## Evaluatie algebra, 12 november 1996.

---

Zijn de volgende uitspraken (1-5) juist of fout? (Argumenteer uw antwoord.)

1. $H, I, J$ idealen in $R$. Dan is

$$H \cap (I + J) = (H \cap I) + (H \cap J).$$

*Niet waar. In de veeltermenring* $\mathbb{Q}[X, Y]$, *is* $(X) \cap ((X - Y) + (X + Y)) = (X)$ *maar* $X \notin (X) \cap (X - Y) + (X) \cap (X + Y) = (X^2 - XY) + (X^2 + XY)$.

2. Zij $R$ een Noethers domein waarin elk ideaal dat voortgebracht is door 2 elementen een hoofdideaal is. Dan is $R$ een HID.

*Waar. Elk ideaal is eindig voortgebracht omdat de ring Noethers is. Met induktie volgt dan uit de andere voorwaarde dat alle idealen eindig voortgebracht zijn.*

3. Zij $\sigma : \mathbb{C} \to \mathbb{C}$ een ringmorfisme en $\alpha \in \mathbb{C}$ een algebraïsch element over $\mathbb{Q}$ dan is $\sigma(\alpha)$ ook algebraïsch over $\mathbb{Q}$.

*Waar. Zij* $\sum a_i \alpha^i = 0$ *met* $a_i \in \mathbb{Q}$. *Dan is* $0 = \sigma(\sum a_i \alpha^i)) = \sum \sigma(a_i)\sigma(\alpha^i) = \sum a_i \sigma(\alpha^i)$. *De eerste gelijkheid vermits* $\sigma$ *een morfisme is en de tweede gelijkheid vermits elk morfisme op* $\mathbb{Q}$ *gelijk is aan de identiteit. We vinden zelfs dat* $\sigma(\alpha)$ *een wortel is van dezelfde veeltermen waarvan* $\alpha$ *een wortel is.*

4. Elk rationaal getal $a \in \mathbb{Q}$ is algebraïsch over $\mathbb{Z}$.

*Waar. Zij* $\frac{a}{b} \in \mathbb{Q}$ *dan is* $\frac{a}{b}$ *een wortel van* $bX - a$.

5. Zij $f(X)$ een irreducibele veelterm over $\mathbb{Q}$ en $a, b \in \mathbb{C}$ wortels van $f(X)$.

   a) Dan is $\mathbb{Q}[a]$ een veld.

   b) Dan is $\mathbb{Q}[a] \cong \mathbb{Q}[b]$.

*Beide waar.* $\mathbb{Q}[a] \cong \mathbb{Q}[b] \cong \mathbb{Q}[X]/(f(X))$. *Het laatste is een veld vermits* $f(X)$ *irreducibel is en elke irreducibele veelterm een maximaal ideaal in* $\mathbb{Q}[X]$ *voortbrengt.*

*Opmerking. Als* $f(X)$ *niet irreducibel is, is* $\mathbb{Q}[a]$ *nog steeds een veld (a is ook de wortel van een irreducibele veelterm) maar* $\mathbb{Q}[a] \ncong \mathbb{Q}[b]$. *Voorbeeld* $f(X) = (X - 1)(X^2 + 1)$, $\mathbb{Q}[1] \ncong \mathbb{Q}[i]$.

---

6. Zijn $a = 1 - 7i \in \mathbb{Z}[i]$ en $b = 2 - 2i \in \mathbb{Z}[i]$. Bepaal $\text{ggd}(a, b)$ en $s, t \in \mathbb{Z}[i]$ zodat $\text{ggd}(a, b) = sa + tb$. (Recursie gebruiken)

*Enkele stappen uit de berekening:* $c_1 = 1, c_2 = 0, d_1 = 0, d_2 = 1$

$\frac{1-7i}{2-2i} = \frac{(1-7i)(2+2i)}{(2-2i)(2+2i)} = \frac{4-3i}{2}$.

*Ga na op een tekening dat voor het quotient* $q \in \mathbb{Z}[i]$, $2 - i$ *(of* $2 - 2i$*) kan gekozen worden. Dan is*

$$1 - 7i = (2 - 2i)q + r = (2 - 2i)(2 - i) + (-1 - i).$$

$r_1 = c_1 - qd_1 = 1, r_2 = c_2 - qd_2 = -2 + i$

*Stel nu* $c_1 = d_1 = 0, c_2 = d_2 = 1, d_1 = r_1 = 1, d_2 = r_2 = -2 + i$.

