ALGEBRA I, 2DE KANDIDATUUR WISKUNDE
18 NOVEMBER 1994

When shall we meet again? ...

When the hurlyburly's done
When the battle's lost and won.

THEORIE

Zijn de volgende uitspraken juist of fout? Indien juist geef een korte verklaring of verwijs naar een resultaat uit de nota's. Indien de uitspraak fout is geef een tegenvoorbeeld.

Thrice to thine ...

1. Zij R een ring, $I \lhd R$ en $I \neq R$. Dan bestaat er een ideaal $J \lhd R$, $J \neq R$, zodat R/J een veld is en voor alle $r \in I$ geldt $r \bmod J = 0$.

2. Zij R een hoofdideaal domein en $P \lhd R$ een priemideaal, $P \neq 0$, dan is R/P een veld.

3. Alle domeinen R zijn hoofdideaal domeinen.

and thrice to mine,

4. Stel $f(X), g(X) \in \mathbb{Z}[X]$, $g(X) \neq 0$. Er bestaan polynomen $q(X), r(X) \in \mathbb{Z}[X]$ zodat

$$f(X) = g(X)q(X) + r(X)$$

waarbij $\deg r(X) < \deg g(X)$ of $r(X) = 0$.

5. Als I en J idealen zijn in een ring R dan geldt steeds $I \cap J = IJ$.

6. De volgende ringen zijn isomorf:

$$\mathbb{Z}[X]/(2,X)(3,X^2-X) \cong \mathbb{Z}[X]/(2,X) \times \mathbb{Z}[X]/(3,X^2-X) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

And thrice again, to make up nine.[1]

7. Er zijn geen surjectieve morfismen van een veld naar een ring met echte nuldelers.

[1] Verzen uit: *Macbeth, W.Shakespeare*

8. Zij $\varphi : R \to S$ en $\psi : R \to S'$ ringmorfismen.

a) Als $\ker\varphi = \ker\psi$, hebben φ en ψ isomorfe beelden.

b) Als $\ker\varphi \cong \ker\psi$, hebben φ en ψ isomorfe beelden.

9. Zij R een ring. Elk element $a \in R$ definieert een morfisme

$$\begin{aligned} \varphi_a : R[X] &\to R \\ X &\mapsto a \\ f(X) &\mapsto f(a) \end{aligned}$$

(dit feit hoef je niet te verklaren of te verifiëren). Als $a, b \in R$ en $a \neq b$ dan geldt $\ker\varphi_a \neq \ker\varphi_b$.

Oefeningen

Oef. 1

a) Factoriseer het polynoom $X^4 + X + 1$ over het veld $\mathbb{F}_2$.

b) Factoriseer het polynoom $2X^3 + 2X^2 + 2X + 4$ over $\mathbb{Z}$.

c) Is $(2X^3 + 2X^2 + 2X + 4)\mathbb{Z}[X]$ een priemideaal in $\mathbb{Z}[X]$?

Oef. 2

Zij $f(X) \in \mathbb{F}_p[X]$ stel dat $f(a) = 0$ voor alle $a \in \mathbb{F}_p$. Toon aan dat

$$f(X) = (X^p - X)h(X)$$

met $h(X) \in \mathbb{F}_p[X]$.

Oef. 3

Zij K een veld, $K[X]$ een veeltermring in één variabele over K. Zij I een echt ideaal in $K[X]$.

a) Er bestaat een polynoom $f(X) \in K[X]$ zodat $I = (f(X))$.

b) Zij $A = K[X]/I$. Dan is er een inbedding van K in A.

c) A is een K-vectorruimte.

d) Stel $I = (f(X))$, $d = \deg f(X)$ en $\overline{X}$ is de klasse van X in de quotientring A. Dan is

$$\{1, \overline{X}, \overline{X}^2, \overline{X}^3, \ldots, \overline{X}^{d-1}\}$$

een lineair voortbrengend stel voor de K-vectorruimte A.

e) $\dim_K A = d$.

