[X, Y] = \mathbb{C}[Y][X]$ kan dit ontbonden worden als $(X + 2Y + iY)(X + 2Y - iY)$; in $\mathbb{Q}[Y][X]$ is deze ontbinding niet mogelijk, en het volgt dat het monische tweedegraadspolynoom $X^2 + 4XY + 5Y^2$ in X met coëfficiënten in $\mathbb{Q}[Y]$ irreducibel is (het heeft geen nulpunten in $\mathbb{Q}[Y]$).

   (Alternatief (zoals één van jullie vond) kun je X vervangen door $X + Y$; je krijgt dan $X^2 + 2XY + Y^2 + 4XY + 4Y^2 + 5Y^2 = X^2 + 6XY + 10Y^2$ in $\mathbb{Z}[Y][X]$. Dit is Eisenstein bij $2 \in \mathbb{Z}[Y]$ en primitief, dus irreducibel in $\mathbb{Z}[Y][X]$ en $\mathbb{Q}(Y)[X]$, dus ook in $\mathbb{Q}[Y][X]$. Ook het oorspronkelijke polynoom is dan irreducibel.) (Merk op: het is *niet* Eisenstein bij Y.)

   Als irreducibel element van de UFD $\mathbb{Q}[X, Y]$ brengt $X^2 + 4XY + 5Y^2$ een priemideaal voort. Dus $(X^2 + 4XY + 5Y^2)$ is een priemideaal in $\mathbb{Q}[X, Y]$. Maar het is duidelijk strikt bevat in (X, Y), wat een maximaal ideaal is (het quotiënt is het lichaam $\mathbb{Q}$), dus het is geen maximaal ideaal.

2. Laat R een commutatieve ring met 1 zijn. Ter herinnering: een element $a \in R$ is **nilpotent** als $a \neq 0$ en er een positief geheel getal n bestaat met $a^n = 0$. Een element $b \in R$ is **idempotent** als $b \neq 0, 1$ en $b^2 = b$.

   (a) (**5 pt**) Bewijs: R bevat een nilpotent element $\iff$ $R[X]$ bevat een nilpotent element.

   (b) (**5 pt**) Bewijs: $R[X]$ bevat een idempotent element van graad 1 $\implies$ R bevat een nilpotent element èn een idempotent element.

   (c) (**5 pt**) Bewijs dat $\mathbb{Z}/12\mathbb{Z}$ zowel een nilpotent element als een idempotent element bevat.

   (d) (**5 pt**) Bewijs dat $(\mathbb{Z}/12\mathbb{Z})[X]$ geen idempotent element van graad 1 bevat. (De omkering van (b) geldt dus niet.)

   Uitwerking.

   (a) Een nilpotent element van R is ook een nilpotent element van $R[X]$, want R is een deelring van $R[X]$. Laat $a(X) = a_k X^k + \cdots + a_1 X + a_0$ een nilpotent element van $R[X]$ zijn. Het is dan niet gelijk aan 0 en we mogen aannemen dat de kopcoëfficiënt a_k niet 0 is. Er bestaat een positief geheel getal n zo dat $a(X)^n = 0$. De coëfficiënt van X^{kn} in $a(X)^n$ is a_k^n. Dus $a_k^n = 0$, dus a_k is een nilpotent element van R. (Je kunt dit ook met a_0 proberen, maar a_0 kan 0 zijn, en je moet in feite met de "staartcoëfficiënt" van $a(X)$ werken, waarvan je wel mag aannemen dat die ongelijk 0 is.)

   (b) Zo'n element is te schrijven als $aX + b$. Omdat het idempotent is geldt $(aX + b)^2 = aX + b$, dus $a^2X^2 + 2abX + b^2 = aX + b$, dus $a^2 = 0$ en $b^2 = b$. Dus a is nilpotent en b is idempotent en we zijn klaar!?? Nou nee! We hebben nodig dat $a \neq 0$ en dat $b \neq 0, 1$; dit is deel van de definitie. We weten dat $a \neq 0$ omdat $aX + b$ een nilpotent element van graad 1 geacht werd te zijn. Verder, uit $a^2X^2 + 2abX + b^2 = aX + b$ volgt ook nog $2ab = a$. Als $b = 0$ volgt $a = 0$, tegenspraak; als $b = 1$, dan $2a = a$ en opnieuw $a = 0$, tegenspraak. Dus nu is bewezen dat a inderdaad nilpotent is en dat b inderdaad idempotent is.