*Vermits* $2 - 2i$ *deelbaar is door* $-1 - i$ *volgt* $ggd(1 - 7i, 2 - 2i) = -1 - i$ *en*

$$c_2(1 - 7i) + d_2(2 - 2i) = 1 \cdot (1 - 7i) + (-2 + i)(2 - 2i) = -1 - i.$$

7. Factoriseer $X^4 + 2X^3 + X^2 + 1$ over $\mathbb{F}_5$.

*Enkele stappen uit de berekening:*

*Zij* $f(X) = X^4 + 2X^3 + X^2 + 1$. *Vermits* $f(1) = 5 = 0$ *en* $f(-2) = 5 = 0$ *volgt*

$$X^4 + 2X^3 + X^2 + 1 = (X - 1)(X + 2)(X^2 + aX + b).$$

*De coëfficiënten in het linkerlid vergelijken met deze in het rechterlid geeft:*

$$\begin{aligned} a + 1 &= 2 \\ b - 2 + a &= 1 \\ -2a + b &= 0 \\ -2b &= 1 \end{aligned}$$

*Hieruit vindt men* $a = 1$ *en* $b = 2$. *Dus*

$$X^4 + 2X^3 + X^2 + 1 = (X - 1)(X + 2)(X^2 + X + 2).$$

8. Zij $R$ een ring en $I, I_1, I_2, \ldots, I_n$ idealen in $R$. Zij $\text{Rad}(I) = \{r \in R | r^n \in I \text{ voor een } n > 0\}$ het radikaal van $I$.

a) Toon aan dat:

i) $\text{Rad}(\text{Rad}(I)) = \text{Rad}(I)$.

ii) $\mathrm{Rad}(I_1 I_2 \cdots I_n) = \mathrm{Rad}(\cap_{j=1}^n I_j) = \cap_{j=1}^n \mathrm{Rad}(I_j)$.

iii) $\mathrm{Rad}(I^m) = \mathrm{Rad}(I)$.

b) Stel $J \subset \mathrm{Rad}(I)$ is een eindig voortgebracht ideaal in $R$. Bewijs dan dat er een $n > 0$ bestaat zodat $J^n \subset I$.

*i) Zij $a \in Rad(I)$ uit $Rad(Rad(I)) = \{r \in R | r^n \in Rad(I)\}$ volgt dan onmiddellijk $Rad(I) \subset Rad(Rad(I))$.*

*Zij $a \in Rad(Rad(I))$, dan is $a^n \in Rad(I)$ voor een $n \in \mathbb{N}$ en dus $(a^n)^m \in I$ voor een $m \in \mathbb{N}$. Dus $a^{nm} \in I$, wat betekent dat $a \in Rad(I)$.*

*ii) $I_1 \cdots I_n \subset \cap_{j=1}^n I_j$. Uit de definite van het radikaal volgt $Rad(I_1 I_2 \cdots I_n) \subset Rad(\cap_{j=1}^n I_j)$.*

*Zij nu $a \in Rad(\cap_{j=1}^n I_j)$ dan is er een getal $m$ zodat $a^m \in \cap_{j=1}^n I_j$. Dus $a^m \in I_j$ voor alle $j = 1, \ldots, n$. Dit impliceert dat $a^{mn} \in I_1 \cdots I_n$. Dus $Rad(\cap_{j=1}^n I_j) \subset Rad(I_1 I_2 \cdots I_n)$.*

*Zij $a \in Rad(\cap_{j=1}^n I_j)$ dan is $a^m \in \cap_{j=1}^n I_j$ voor zekere $m$. Dus $a^m \in I_j$ voor alle $j$. Dit impliceert $a \in Rad(I_j)$ voor alle $j$. Hieruit volgt de inclusie $Rad(\cap_{j=1}^n I_j) \subset \cap_{j=1}^n Rad(I_j)$.*

