Tentamen Ringen en Galoistheorie, 30-6-2008, 14-17 uur

Dit is een open boek tentamen. Dat wil zeggen, de dictaten mogen gebruikt worden maar geen andere zaken zoals aantekeningen, uitwerkingen, etc.

Geef een goede onderbouwing van je antwoorden. Succes!

1. (*35 punten, 5 per onderdeel*) Zijn de volgende uitspraken goed of fout? Verklaar je antwoord.

   (a) De ring $\mathbb{Z}[\sqrt{2}]$ heeft een oneindige éénhedengroep.

   (b) De ring $\mathbb{Z}/15\mathbb{Z}$ is een lichaam.

   (c) De ring $\mathbb{Q}[X, Y]$ is een hoofdideaalring.

   (d) Het lichaam $\mathbb{F}_{256}$ heeft graad 4 over $\mathbb{F}_4$.

   (e) Stel L/K is een Galoisuitbreiding en M een tussenlichaam, dat wil zeggen $K \subset M \subset L$. Dan is M/K een Galoisuitbreiding.

   (f) Zelfde situatie als daarnet. Dan is L/M een Galoisuitbreiding.

   (g) Zij L/K een eindige uitbreiding en M_1, M_2 twee tussenlichamen die Galois zijn over K. Dan is $M_1 \cap M_2$ Galois over K.

2. (*25 punten*) We bestuderen de quotientring $R[X]/(X^2-1)$ voor $R = \mathbb{Q}$ en $R = \mathbb{Z}$. In deze opgave verstaan we onder $R \times R$ de productring van R met zichzelf.

   (a) (*7 pt*) Bewijs dat $\mathbb{Q}[X]/(X^2-1)$ en $\mathbb{Q} \times \mathbb{Q}$ ring-isomorf zijn (hint: gebruik Chinese reststelling). Geef een expliciet isomorfisme aan.

   (b) (*7 pt*) Bepaal de elementen e in de ring $\mathbb{Z}[X]/(X^2 - 1)$ zó dat $e^2 = e$.

   (c) (*7 pt*) Bepaal de elementen e in de ring $\mathbb{Z} \times \mathbb{Z}$ zó dat $e^2 = e$. en toon aan dat $\mathbb{Z}[X]/(X^2 - 1)$ en $\mathbb{Z} \times \mathbb{Z}$ niet ring-isomorf zijn.

   (d) (*4 pt*) Nu nemen we $X^2 - X$ in plaats van $X^2 - 1$. Laat zien dat $\mathbb{Z}[X]/(X^2 - X)$ ring-isomorf is met $\mathbb{Z} \times \mathbb{Z}$. Geef een expliciet isomorfisme aan.

ZOZ

3. (*40 punten*) Beschouw het polynoom $f = X^8 - tX^4 + 1 \in \mathbb{Q}(t)[X]$ in de variabelen X, t en zij L het splijtlichaam van f over het grondlichaam $\mathbb{Q}(t)$.

   (a) (*5 pt*) Toon aan dat f irreducibel is als polynoom in $\mathbb{Q}[t, X]$ (hint: kijk naar de graad in t).

   (b) (*5 pt*) Toon nu aan dat f irreducibel is in $\mathbb{Q}(t)[X]$.

   (c) (*5 pt*) Stel dat $\alpha \in L$ een nulpunt is van f, dat wil zeggen: $\alpha^8 - t\alpha^4 + 1 = 0$. Laat zien dat $i\alpha$ en $1/\alpha$ ook nulpunten van f zijn (hierin is $i = \sqrt{-1}$). Bepaal vervolgens alle nulpunten van f in termen van α.

   (d) (*5 pt*) Zij α als daarnet. Laat zien dat $t \in \mathbb{Q}(\alpha)$.

   (e) (*5 pt*) Er is gegeven dat $i \notin \mathbb{Q}(\alpha)$. Bepaal de graad $[L : \mathbb{Q}(t)]$.