   (c) Dit is makkelijk: $6 \in \mathbb{Z}/12\mathbb{Z}$ is nilpotent, want $6 \neq 0$ terwijl $6^2 = 36 = 0$. (Het is niet moeilijk in te zien dat 6 het enige nilpotente element van $\mathbb{Z}/12\mathbb{Z}$ is.) Verder is $4 \in \mathbb{Z}/12\mathbb{Z}$ idempotent, want $4 \neq 0, 1$ terwijl $4^2 = 16 = 4$. (Ook 9 is idempotent, en 4 en 9 zijn de enige idempotente elementen van $\mathbb{Z}/12\mathbb{Z}$.)

   (d) Stel $aX + b$ is een idempotent element van $(\mathbb{Z}/12\mathbb{Z})[X]$ van graad 1. Dan $a \neq 0$, $a^2 = 0$, $2ab = a$ en $b^2 = b$. Dus $a = 6$ (dit moet nu wel bewezen worden). Dan levert $a = 2ab$ dat $6 = 12b = 0$, tegenspraak. Als alternatief voor de laatste stap kun je alle b die voldoen aan $b^2 = b$ inspecteren; dit zijn 4, 9, 0 en 1 (moet bewezen worden). Merk op dat je $b = 0$ en $b = 1$ niet mag vergeten hier, tenzij je onderdeel (b) correct had opgelost; gegeven is dat $aX + b$ idempotent is, niet dat b idempotent is.

3. Laat $f = X^2 + 2 \in \mathbb{F}_5[X]$ en laat α een wortel van dit irreducibele polynoom zijn. Laat $K = \mathbb{F}_5(\alpha)$; dit is een eindig lichaam.

   (a) (**2 pt**) Hoeveel elementen heeft K?

   (b) (**4 pt**) Schrijf G voor de multiplicatieve groep $K^* = K - \{0\}$ van K. Bewijs dat α orde 8 heeft in G (dus in het bijzonder dat $\alpha^4 \neq 1$).

   (c) (**4 pt**) Bewijs dat $\alpha + 2$ orde 3 heeft in G.

   (d) (**5 pt**) Bewijs dat G cyclisch is en bepaal een voortbrenger van G.

   (e) (**5 pt**) Bepaal een monisch irreducibel polynoom g van graad 2 in $\mathbb{F}_5[X]$ zo dat het beeld van X in $\mathbb{F}_5[X]/(g)$ een voortbrenger is van de multiplicatieve groep van dat lichaam.

Uitwerking.

(a) f is het minimumpolynoom van α over $\mathbb{F}_5$, dus α heeft graad 2 over $\mathbb{F}_5$, dus $K = \mathbb{F}_5(\alpha)$ is een 2-dimensionale vectorruimte over $\mathbb{F}_5$, dus K heeft $5^2 = 25$ elementen.

(b) G heeft dus 24 elementen. Merk op dat $\alpha^2 = -2 = 3$ in $\mathbb{F}_5$, dus $\alpha^4 = 9 = 4$ en $\alpha^8 = 16 = 1$. De orde van α is dus een deler van 8, maar niet van 4, dus de orde is 8.

(c) $(\alpha+2)^2 = \alpha^2+4\alpha+4 = 4\alpha+2$ en $(\alpha+2)^3 = (\alpha+2)(4\alpha+2) = 4\alpha^2+10\alpha+4 = 12 + 0 + 4 = 16 = 1$. De orde van $\alpha + 2$ is dus een deler van 3 maar niet 1, dus de orde is 3.