Oef. 4

Zij R een ring met eenheidselement, R niet noodzakelijk commutatief. Onderstel dat voor alle $a \in R$ geldt $a^2 = a$. Toon aan dat:

a) R een commutatieve ring is van karakteristiek 2.

b) alle priemidealen in R maximale idealen zijn.

c) als P een maximaal ideaal is, is $R/P \cong \mathbb{F}_2$.

d) R een $\mathbb{F}_2$ vectorruimte is.

e) als R bovendien een *eindig dimensionale* $\mathbb{F}_2$-vectorruimte is dan geldt dat R *ring*-isomorf is met

$$\underbrace{\mathbb{F}_2 \times \mathbb{F}_2 \times \ldots \times \mathbb{F}_2}_{n}$$

waarbij $n = \dim_{\mathbb{F}_2} R$.

HINT: Induktie naar de dimensie van R over $\mathbb{F}_2$. Beschouw elementen $e, e-1 \in R$, met $e \neq 0, 1$. Pas de chinese reststelling toe.

ALGEBRA I, 2DE KANDIDATUUR WISKUNDE

20 DECEMBER 1994

THEORIE

Zijn de volgende uitspraken juist of fout? Indien juist geef een korte verklaring of verwijs naar resultaten uit de nota's. Indien de uitspraak fout is geef een tegenvoorbeeld.

1. *Zij R een UFD en K het breukenveld van R.*

a) Zij $r \in R$, r een irreducibel element, dan is Rr een priemideaal in R.

b) Een niet constante veelterm $f(X) \in R[X]$ die irreducibel is over K is irreducibel over R.

c) Een niet constante veelterm $f(X) \in R[X]$ die irreducibel is over R is irreducibel over K.

In een willekeurig domein geldt dat een priemelement irreducibel is. Het omgekeerde is niet waar bv. in de ring $\mathbb{Z}[\sqrt{-5}]$ verifieert men eenvoudig dat $(1+\sqrt{-5})$ een irreducibel element is maar geen priemelement ($(1+\sqrt{-5})$ deelt 6 maar het deelt noch 2 noch 3).

Lemma 1.13.13 stelt echter dat een factorisatie domein een uniek factorisatie domein is als en slechts als elk irreducibel element een priem element is. Dus de uitspraak 1 a) is juist.

De veelterm $2X \in \mathbb{Z}[X]$ is irreducibel over $\mathbb{Q}$ vermits het een veelterm is van de 1ste graad. In $\mathbb{Z}[X]$ heeft $2X$ echter twee irreducibele factoren, namelijk 2 en X.

Uit het lemma van Gauss (cf. 1.13.25, 1.13.27) volgt dat dit soort tegenvoorbeelden voor de uitspraak 1 b) de enige zijn. Het lemma van Gauss zegt namelijk dat *primitieve* veeltermen over een UFD, R, irreducibel zijn in $R[X]$ als en slechts als ze irreducibel zijn in $K[X]$. Hieruit volgt dat uitspraak 1c) waar is omdat een irreducibele veelterm over een UFD, noodzakelijk een primitieve veelterm is.

2. *Zij K een veld en L een velduitbreiding van K. Zij*

$$\varphi : K[X,Y] \to L$$

een K-algebra homomorfisme met $\ker\varphi = P$. Stel P is een niet nul priemideaal in $K[X,Y]$ dat niet maximaal is.

Dan is:

a) $\varphi(X)$ of $\varphi(Y)$ transcendent over K.

b) de verzameling $\{\varphi(X), \varphi(Y)\}$ algebraïsch afhankelijk over K.

Het beeld $A = K[\varphi(X), \varphi(Y)]$ van het K-algebra homomorfisme, is isomorf (als K-algebra) met $K[X,Y]/\ker\varphi$ (cf. de isomorfie stelling 2.1.10). Als de beide elementen $\varphi(X)$ en $\varphi(Y)$ algebraïsch zijn over K dan is K-algebra $A = K[\varphi(X), \varphi(Y)]$ algebraïsch over K (cf. gevolg 2.3.5). Vermits A een deel is van het veld L, heeft A geen nuldelers en dus impliceert gevolg 2.4.2 dat A zelf een veld is. Maar dan is $\ker\varphi$ en maximaal ideaal, wat in tegenstrijd is met de hypothesen.