   (f) (*9 pt*) Laat zien dat er elementen σ, τ, c van de Galoisgroep $\mathrm{Gal}(L/\mathbb{Q}(t))$ zijn met

   $$\sigma(\alpha) = i\alpha, \quad \sigma(i) = i$$
   $$\tau(\alpha) = 1/\alpha, \quad \tau(i) = i$$
   $$c(\alpha) = \alpha, \quad c(i) = -i$$

   en laat zien dat ze de Galoisgroep voortbrengen.

   (g) (*6 pt*) Wat is het deellichaam van L dat via de Galoiscorrespondentie correspondeert met de ondergroep voortgebracht door σ?

Uitwerkingen

1. Zijn de volgende uitspraken goed of fout? Verklaar je antwoord.

   (a) De ring $\mathbb{Z}[\sqrt{2}]$ heeft een oneindige éénhedengroep.
   Dit is juist, $1 + \sqrt{2}$ is een éénheid (met inverse $\sqrt{2} - 1$) en dus ook alle gehele machten $(1 + \sqrt{2})^n$.

   (b) De ring $\mathbb{Z}/15\mathbb{Z}$ is een lichaam.
   Dit is onjuist want, $3 \cdot 5 \equiv 0 (\mathrm{mod}\ 15)$, en dus zijn 3 en 5 nuldelers. Een lichaam bevat geen nuldelers.

   (c) De ring $\mathbb{Q}[X, Y]$ is een hoofdideaalring.
   Dit is onjuist, want (X, Y) is geen hoofdideaal.

   (d) Het lichaam $\mathbb{F}_{256}$ heeft graad 4 over $\mathbb{F}_4$.
   Dit is juist, er geldt $\mathbb{F}_2 \subset \mathbb{F}_4 \subset \mathbb{F}_{256}$ en verder, $[\mathbb{F}_{256} : \mathbb{F}_2] = 8$ en $[\mathbb{F}_4 : \mathbb{F}_2] = 2$. Dus $[\mathbb{F}_{256} : \mathbb{F}_4] = 8/2 = 4$.

(e) Stel L/K is een Galoisuitbreiding en M een tussenlichaam, dat wil zeggen $K \subset M \subset L$. Dan is M/K een Galoisuitbreiding.
Dit is onjuist, kijk naar het voorbeeld $K = \mathbb{Q}$ M een wortellichaam van $x^3 - 2$ en L het splijtlichaam van $x^3 - 2$.
Alternatief, M/K is Galois dan en slechts dan als $\mathrm{Gal}(L/M)$ een normaaldeler is van $\mathrm{Gal}(L/K)$.

(f) Zelfde situatie als daarnet. Dan is L/M een Galoisuitbreiding.
Dit is juist. De uitbreiding L/M is zeker separabel. Verder is L/K splijtlichaam van een polynoom $f(x) \in K[x]$, dus is het ook splijtlichaam van $f(x) \in M[x]$.

(g) Zij L/K een eindige uitbreiding en M_1, M_2 twee tussenlichamen die Galois zijn over K. Dan is $M_1 \cap M_2$ Galois over K.
Dit is juist, voor elke $\sigma \in \mathrm{Gal}(L/K)$ geldt $\sigma(M_1) = M_1$ en $\sigma(M_2) = M_2$. Dus ook $\sigma(M_1 \cap M_2) = M_1 \cap M_2$.

2. We bestuderen de quotientring $R[X]/(X^2 - 1)$ voor $R = \mathbb{Q}$ en $R = \mathbb{Z}$. In deze opgave verstaan we onder $R \times R$ de productring van R met zichzelf.

(a) Bewijs dat $\mathbb{Q}[X]/(X^2 - 1)$ en $\mathbb{Q} \times \mathbb{Q}$ ring-isomorf zijn. Geef een expliciet isomorfisme aan.
Merk op dat $(X-1)+(X+1) = \mathbb{Q}[X]$, want $(X+1)/2-(X-1)/2 = 1$. Dus geldt volgens de chinese reststelling dat

$$\mathbb{Q}[X]/(X^2 - 1) \simeq \mathbb{Q}[X]/(X - 1) \times \mathbb{Q}[X]/(X + 1).$$

Omdat $\mathbb{Q}[X]/(X - 1) \simeq \mathbb{Q}$ en $\mathbb{Q}[X]/(X + 1) \simeq \mathbb{Q}$ volgt de eerste bewering.