*Zij $a \in \cap_{j=1}^n Rad(I_j)$ dan is $a \in Rad(I_j)$ voor alle $j$. Er is dus een getal $m_j$ zodat $a^{m_j} \in I_j$, voor alle $j$. Dan volgt dat $a^{m_1 + \cdots m_n} \in \cap_{j=1}^n I_j$. Dit impliceert $a \in Rad(\cap_{j=1}^n I_j)$. Dit bewijst de andere inclusie.*

*iii) Volgt uit punt ii) met $I_j = I$ voor alle $j$.*

*b) Bew: $J = Rx_1 + \cdots + Rx_m$. Dan is $J^n$ voortgebracht door alle "monomen" van graad $n$ in $x_1, \ldots, x_m$. Wegens $J \subset Rad(I)$, bestaat er voor alle $i = 1, \ldots, m$ een $n_i$ zodat $x_i^{n_i} \in I$. Neem nu $n = \sum_{i=1}^m n_i$. Dan is*

$$J^n \text{ voortgebracht door de monomen } x_1^{i_1} \cdots x_m^{i_m} \text{ met } \sum_{j=1}^m i_j = n = n_1 + \cdots + n_m.$$

*Neem zulk een voortbrenger $x_1^{i_1} \cdots x_m^{i_m}$. Dan is er een $j \in \{1, \ldots, m\}$ zodat $i_j \geq n_j$. Dus*

$$x_1^{i_1} \cdots x_m^{i_m} = x_j^{n_j}(x_1^{i_1} \cdots x_j^{i_j - n_j} \cdots x_m^{i_m}) \in I.$$

*Vermits elke voortbrenger van $J^n$ een element is uit $I$, volgt $J^n \subset I$.*

9. Zij $R$ een ring en $I$ een ideaal in $R$. Zij $M$ een eindig voortgebracht $R$-moduul. Zij, per definitie, $IM$ de verzameling van alle eindige sommen van elementen, $am$, met $a \in I$ en $m \in M$.

a) Toon aan dat $IM$ een deelmoduul is van $M$.

b) Toon aan dat als $I$ bevat is in alle maximale idealen van $R$, uit $IM = M$ volgt dat $M = 0$.

## Evaluatie algebra, 17 december 1996.

---

1. Beschrijf schematisch alle deelvelden van

   a) $\mathbb{F}_{2^{12}}$

   b) $\mathbb{F}_{3^{12}}$.

2. Factoriseer de volgende veeltermen:

   a) $X^3 - X - 1$ over $\mathbb{F}_3$.

   b) $X^4 - X^3 - 4X^2 - 6X + 10$ over $\mathbb{Z}$.

   c) $X^4 + (2+i)X + 5$ over $\mathbb{Z}[i]$.

HINT: MAAK GEBRUIK VAN DE IRREDUCIBILITEITS CRITERIA, BLZ. 147.

3. Zij $\alpha \in \mathbb{C}$ een wortel van $X^4 + (2+i)X + 5$. Bepaal de minimaal veelterm van $\alpha$ over $\mathbb{Q}$.

4. Bepaal de wortels van de veelterm

$$\beta X^2 + \beta^2 X + \beta^5$$

in $\mathbb{F}_2^a$. Hierbij is $\beta \in \mathbb{F}_2^a$ zodat $\beta^3 + \beta + 1 = 0$.

5. Karakteriseer de priemgetallen $p \in \mathbb{Z}$ die ook priemelementen zijn in de ring van gehelen van de imaginair kwadratische uitbreiding $\mathbb{Q}[\sqrt{-6}]$.

6. Karakteriseer alle priemgetallen in $\mathbb{Z}$ van de vorm $a^2 + 2b^2$ met $a, b \in \mathbb{Z}$.

---

Zijn de volgende uitspraken (7-14) juist of fout? (Argumenteer uw antwoord.)

7. Zij $L/K$ een eindige uitbreiding en $K \subset L \subset M$ een toren van velduitbreidingen. Een element $\alpha \in M$ dat algebraïsch is over $L$ is ook algebraïsch over $K$.

8. Zij $\alpha \in K^a$ een algebraïsch element over een veld $K$. Zij $K \subset L$ een velduitbreiding.

   a) De minimaal veelterm $f_{\alpha,K}(X)$ van $\alpha$ over $K$ is een veelvoud van de minimaalveelterm $g_{\alpha,L}(X)$ van $\alpha$ over $L$.

b) $f_{\alpha,K}(X)$ en $g_{\alpha,L}(X)$ zoals in a). Dan is $\deg f_{\alpha,K}(X) > g_{\alpha,L}(X)$.