(d) G is een abelse groep want K is commutatief. Omdat $\text{ggd}(8, 3) = 1$ is de orde van $\alpha(\alpha+2)$ dan gelijk aan $8 \times 3 = 24$. (Toepassing van een bekend resultaat uit de groepentheorie: als g en h commuteren en de ordes van g en h zijn eindig en relatief priem, dan is de orde van gh gelijk aan het product van de ordes van g en h.) Omdat $|G| = 24$, is G dus cyclisch en $\alpha(\alpha + 2) = 2\alpha + 3$ is een voortbrenger van G.

Als je je het resultaat uit de groepentheorie niet precies herinnert, maar wel denkt dat $\alpha(\alpha + 2)$ orde 24 zal hebben, kun je dit als volgt bewijzen: het is evident dat $(\alpha(\alpha + 2))^{24} = 1$; we hebben nodig dat $(\alpha(\alpha + 2))^d \neq 1$ voor elke deler d van 24. De priemdelers van 24 zijn 2 en 3 en het is voldoende te bewijzen dat de d-de macht niet 1 is voor $d = 24/2$ en $d = 24/3$ (ga dit na: alle echte delers van 24 delen 12 of 8 of allebei). Welnu, $(\alpha(\alpha + 2))^{12} = \alpha^{12}(\alpha + 2)^{12} = \alpha^4 \neq 1$ en $(\alpha(\alpha + 2))^8 = \alpha^8(\alpha + 2)^8 = (\alpha + 2)^2 \neq 1$.

(e) K is isomorf met $\mathbb{F}_5[X]/(g)$ en g is het minimumpolynoom van het beeld van X. We zoeken dus het minimumpolynoom van een voortbrenger van de multiplicatieve groep van het eindige lichaam. In (d) hebben we gezien dat $2\alpha+3$ een voortbrenger is. De Galoisgroep van K over $\mathbb{F}_5$ wordt voortgebracht door het Frobeniusautomorfisme dat α naar $\alpha^5 = -\alpha$ stuurt ($-\alpha$ is de andere wortel van f). Het minimumpolynoom van $2\alpha + 3$ is dan $(X - (2\alpha + 3))(X -$

$(-2\alpha+3) = (X-3)^2-(2\alpha)^2 = X^2-6X+9-4\alpha^2 = X^2-X-3 = X^2+4X+2$. Dus $g = X^2+4X+2$ is één zo'n polynoom.

4. Zij $f = X^3 - 3X + 1$.

   (a) (**4 pt**) Bewijs dat f irreducibel is in $\mathbb{Q}[X]$.

   (b) (**4 pt**) Laat α een wortel zijn van f en laat $K = \mathbb{Q}(\alpha)$. Bewijs dat f in $K[X]$ deelbaar is door $X - \alpha$, met quotiënt $g = X^2 + \alpha X + (\alpha^2 - 3)$.

   (c) (**4 pt**) Bewijs dat $\alpha^2 - 2$ een wortel is van g.

   (d) (**4 pt**) Bewijs dat K een Galois-uitbreiding is van $\mathbb{Q}$.

   (e) (**4 pt**) Bewijs dat er een uniek automorfisme σ van K bestaat met $\sigma(\alpha) = \alpha^2 - 2$. Bepaal de orde van σ.

   Uitwerking.

   (a) f is een monisch derdegraadspolynoom in $\mathbb{Z}[X]$. Het is irreducibel als het geen nulpunten in $\mathbb{Z}$ heeft. Zo'n nulpunt moet de constante term delen, maar 1 en -1 zijn geen nulpunten, dus f is irreducibel in $\mathbb{Z}[X]$ en in $\mathbb{Q}[X]$.

   (b) De deelbaarheid geldt in $K[X]$ omdat K een lichaam is dat $\mathbb{Q}$ en α bevat. Narekenen dat $(X - \alpha)g = f$ bewijst dan dat g het quotiënt is.

   (c) Reken na dat $g(\alpha^2 - 2) = 0$.