Een isomorfisme wordt gegeven door $f(X) \mapsto (f(1), f(-1))$.

(b) Bepaal de elementen e in de ring $\mathbb{Z}[X]/(X^2 - 1)$ zó dat $e^2 = e$.
Elke restklasse van $\mathbb{Z}[X]/(X^2 - 1)$ heeft een representant van de vorm $aX + b$. We lossen op, $(aX + b)^2 \equiv aX + b (\mathrm{mod}\ X^2 - 1)$. Omdat $(aX+b)^2 \equiv a^2X^2+2abX+b^2 \equiv 2abX+a^2+b^2 (\mathrm{mod}\ X^2-1)$ betekent dit dat $2ab = a$ en $a^2 + b^2 = b$. Uit de eerste vergelijking volgt dat $a(2b - 1) = 0$. Omdat $2b - 1 \neq 0$ voor alle $b \in \mathbb{Z}$ moet gelden dat $a = 0$. Uit de tweede vergelijking volgt dat $b^2 = b$ en dus $b = 0$ of 1. De oplossingen zijn dus 0 en 1.

(c) Bepaal de elementen e in de ring $\mathbb{Z} \times \mathbb{Z}$ zó dat $e^2 = e$. en toon aan dat $\mathbb{Z}[X]/(X^2 - 1)$ en $\mathbb{Z} \times \mathbb{Z}$ niet ring-isomorf zijn.
Stel $e = (a, b)$. Uit $e^2 = e$ volgt nu $(a^2, b^2) = (a, b)$. En dus $a^2 = a, b^2 = b$, waaruit volgt: $a = 0, 1$ en $b = 0, 1$. Antwoord: $(0, 0), (0, 1), (1, 0), (1, 1)$.

Bij isomorfie van $\mathbb{Z}[X]/(X^2-1)$ en $\mathbb{Z}\times\mathbb{Z}$ zou de vergelijking $e^2 = e$ in beide ringen hetzelfde aantal oplossingen moeten hebben. Dat is niet het geval en dus zijn de ringen niet isomorf.

(d) Nu nemen we $X^2 - X$ in plaats van $X^2 - 1$. Laat zien dat $\mathbb{Z}[X]/(X^2 - X)$ ring-isomorf is met $\mathbb{Z} \times \mathbb{Z}$. Geef een expliciet isomorfisme aan.
We passen de chinese reststelling toe op de idealen $I = (X)$ en $J = (X - 1)$. Merk op dat $X - (X - 1) = 1$, dus $I + J = \mathbb{Z}[X]$. Uit de chinese reststelling volgt

$$\mathbb{Z}[X]/(X^2 - X) \simeq \mathbb{Z}[X]/(X) \times \mathbb{Z}[X]/(X - 1)$$

en omdat $\mathbb{Z}[X]/(X) \simeq \mathbb{Z} \simeq \mathbb{Z}[X]/(X - 1)$ volgt onze eerste bewering.
Een isomorfisme wordt gegeven door $f(x) \mapsto (f(0), f(1))$.

3. Beschouw het polynoom $f = X^8 - tX^4 + 1 \in \mathbb{Q}(t)[X]$ in de variabelen X, t en zij L het splijtlichaam van f over het grondlichaam $\mathbb{Q}(t)$.

(a) Toon aan dat f irreducibel is als polynoom in $\mathbb{Q}[t, X]$.
Stel $f = g \cdot h$. De graad van g of h in t moet nul zijn, dus is g of h een polynoom in X, zeg $g(X)$. In het bijzonder deelt $g(X)$ zowel $X^8 + 1$ als X^4. Dus $g(X)$ deelt 1 en is dus constant. Met andere woorden, f heeft alleen triviale delers.