Als de verzameling $\{\varphi(X), \varphi(Y)\}$ algebraïsch onafhankelijk is dan bepaalt φ een isomorfisme tussen de K-algebra A en de veelterm algebra $K[X,Y]$. Dit impliceert dat $\ker\varphi = 0$ (cf. lemma 2.2.8). Wat eveneens in tegenspraak is met de hypothesen.

Vb. Zij $\varphi : K[X,Y] \to K(Y)$ het K-morfisme dat $X \mapsto 0$ en $Y \mapsto Y$. Dan is de kern van φ het priemideaal voortgebracht door X.

3. *Zij $f(X)$ een irreducibel monisch polynoom over een veld K, met* $\deg f(X) = 2n+1$. *Zij α een wortel van $f(X)$ in een algebraïsche sluiting van K.*

a) $f(X)$ is het minimaal polynoom van α.

b) Alle wortels van $f(X)$ zijn elementen van $K(\alpha)$.

c) $K(\alpha^2) = K(\alpha)$.

Als α een wortel is van $f(X)$ dan moet $f(X)$ een veelvoud zijn van het minimaal polynoom van α (cf. definitie 2.3.6). Vermits $f(X)$ monisch en irreducibel is kan dit enkel als $f(X)$ gelijk is aan het minimaal polynoom van α.

De veelterm $X^3 - 2$ is irreducibel over het veld $\mathbb{Q}$ dit volgt uit het criterium van Eisenstein (cf. 1.13.32) en het lemma van Gauss (cf. 1.13.25, 1.13.27). Het veld $\mathbb{Q}(\alpha)$ heeft graad 3 over $\mathbb{Q}$ (cf. stelling 2.3.7). Stel dat $\mathbb{Q}(\alpha)$ alle wortels van $X^3 - 2$ bevat. Dan bevat $\mathbb{Q}(\alpha)$ ook het element $\alpha^{-1} \cdot \alpha e^{\frac{2\pi i}{3}} = e^{\frac{2\pi i}{3}}$, i.e. de derde eenheidswortel $e^{\frac{2\pi i}{3}} \in \mathbb{Q}(\alpha)$. Het minimaal polynoom van $e^{\frac{2\pi i}{3}}$ is $X^2 + X + 1$ en dus is $[\mathbb{Q}(e^{\frac{2\pi i}{3}}) : \mathbb{Q}] = 2$. Maar $\mathbb{Q}(e^{\frac{2\pi i}{3}}) \subset \mathbb{Q}(\alpha)$ dus zou 2 een deler moeten zijn van 3 vanwege de produkt formule (cf. stelling 2.4.4). Dit geeft een tegenvoorbeeld voor 1 b).

De velden waarvoor de uitspraak 1 b) geldt zijn per definitie de normale uitbreidingen van K, cf. 3.1.22.

Merk op dat $X^2 - \alpha^2$ het element α als wortel heeft. Het minimaal polynoom van α over het veld $K(\alpha^2)$ is dus van graad ≤ 2. We moeten aantonen dat deze graad 1 is. Stel

$[K(\alpha) : K(\alpha^2)] = 2$ dan volgt uit de produkt formule (cf. stelling 2.4.4) dat 2 een deler is van $[K(\alpha) : K] = 2n + 1$. Dit is onmogelijk dus moet $[K(\alpha) : K(\alpha^2)] = 1$.

Oefeningen

1. *Zij $\alpha \in \mathbb{C}$ een wortel van de veelterm*

$$X^3 + 26X + (3 + 2i)$$

over $\mathbb{Q}(i)$.

Bepaal het minimaal polynoom van α over $\mathbb{Q}$.

De ring $\mathbb{Z}[i]$ is een HID en dus een UFD. In $\mathbb{Z}[i]$ is

$$26 = 2 \cdot 13 = 2 \cdot (3 + 2i)(3 - 2i).$$

De getallen $3 + 2i$ en $3 - 2i$ zijn irreducibel in $\mathbb{Z}[i]$ vermits hun norm een priemgetal in $\mathbb{Z}$ is, cf. oefening 1.13.12. Uit het irreducibiliteitscriterium van Eisenstein volgt dat

$$f(X) = X^3 + 26X + (3 + 2i)$$

een irreducibel polynoom is over $\mathbb{Z}[i]$ en dus ook over $\mathbb{Q}(i)$ (cf. 1.13.27) Als we het polynoom $X^3 + 26X + (3 + 2i)$ vermenigvuldigen met zijn complex toegevoegde $X^3 + 26X + (3 - 2i)$ dan bekomen we een polynoom $g(X)$ van graad 6 in $\mathbb{Q}(i)$ waarvan de coëfficiënten invariant zijn onder complexe toevoeging en dus in $\mathbb{Q}$ liggen.