   (d) We hebben al twee wortels van f in K, namelijk α en $\alpha^2 - 2$; deze zijn niet gelijk, want $1, \alpha, \alpha^2$ is een basis van K over $\mathbb{Q}$. De derde wortel van f zit dan ook in K, want de drie wortels hebben som 0 (het tegengestelde van de coëfficiënt van X^2 in het monische polynoom f). (De derde wortel is dus $-\alpha^2 - \alpha + 2$.) Dus $K = \mathbb{Q}(\alpha)$ is het splijtlichaam van f over $\mathbb{Q}$. Dus K is Galois over $\mathbb{Q}$, want de drie nulpunten van f zijn verschillend. Of: K is normaal over $\mathbb{Q}$ vanwege St. 8.3.11 en K is zeker separabel over $\mathbb{Q}$, dus K is Galois over $\mathbb{Q}$.

   (e) Elk automorfisme van K is beperkt tot $\mathbb{Q}$ de identiteit, dus een element van $G = \mathrm{Gal}(K/\mathbb{Q})$. Een element van G ligt vast door het beeld van α, wat een wortel van f moet zijn. Dus σ bestaat en is uniek. De orde van G is $3 = [K : \mathbb{Q}]$. De orde van σ is niet 1, dus de orde is 3. Dit is ook direct na te rekenen: $\sigma^3(\alpha) = \alpha$.

5. Zij $f = X^5 - 2 \in \mathbb{Q}[X]$ en laat α de reële wortel van f zijn. Laat ζ een primitieve vijfdemachts eenheidswortel zijn ($\zeta^5 = 1$, $\zeta \neq 1$).

   (a) (**4 pt**) Bewijs dat $L = \mathbb{Q}(\alpha, \zeta)$ het splijtlichaam is van f over $\mathbb{Q}$.

   (b) (**4 pt**) Bewijs dat $[L : \mathbb{Q}] = 20$.

   (c) (**4 pt**) Laat $G = \mathrm{Gal}(L/\mathbb{Q})$. Bewijs dat er elementen σ en τ van G bestaan zo dat

$$\sigma(\alpha) = \alpha\zeta, \qquad \sigma(\zeta) = \zeta\,; \qquad \tau(\alpha) = \alpha, \qquad \tau(\zeta) = \zeta^2.$$

(d) (**3 pt**) Bepaal de ordes van σ en τ en bewijs dat $G = \langle \sigma, \tau \rangle$.

(e) (**5 pt**) Vind twee tussenlichamen M van $L/\mathbb{Q}$ die Galois zijn over $\mathbb{Q}$ en waarvoor geldt $\mathbb{Q} \neq M \neq L$. Bepaal primitieve elementen voor die twee tussenlichamen (d.w.z., die zo'n tussenlichaam voortbrengen over $\mathbb{Q}$).

(f) (**5 pt**) Bewijs dat er precies twee tussenlichamen M van $L/\mathbb{Q}$ bestaan die Galois zijn over $\mathbb{Q}$ en waarvoor geldt $\mathbb{Q} \neq M \neq L$.

Uitwerking.

(a) De wortels van f zijn $\alpha\zeta^k$ met $k = 0, 1, 2, 3, 4$. Het splijtlichaam van f over $\mathbb{Q}$ is dus $\mathbb{Q}(\alpha, \alpha\zeta, \alpha\zeta^2, \alpha\zeta^3, \alpha\zeta^4)$. Dit is bevat in $\mathbb{Q}(\alpha, \zeta)$. Omgekeerd bevat het $\mathbb{Q}(\alpha, \zeta)$ ook, want $\alpha \neq 0$. Dus $L = \mathbb{Q}(\alpha, \zeta)$ is het splijtlichaam van f over $\mathbb{Q}$.

(b) $f \in \mathbb{Z}[X]$ is Eisenstein bij $2 \in \mathbb{Z}$, dus irreducibel in $\mathbb{Q}[X]$. Dus is f het minimumpolynoom van α over $\mathbb{Q}$ en $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$. Anderzijds weten we dat $(X^5 - 1)/(X - 1)$ het minimumpolynoom is van ζ over $\mathbb{Q}$, dus $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$. De graad van L over $\mathbb{Q}$ is dus ten hoogste 20. Maar L bevat zowel $\mathbb{Q}(\alpha)$ als $\mathbb{Q}(\zeta)$, dus $[L : \mathbb{Q}]$ is deelbaar door zowel 5 als 4, dus $[L : \mathbb{Q}] = 20$.

