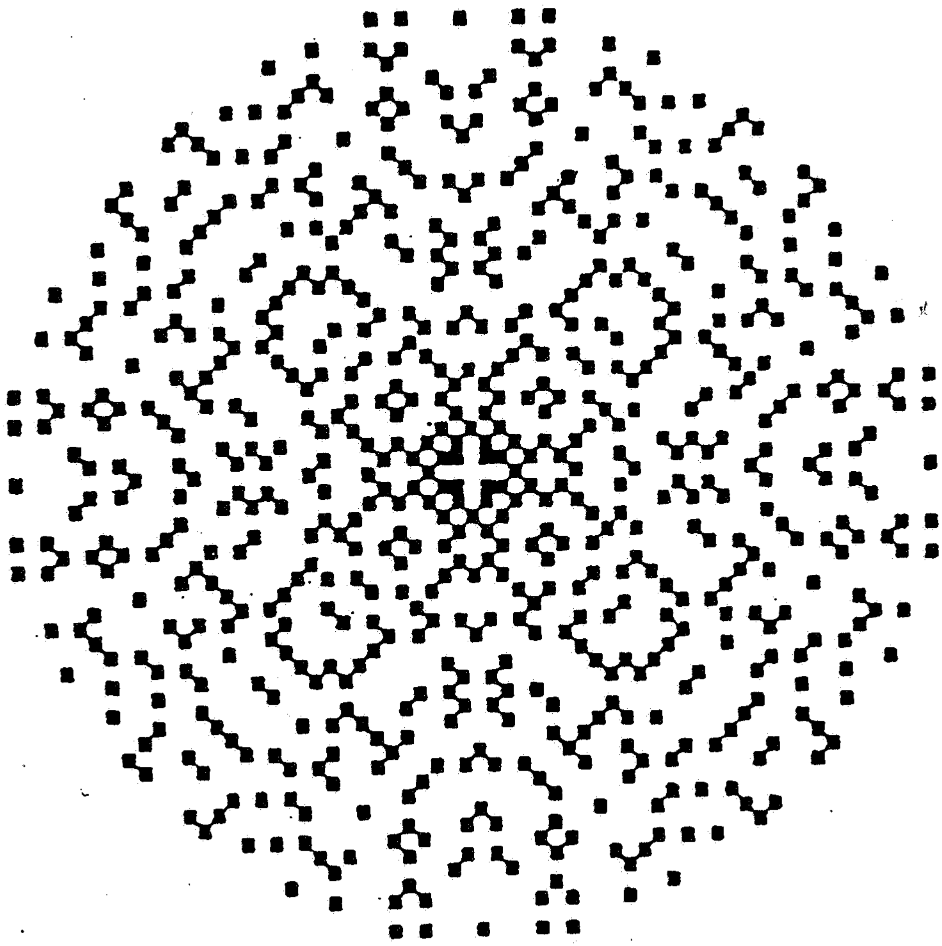
Evaluatie Algebra, 2^e Kand. Wiskunde
14 november 1995



Priemelementen $a + bi$ in $\mathbb{Z}[i]$, met $a^2 + b^2 < 1000$

(

Theorie

1. Zij R een ring, I, J idealen in R.

   a) Definieer de idealen $I + J, IJ$.
   Schrijf een algemeen element op uit elk van deze idealen.

   b) Zij $N = \{a \in R | a \text{ is een nuldeler}\} \cup \{0\}$.
   Zij $a \in N$ dan is elk veelvoud ab, met $b \in R$, ook een element van N. Namelijk, neem $r \in R, r \neq 0$ zodat $ra = 0$ dan volgt $r(ab) = (ra)b = 0$. Dit impliceert dat $ab = 0$ of dat ab een nuldeler is.
   N is eveneens gesloten onder optelling. Stel $c, d \in N$, kies $r, s \in R$, $r \neq 0$ en $s \neq 0$ zodat $rc = 0$ en $sd = 0$. Dan geldt

   $$rs(c + d) = src + rsd = 0.$$

   Dus ook $c + d$ is nul of een nuldeler. We besluiten dat N een ideaal is in R. Toon met een tegenvoorbeeld aan dat dit besluit fout is!
   Waar loopt de redenering mis?

2. Zij R een ring en I een ideaal in R.

   a) Definieer de quotiëntring R/I en formuleer de isomorfie stelling.

   b) Zij $\varphi : R \to S$ een surjectief ringmorfisme.
   Stel $\ker\varphi \subset I$.
   Toon aan dat $\varphi^{-1}(\varphi(I)) = I$.

   c) Beschouw voor idealen I en J in R de canonische surjecties

   $$\pi_I : R \to R/I$$

   $$\pi_J : R \to R/J.$$

   Dan bestaat er een uniek morfisme

   $$\eta : R/J \to R/I$$

   zodat

   $$\eta \circ \pi_J = \pi_I$$

   als en slechts als ...
   Vul aan en verklaar!