9. Zij $f(X)$ een irreducibele veelterm over een veld $K$ en $g(X)$ een willekeurige veelterm over $K$ zodat $f(X)$ en $g(X)$ een wortel $\alpha \in K^a$ gemeen hebben. Dan zijn alle wortels van $f(X)$ ook wortels van $g(X)$.

10. Zij $f(X)$ een primitieve veelterm over $\mathbb{Z}$ (i.e. $\text{cont}(f(X)) = 1$). Dan is $f(X)$ irreducibel over $\mathbb{Z}$ als en slechts als $f(X)$ irreducibel is over $\mathbb{Q}$.

11. Zij $R$ een ring en $I$ een ideaal in $R$.

a) Als $I$ het produkt is van verschillende maximale idealen in $R$, dan is $R/I$ isomorf met het direkt produkt van velden.

b) Zelfde bewering maar nu met $I$ het produkt van maximale idealen. (Dus het woord "veschillende" weglaten.)

12. Een velduitbreiding is algebraïsch als en slecht als het een eindige uitbreiding is.

13.

a) Zij $\sigma : K \to K$ een automorfisme van velden. Zij $f(X) = \sum a_i X^i \in K[X]$ een irreducibele veelterm over $K$. Definieer $\sigma(f)(X) = \sum \sigma(a_i) X^i \in K[X]$. Dan is $\sigma(f)(X)$ ook irreducibel over $K$.

b) Zij $\sigma : K \to L$ een morfisme van velden. Zij $f(X) = \sum a_i X^i \in K[X]$ een irreducibele veelterm over $K$. Definieer $\sigma(f)(X) = \sum \sigma(a_i) X^i \in L[X]$. Dan is $\sigma(f)(X)$ ook irreducibel over $L$.

14. Zij $f(X) \in \mathbb{F}_p[X]$ een irreducibele veelterm met $\deg f(X) = 4$ en $g(X) \in \mathbb{F}_p[X]$ een willekeurige veelterm met $\deg g(X) = 2$. Zij $\alpha \in \mathbb{F}_p^a$ een wortel van $f(X)$ en $\beta \in \mathbb{F}_p^a$ een wortel van $g(X)$. Dan geldt

$$\beta \in \mathbb{F}_p(\alpha).$$

## Evaluatie algebra, 17 december 1996.

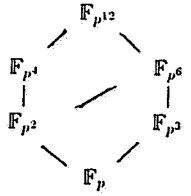
---

1. Beschrijf schematisch alle deelvelden van

a) $\mathbb{F}_{2^{12}}$

b) $\mathbb{F}_{3^{12}}$.

*Voor elk priem getal $p$ geldt (structuur stelling van de eindige velden):*




2. Factoriseer de volgende veeltermen:

a) $X^3 - X - 1$ over $\mathbb{F}_3$.

*De veelterm is irreducibel vermits er geen wortels zijn in $\mathbb{F}_3$.*

b) $X^4 - X^3 - 4X^2 - 6X + 10$ over $\mathbb{Z}$.

$(X-1)(X^3 - 4X - 10)$, *de derde graads factor is irreducible vermits modulo 3 we de veelterm $X^3 - X - 1$ bekomen.*

c) $X^4 + (2+i)X + 5$ over $\mathbb{Z}[i]$.

*Deze veelterm is irreducibel vanwege het criterium van Eisenstein, $5 = (2+i)(2-i)$. Verder zijn $(2-i)$ en $(2+i)$ verschillende priemen in $\mathbb{Z}[i]$.*

3. Zij $\alpha \in \mathbb{C}$ een wortel van $X^4 + (2+i)X + 5$. Bepaal de minimaal veelterm van $\alpha$ over $\mathbb{Q}$.

*De minimaal veelterm van $\alpha$ over $\mathbb{Q}$ is van graad 8. Dit volgt uit oefening 11 en de produkt formule. Dus*

$$(X^4 + (2+i)X + 5)(X^4 + (2-i)X + 5) = X^8 + 4X^5 + 10X^4 + 5X^2 + 20X + 25$$

*is de minimaal veelterm van $\alpha$.*



4. Bepaal de wortels van de veelterm

$$\beta X^2 + \beta^2 X + \beta^5$$

in $\mathbb{F}_2^a$. Hierbij is $\beta \in \mathbb{F}_2^a$ zodat $\beta^3 + \beta + 1 = 0$.