(c) G heeft dus 20 elementen. Anderzijds zijn er voor het beeld van α onder een element van G ten hoogste 5 mogelijkheden, en voor het beeld van ζ ten hoogste 4 mogelijkheden; en een element van G ligt vast door zijn effect op α en ζ. Omdat $|G| = 20$ komen alle mogelijkheden voor! I.h.b. zijn zowel σ als τ uniek bepaalde elementen van G (want $\alpha\zeta$ resp. ζ^2 is een wortel van het minimumpolynoom van α resp. ζ over $\mathbb{Q}$).

(d) Het is vrijwel direct duidelijk dat de orde van σ gelijk is aan 5. Met iets meer werk is in te zien dat de orde van τ gelijk is aan 4. De groep $\langle \sigma, \tau \rangle$ is een ondergroep van G waarvan de orde zowel deelbaar is door de orde van σ als door de orde van τ. De orde van de ondergroep is dus deelbaar door 20. Maar $|G| = 20$, dus $\langle \sigma, \tau \rangle = G$.

(e) Eén zo'n tussenlichaam is $\mathbb{Q}(\zeta)$. Dit is het splijtlichaam over $\mathbb{Q}$ van $X^4 + X^3 + X^2 + X + 1$, dus Galois over $\mathbb{Q}$. Velen meenden dat $\mathbb{Q}(\alpha)$ ook zo'n tussenlichaam is; maar $\mathbb{Q}(\alpha)$ is zeker niet Galois over $\mathbb{Q}$: het bevat maar één wortel van f ! Als we ons realiseren dat de Galoisgroep van $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$ gelijk is aan $\langle \tau \rangle$, dus isomorf met $\mathbb{Z}/4\mathbb{Z}$, komen we verder: de normale ondergroep $\langle \tau^2 \rangle \cong \mathbb{Z}/2\mathbb{Z}$ correspondeert met een deellichaam dat Galois is over $\mathbb{Q}$, namelijk $\mathbb{Q}(\zeta)^{\langle \tau^2 \rangle}$. Omdat $\tau^2(\zeta) = \zeta^4 = \zeta^{-1}$, is $\zeta + \zeta^{-1}$ een element van dit deellichaam. Het zit niet in $\mathbb{Q}$, want dan zou ζ graad 2 over $\mathbb{Q}$ hebben. Dus $\zeta + \zeta^{-1}$ is een primitief element voor dit tussenlichaam, en ζ is natuurlijk een primitief element voor $\mathbb{Q}(\zeta)$.

(f) We moeten bewijzen dat $G = \langle \sigma, \tau \rangle$ precies twee normale ondergroepen ongelijk aan $\{\mathrm{id}\}$ en G bevat. Kijkend naar de effecten op α en ζ zien we dat $\tau\sigma = \sigma^2\tau$. De 20 elementen van G zijn dan $\sigma^i\tau^j$ met $0 \leq i \leq 4$ en $0 \leq j \leq 3$. Een normale ondergroep is een vereniging van conjugatieklassen. De conjugatieklassen van G zijn $\{\sigma^i\tau | 0 \leq i \leq 4\}$, $\{\sigma^i\tau^2 | 0 \leq i \leq 4\}$, $\{\sigma^i\tau^3 | 0 \leq i \leq 4\}$,

$\{\sigma^i | 1 \leq i \leq 4\}$ en $\{\mathrm{id}\}$, zoals niet al te moeilijk is in te zien. Een ondergroep die de klasse van τ of van $\tau^3 = \tau^{-1}$ bevat is gelijk aan G. We zien dat een normale ondergroep ongelijk aan $\{\mathrm{id}\}$ het element σ moet bevatten, en dus $\langle\sigma\rangle$. We zien ook dat $\langle\sigma\rangle$ een normale ondergroep is. Omdat $G/\langle\sigma\rangle \cong \langle\tau\rangle \cong \mathbb{Z}/4\mathbb{Z}$ vinden we nog één andere ondergroep van de gewenste soort, namelijk $\langle\sigma, \tau^2\rangle$.