(b) Toon nu aan dat f irreducibel is in $\mathbb{Q}(t)[X]$.
Het lichaam $\mathbb{Q}(t)$ is quotientenlichaam van $\mathbb{Q}[t]$. De ring $\mathbb{Q}[t]$ is ontbindingsring. Uit het Lemma van Gauss volgt dat irreducibiliteit van een monisch (in X) polynoom in $\mathbb{Q}[t, X]$ irreducibiliteit van dat polynoom in $\mathbb{Q}(t)[X]$ impliceert.

(c) Stel dat $\alpha \in L$ een nulpunt is van f, dat wil zeggen: $\alpha^8 - t\alpha^4 + 1 = 0$. Laat zien dat $i\alpha$ en $1/\alpha$ ook nulpunten van f zijn (hierin is $i = \sqrt{-1}$). Bepaal vervolgens alle nulpunten van f in termen van α.
Het eerste deel van de opgave is gewoon narekenen. De verzameling nulpunten wordt,

$$\alpha\ i\alpha,\ -\alpha,\ -i\alpha,\ \frac{1}{\alpha},\ \frac{i}{\alpha}, \frac{-1}{\alpha},\ \frac{-i}{\alpha}.$$

(d) Zij α als daarnet. Laat zien dat $t \in \mathbb{Q}(\alpha)$.
Dit volgt uit

$$\alpha^8 - t\alpha^4 + 1 = 0 \Rightarrow t = \frac{\alpha^8 + 1}{\alpha^4}.$$

(e) Er is gegeven dat $i \notin \mathbb{Q}(\alpha)$. Bepaal de graad $[L : \mathbb{Q}(t)]$.
Uit de voorgaande opgaven is duidelijk dat $L = \mathbb{Q}(i, \alpha)$. merk nu op, $[L : \mathbb{Q}(t)] = [L : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}(t)]$. We weten uit het tweede onderdeel dat $[\mathbb{Q}(\alpha) : \mathbb{Q}(t)] = 8$ en uit het gegeven dat $i \notin \mathbb{Q}(\alpha)$ dat $[L : \mathbb{Q}(\alpha)] = [\mathbb{Q}(i, \alpha) : \mathbb{Q}(\alpha)] = 2$. De graad is dus $2 \cdot 8 = 16$.

(f) Laat zien dat er elementen σ, τ, c van de Galoisgroep $\mathrm{Gal}(L/\mathbb{Q}(t))$ zijn met

$$\sigma(\alpha) = i\alpha, \quad \sigma(i) = i$$
$$\tau(\alpha) = 1/\alpha, \quad \tau(i) = i$$
$$c(\alpha) = \alpha, \quad c(i) = -i$$

en laat zien dat ze de Galoisgroep voortbrengen.
Omdat $L/\mathbb{Q}(t)$ normaal en separabel is bestaat $\mathrm{Gal}(L/\mathbb{Q}(t))$ uit 16 elementen. Een element ρ in deze groep stuurt α naar één van de 8 nulpunten van f en i naar $\pm i$. In totaal zijn hiervoor 16 mogelijkheden, precies correponderend met de orde van de Galoisgroep. Dus moeten er elementen σ, τ, c bestaan met de gewenste eigenschappen. We kunnen laten zien dat de elementen $c^i \tau^j \sigma^k$ met $i = 0, 1,\ j = 0, 1,\ k = 0, 1, 2, 3$ allen verschillend zijn. Dit zijn 16 elementen en dus brengen c, τ, σ de Galoisgroep voort.

(g) Wat is het deellichaam van L dat via de Galoiscorrespondentie correspondeert met de ondergroep voortgebracht door σ?
De ondergroep voortgebracht door σ bevat 4 elementen. Zij L^σ het invariantenlichaam. Dan geldt $[L : L^\sigma] = 4$ en dus ook $[L^\sigma : \mathbb{Q}(t)] = 16/4 = 4$. Het is duidelijk dat L^σ de elementen i en α^4 bevat. Omdat $\mathbb{Q}(\alpha^4, i)$ graad 4 over $\mathbb{Q}(t)$ heeft, moet gelden $L^\sigma = \mathbb{Q}(i, \alpha^4)$.