*3 wegdelen geeft de vergelijking:*

$$X^2 + \beta X + \beta^4.$$

*Transformeren via $X = \beta Y$ geeft*

$$Y^2 + Y + \beta^2.$$

*Het spoor van $\beta^2$ is nul, dus er is een wortel in $\mathbb{F}_8$. Vermits 1 spoor 1 heeft, bekomen we met de formule voor de wortels : $\beta^4$ en $\beta^4 + 1$. De oplossingen van de oorspronkelijke vergelijking zijn dan $\beta^5 = \beta^2 + \beta + 1$ en $\beta^5 + \beta = \beta^2 + 1$.*

5. Karakteriseer de priemgetallen $p \in \mathbb{Z}$ die ook priemelementen zijn in de ring van gehelen van de imaginair kwadratische uitbreiding $\mathbb{Q}(\sqrt{-6})$.

*$p \in \mathbb{Z}$ is priem in $\mathbb{Z}[\sqrt{-6}]$ dan en slechts dan als*

$$\mathbb{Z}[\sqrt{-6}]/(p) \cong \mathbb{F}_p[X]/(X^2 + 6)$$

*een domein is. Dus als en slechts als $-6$ geen kwadraatrest is modulo $p$, i.e. $(\frac{-6}{p}) = -1$. Voor $p = 2$ en $p = 3$ is 0 een tweevoudige wortel in $\mathbb{F}_p$. Voor $p \neq 2$ en $p \neq 3$ vinden we met de wederkerigheidswet:*

$$(\frac{-6}{p}) = -1$$

*dan en slechts dan als*

$$p \equiv \pm 3 \bmod 8 \text{ en } p \equiv 1 \bmod 3$$

*of*

$$p \equiv \pm 1 \bmod 8 \text{ en } p \equiv -1 \bmod 3.$$

*Met behulp van de chinese reststelling vinden we dat $p$ een priemelement is in $\mathbb{Z}(\sqrt{-6})$ als en slechts als*

$$p \equiv 13, 17, 19, 23 \bmod 24.$$

6. Karakteriseer alle priemgetallen in $\mathbb{Z}$ van de vorm $a^2 + 2b^2$ met $a, b \in \mathbb{Z}$

*Een priemgetal $p$ is van de vorm $a^2 + 2b^2$ als en slecht als $p$ factoriseert in $\mathbb{Z}[\sqrt{-2}]$, namelijk*

$$p = (a + b\sqrt{-2})(a - b\sqrt{-2}).$$

*Bv. $2 = 0 + 2 \cdot 1$. We zoeken dus nog de oneven priemen $p$ waarvoor $(\frac{-2}{p}) = 1$. Dit geldt als en slecht als*

$$p \equiv 1, 3 \bmod 8.$$

Zijn de volgende uitspraken (1-5) juist of fout? (Argumenteer uw antwoord.)

7. Zij $K \subset L$ een eindige uitbreiding en $K \subset L \subset M$ een toren van velduitbreidingen. Een element $\alpha \in M$ dat algebraïsch is over $L$ is ook algebraïsch over $K$.

*Juist. Dit volgt uit gevolg 3.3.12.*

*We kunnen ook de produkt formule gebruiken,*

$$[L(\alpha) : K] = [L(\alpha) : L][L : K] < \infty,$$

*dit impliceert dat $L(\alpha)$ algebraïsch is over $K$.*

8. Zij $\alpha \in K^a$ een algebraïsch element over een veld $K$. Zij $K \subset L$ een velduitbreiding.

a) De minimaal veelterm $f_{\alpha,K}(X)$ van $\alpha$ over $K$ is een veelvoud van de minimaalveelterm $g_{\alpha,L}(X)$ van $\alpha$ over $L$.

*Juist. $f_{\alpha,K}(X)$ is ook een veelterm over $L$ en de minimaalveelterm $g_{\alpha,L}(X)$ is de voortbrenger van het ideaal van alle veeltermen over $L$ waarvan $\alpha$ een wortel is.*

b) $f_{\alpha,K}(X)$ en $g_{\alpha,L}(X)$ zoals in a). Dan is $\deg f_{\alpha,K}(X) > g_{\alpha,L}(X)$.