Vermits $f(X)$ een irreducibel polynoom is over $\mathbb{Q}(i)$ heeft $\mathbb{Q}(i, \alpha)$ graad 3 over $\mathbb{Q}(i)$ en dus graad 6 over $\mathbb{Q}$ (produkt formule cf. 2.4.4). De graad van het minimaal polynoom van α over $\mathbb{Q}$ is dus een deler van 6 (opnieuw produkt formule). Maar deze graad $[\mathbb{Q}(\alpha) : \mathbb{Q}] > 3$ vermits het minimaal polynoom van α over $\mathbb{Q}(i)$ graad 3 heeft en niet over $\mathbb{Q}$ gedefinieerd is. Dus de graad van het minimaal polynoom van α over $\mathbb{Q}$ is 6. Nu is $g(X)$ een polynoom met α als wortel en $\deg g(X) = 6$, $g(X)$ moet dus het minimaal polynoom zijn van α over $\mathbb{Q}$.

$(g(X) = X^6 + 2^2 \cdot 13X^4 + 2.3X^3 + 2^2 \cdot 13^2X^2 + 2^2 \cdot 3 \cdot 13X + 13.)$

2. *a) Toon aan dat het eindig veld $\mathbb{F}_8$ isomorf is met $\mathbb{F}_2(\alpha)$, waarbij α een wortel is van de vergelijking $X^3 + X + 1 = 0$.*

b) Factoriseer $X^2 + X + \alpha$ over het veld $\mathbb{F}_8$.

Het voldoende om op te merken dat X^3+X+1 een irreducibel polynoom is over $\mathbb{F}_2$. Dit geldt vermits nog 0 nog 1 een wortel is van $X^3+X+1 \in \mathbb{F}_2[X]$. $\mathbb{F}_2(\alpha)$ is dus een veld uitbreiding van graad 3 over $\mathbb{F}_2$, heeft dus 8 elementen en moet dus het veld $\mathbb{F}_8$ zijn.

Vermits

$$\alpha+\alpha^2+\alpha^4 = \alpha(1+\alpha+\alpha^3) = 0$$

volgt dat $X^2+X+\alpha$ een wortel heeft in $\mathbb{F}_8$ (cf. handgeschreven nota's). In dit geval zien we echter onmiddellijk dat α^2 een wortel is van $X^2+X+\alpha$. De andere wortel, $\alpha+1$ bekomen we bijvoorbeeld door $X^2+X+\alpha$ te delen door $X-\alpha$. (Dit volgt eveneens uit de theorerische beschouwingen in de nota's over eindige velden).

3. *Beschouw het polynoom* $f(X) = X^4-2$ *over* $\mathbb{Q}$.

a) Ontbind $f(X)$ *in irreducibele factoren over* $\mathbb{Q}$.

b) Zij $\alpha \in \mathbb{C}\setminus\mathbb{R}$ *een wortel van* $f(X)$. *Ontbind* $f(X)$ *in irreducibele factoren over* $\mathbb{Q}(\alpha,i)$.

c) Ontbind $f(X)$ *in irreducibele factoren over* $\mathbb{Q}(\alpha)$.

d) Bepaal $Aut_{\mathbb{Q}}(\mathbb{Q}(\alpha))$, $Aut_{\mathbb{Q}}(\mathbb{Q}(\alpha,i))$, $Hom_{\mathbb{Q}}(\mathbb{Q}(\alpha),\mathbb{C})$, $Hom_{\mathbb{Q}}(\mathbb{Q}(\alpha,i),\mathbb{C})$.

e) Bepaal het minimaal polynoom van $(1+i)\alpha$ *over* $\mathbb{Q}$.

f) Van welke deelgroep $H < Aut_{\mathbb{Q}}(\mathbb{Q}(\alpha,i))$ *is* $\mathbb{Q}((1+i)\alpha)$ *het fixveld?*