Oefeningen

1. Factorizeer het polynoom

$$X^5 + X^4 + X^3 + X^2 - X - 1$$

in irreduciebele factoren respectievelijk over de velden

$$\mathbb{Q}, \mathbb{F}_2, \mathbb{F}_3 \text{ en } \mathbb{F}_4.$$

($\mathbb{F}_4$ is het veld met 4 elementen gedefinieerd in 1.1.14 punt 1).

2. Bepaal $r, s \in R$ zodat

$$ra + sb = ggd(a, b)$$

met

a) $a = 10,\ b = (2+i)(3+2i),\ R = \mathbb{Z}[i]$

b) $a = 1456,\ b = 235,\ R = \mathbb{Z}$.

3. a) Bepaal $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]^*$

b) Is 2 een irreducibel element in $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$?
Is 3 een irreducibel element in $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$?

c) Zij $a, b \in \mathbb{Z}$. Toon aan dat alle deelringen $\mathbb{Z}[a + b\sqrt{-7}] \subset \mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ hetzelfde breukenveld hebben als $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$.

4. Zij $R = \{f | f : \mathbb{R} \to \mathbb{R}\}$ de ring van functies met puntsgewijze optelling en vermenigvuldiging.

a) Beschrijf de maximale idealen in R.

b) Bepaal $R/M, M$ een maximaal ideaal in R.

c) Beschrijf de canonische surjectie

$$R \to R/M.$$

Evaluatie Algebra I, 19/12/95

Theorie

1. Bepaal alle deelringen van het eindig veld $\mathbb{F}_{p^n}, p$ priem.
   (Niet steunen op stelling 1.15.6, gebruik de produktformule in plaats van lemma 1.15.5)

2. a) Zij R een UFD. Toon aan dat elk element in $R[X]$ een produkt is van priemelementen.

   b) Geef een voorbeeld van een niet Noethers UFD. $k[X_1, \ldots, X_n, \ldots]$
   → niet Noethers.

3. Zij A een eindig voortgebrachte K-algebra en φ een K-homomorfisme (i.e. $\varphi/K = \mathrm{id}_K$);

   $$\varphi : A \to K[X],$$

   zodat $X \in \mathrm{Im}\varphi$.

   a) Toon aan dat A niet algebraïsch is over K.

   b) Toon aan dat A een deelalgebra B bevat zodat

   $$\varphi/B : B \xrightarrow{\sim} K[X]$$

   een isomorfisme is.

Oefeningen

1. a) Toon aan dat $f(X) : X^4 + X + 1$ irreducibel is over $\mathbb{F}_2$.

   b) Zij $\alpha \in \mathbb{F}_2^a$ een wortel van $f(X)$ dan is

   $$\mathbb{F}_2[\alpha] = \mathbb{F}_{16}$$

   c) Toon aan dat er een element $\beta \in \{1, \alpha, \alpha^2, \alpha^3\}$ bestaat zodat

   $$T(\beta) = \beta + \beta^2 + \beta^4 + \beta^8 = 1.$$

   Bepaal dit element. → α^3

   d) Bepaal de wortels van

   $$\alpha^4 X^3 + \alpha X^2 + 1$$

   in $\mathbb{F}_2^a$.

2. ZIj $f(X), g(X)$ en $h(X)$ irreducibele polynomen over $\mathbb{Q}$ met

$$\deg f(x) = p^r, \deg g(X) = q^s \text{ en } \deg h(X) = l^t$$

waarbij p, q, l verschillende priemgetallen zijn.
Bepaal : $[\mathbb{Q}(\alpha,\beta) : \mathbb{Q}], [\mathbb{Q}(\alpha,\beta,\gamma) : \mathbb{Q}(\alpha)]$ en $[\mathbb{Q}(\alpha,\beta,\gamma) : \mathbb{Q}]$.

3. Zij d een kwadraatvrij getal. Alle getallen in $\mathbb{Z}[\omega_d]$ (ω_d zoals gedefinieerd in oefening 1.6.9.) zijn in het complexe vlak construeerbaar met passer en liniaal.

4. Bepaal het minimaal polynoom van de volgende algebraïsche getallen :

   a) $\sqrt[3]{5}$ over $\mathbb{Q}$

   b) $\sqrt[4]{3} + 1$ over $\mathbb{Q}$ en over $\mathbb{Q}(i)$

   c) $\sqrt[3]{5}.\sqrt{2}$ over $\mathbb{Q}$.