*Fout. Een veelterm kan irreducibel blijven over een velduitbreiding. Bv. $f_{0,\mathbb{Q}}(X) = g_{0,\mathbb{C}}(X) = X$. $f_{0,\mathbb{Q}}(X) = g_{0,\mathbb{R}}(X) = X^2 + 1$.*

9. Zij $f(X)$ een irreducibele veelterm over een veld $K$ en $g(X)$ een willekeurige veelterm over $K$ zodat $f(X)$ en $g(X)$ een wortel $\alpha \in K^a$ gemeen hebben. Dan zijn alle wortels van $f(X)$ ook wortels van $g(X)$.

*Juist. Vermits $f(X)$ irreducibel is, is het de minimaalveelterm van $\alpha$ over $K$. Elk veelterm over $K$ waarvan $\alpha$ een wortel is dan een veelvoud van $f(X)$.*

10. Zij $f(X)$ een primitieve veelterm over $\mathbb{Z}$ (i.e. $\text{cont}(f(X)) = 1$). Dan is $f(X)$ irreducibel over $\mathbb{Z}$ als en slechts als $f(X)$ irreducibel is over $\mathbb{Q}$.

*Juist. Dit volgt uit stelling 4.2.10.*

11. Zij $R$ een ring en $I$ een ideaal in $R$.

a) Als $I$ het produkt is van verschillende maximale idealen in $R$, dan is $R/I$ isomorf met het direkt produkt van velden.

*Juist. Dit volgt uit de chinese reststelling vermits verschillende maximale idealen comaximaal zijn.*



b) Zelfde bewering maar nu met $I$ het produkt van maximale idealen. (Dus het woord "veschillende" weglaten.)

*Fout. $\mathbb{Z}/p^2\mathbb{Z}$ heeft nilpotente elementen en kan dus niet het produkt van velden zijn.*

12. Een velduitbreiding is algebraïsch als en slecht als het een eindige uitbreiding is.

*Fout. Een eindige uitbreiding is algebraïsch maar niet omgekeerd. De algebraïsche sluiting van $\mathbb{Q}$ is algebraïsch over $\mathbb{Q}$ maar niet eindig.*

13.

a) Zij $\sigma : K \to K$ een automorfisme van velden. Zij $f(X) = \sum a_i X^i \in K[X]$ een irreducibele veelterm over $K$. Definieer $\sigma(f)(X) = \sum \sigma(a_i)X^i \in K[X]$. Dan is $\sigma(f)(X)$ ook irreducibel over $K$.

*Juist. De definitie van $\sigma(f(X))$ bepaalt een automorfisme van $K[X]$. Een factorisatie van $\sigma(f(X))$ wordt door het inverse van dit automorfisme omgezet in een factorisatie van $f(X)$.*

b) Zij $\sigma : K \to L$ een morfisme van velden. Zij $f(X) = \sum a_i X^i \in K[X]$ een irreducibele veelterm over $K$. Definieer $\sigma(f)(X) = \sum \sigma(a_i)X^i \in L[X]$. Dan is $\sigma(f)(X)$ ook irreducibel over $L$.

*Fout. Neem voor $\sigma$ de canonische injectie van een veld $K$ in een velduitbreiding $L$. Een irreducibele veelterm over $K$ blijft niet noodzakelijk irreducibel over $L$.*

14. Zij $f(X) \in \mathbb{F}_p[X]$ een irreducibele veelterm met $\deg f(X) = 4$ en $g(X) \in \mathbb{F}_p[X]$ een willekeurige veelterm met $\deg g(X) = 2$. Zij $\alpha \in \mathbb{F}_p^a$ een wortel van $f(X)$ en $\beta \in \mathbb{F}_p^a$ een wortel van $g(X)$. Dan geldt

$$\beta \in \mathbb{F}_p(\alpha).$$

*Juist. Als $\beta \in \mathbb{F}_p$ is de bewering triviaal. In het andere geval is $\mathbb{F}_p(\beta) = \mathbb{F}_{p^2} \subset \mathbb{F}_{p^4} = \mathbb{F}_p(\alpha)$.*