Uit het criterium van Eisenstein volgt dat X^4-2 irreducibel is over $\mathbb{Z}$ en dus ook over $\mathbb{Q}$ (lemma van Gauss). De machten van het getal $i \in \mathbb{C}$ geven alle vierde eenheidswortels dus de wortels van $f(X)$ zijn:

$$\alpha, -\alpha, i\alpha, -i\alpha.$$

De factorisatie over $\mathbb{Q}(\alpha,i)$ wordt dan

$$X^4-2 = (X-\alpha)(X+\alpha)(X-i\alpha)(X+i\alpha).$$

Dit geeft

$$(X-\alpha^2)(X+\alpha^2)$$

als factorisatie over $\mathbb{Q}(\alpha)$. Hierbij moeten we opmerken dat $\mathbb{Q}(\alpha,i) \neq \mathbb{Q}(\alpha)$. Moest de gelijkheid wel gelden dan zou eveneens $\mathbb{Q}(\alpha,i) = \mathbb{Q}(i\alpha)$. Dit laatste is onmogelijk vermits $i\alpha \in \mathbb{R}$ (vermits $\alpha \notin \mathbb{R}$ en X^4-2 een wortel heeft in $\mathbb{R}$). Er zijn $[\mathbb{Q}(\alpha,i) : \mathbb{Q}] = 8$

inbeddingen van $\mathbb{Q}(\alpha, i)$ in $\mathbb{C}$. Namelijk

$$\begin{array}{lcl}
\sigma_1 & = & id_{\mathbb{Q}(\alpha,i)} \\
\sigma_2 & : & \alpha \to i\alpha; i \to i \\
\sigma_3 & : & \alpha \to -\alpha; i \to i \\
\sigma_4 & : & \alpha \to -i\alpha; i \to i \\
\sigma_5 & : & \alpha \to \alpha; i \to -i \\
\sigma_6 & : & \alpha \to i\alpha; i \to -i \\
\sigma_7 & : & \alpha \to -\alpha; i \to -i \\
\sigma_8 & : & \alpha \to -i\alpha; i \to -i
\end{array}$$

Dit geeft

$$\begin{array}{lcl}
\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\alpha,i),\mathbb{C}) = \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha,i)) & = & \{\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_5,\sigma_6,\sigma_7,\sigma_8\} \\
\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\alpha),\mathbb{C}) & = & \{\sigma_1,\sigma_2,\sigma_3,\sigma_4\} = \{\sigma_5,\sigma_6,\sigma_7,\sigma_8\} \\
\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha)) & = & \{id_{\mathbb{Q}(\alpha)}\}
\end{array}$$

(De elementen van $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\alpha),\mathbb{C})$ worden bekomen als de restricities van de σ_i tot $\mathbb{Q}(\alpha)$.)

De automorfisme groep (Galois groep) $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha,i))$ is de diheder groep met 8 elementen. Dit volgt uit het feit dat de groep een element van orde 4 heeft, σ_2, en niet commutatief is, $\sigma_5 \circ \sigma_2 \neq \sigma_2 \circ \sigma_5$.

Om het minimaal polynoom van $(1+i)\alpha$ te vinden beschouwen we alle toegevoegden $\sigma_1((1+i)\alpha), \ldots, \sigma_8((1+i)\alpha)$. Dit geeft 4 verschillende elementen

$$(1+i)\alpha, (i-1)\alpha, (-1-i)\alpha, (1-i)\alpha.$$

Het minimaal polynoom van $(1+i)\alpha$ zal dus graad 4 hebben en is gelijk aan

$$(X-(1+i)\alpha)(X-(i-1)\alpha)(X-(-1-i)\alpha)(X-(1-i)\alpha) = X^4+8.$$

Het fixveld van de deelgroep $H = \{\sigma_1, \sigma_6\}$ bevat $\mathbb{Q}((1+i)\alpha)$. Door de graden te vergelijken zien we dat $\mathbb{Q}((1+i)\alpha)$ het fixveld is van $\{\sigma_1, \sigma_6\}$, ($[\mathbb{Q}(\alpha,i)^H : \mathbb{Q}] = 2$, stelling 2.6.16.