5. a) Hoeveel deelvelden in $\mathbb{Q}^a$ bestaan er die isomorf zijn met $\mathbb{Q}(\sqrt[4]{3})$.

   b) Zij α een algebraïsch element over $\mathbb{Q}$. Toon aan dat het aantal deelvelden van $\mathbb{Q}(\alpha)$ eindig is.

Examen Algebra I. Februari 1996

I. THEORIE

1. Zij R een uniek factorisatie domein, p een priemelement van R. Zij $f(X) \in R[X]$,

$$f(X) = X^n + \sum_{i=0}^{n-1} a_i X^i,$$

met $a_i \equiv 0 \bmod p$. Als $f(X) = g(X)h(X)$, $g(X), h(X) \in R[X]$, dan is

$$g(X) = X^d + \sum_{i=0}^{d-1} b_i X^i, \text{ met } b_i \equiv 0 \bmod p$$

en

$$h(X) = X^f + \sum_{i=0}^{f-1} c_i X^i, \text{ met } c_i \equiv 0 \bmod p.$$

Bewijs dit!

2. Toon aan dat twee eindige velden met hetzelfde aantal elementen isomorf zijn.

3. Zij K een veld en $K[\alpha, \beta]$ een K-algebra. Zij

$$\begin{array}{rcl} \varphi : K[\alpha,\beta] & \to & K[X] \\ \alpha & \mapsto & X \\ \beta & \mapsto & X^n + \sum_{i=0}^{n-1} a_i X^i \text{ (met } n > 0) \end{array}$$

een injectief K-morfisme van $K[\alpha,\beta]$ naar de veeltermring $K[X]$. Toon aan dat

a) $\{\alpha, \beta\}$ een algebraïsch afhankelijke verzameling is.

b) α transcendent is over K.

c) β transcendent is over K.

d) α algebraïsch is over $K(\beta)$.

e) β algebraïsch is over $K(\alpha)$.

II. OEFENINGEN

4. Bereken in $\mathbf{Z}[i]$ de voortbrenger van het ideaal

$$\mathbf{Z}[i](1+3i) + \mathbf{Z}[i](3+3i).$$

5. Factoriseer $X^4 + X^3 + X^2 + X + 1$ over $\mathbf{F}_2, \mathbf{F}_4$ en over $\mathbf{F}_8$.

6. Zij $f(X)$ een irreducibel polynoom over een veld K van karakteristiek nul. Stel $\alpha \in K^a$ is een wortel van f en er bestaat een $b \in K$ zodat $K(\sqrt{b}) \subset K(\alpha)$. Toon aan dat

a) $\deg f(X)$ even is.

b) $f(X) = g(X)^2 + bh(X)^2$, met $g(X), h(X) \in K[X]$.

Algebra, Februari 1996.

---

1. Factoriseer de volgende veeltermen:

ok a) $X^4 - X^2 - 1$ over $\mathbb{Q}$.

ok b) $X^6 - X^3 - 1$ over $\mathbb{F}_3$.

ok 2. Bepaal de wortels van de veelterm

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

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

3. Toon aan dat de niet nul priemidealen in de ring $\mathbb{Z}[\sqrt{d}]$ met d een kwadraatvrij geheel getal, maximale idealen zijn.

4. Voor welke priemgetallen in $\mathbb{Z}$ is $X^n - p$ zeker irreducibel in $\mathbb{Z}[\sqrt{-5}]$.

5. Zij R een ring en I een ideaal in R dat maximaal is in de verzameling van alle niet-hoofdidealen. Toon aan dat I een priemideaal is.

---

2) Het spoor van β^2 is 0 dus is er een wortel in $\mathbb{F}_8$
vermits 1 spoor 1 heeft, bekomen we met de
formule vr de wortels β^4 en $\beta^4 + 1$

$a + b\sqrt{-5}$

$\mathbb{Z}[\sqrt{-5}] / P$

$a \bmod P + b\sqrt{-5} \bmod P$

$a \bmod P \equiv a \bmod (P \cap \mathbb{Z})$

$\mathbb{Z}/p\mathbb{Z}[\sqrt{-5}]$

Zijn de volgende uitspraken (6-11) juist of fout? (Argumenteer uw antwoord.)

ok [redacted] Alle maximale idealen in een ring zijn priem. juist : p 49

7. Als I en J twee comaximale idealen zijn in een ring R, dan zijn I^n en J^m ook comaximaal in R.

[redacted] De verzameling van de niet eenheden in een ring vormt een ideaal. fout : (*)

ok [redacted] Het splijtveld van een eindige verzameling veeltermen over een veld K, is een eindige uitbreiding van K. juist

[redacted]. 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 het aantal verschillende wortels van $\sigma(f)(X)$ in de algebraïsche sluiting van K gelijk aan het aantal verschillende wortels van $f(X)$ in de algebraïsche sluiting van K. juist

11. Als $\alpha \in \mathbb{C}$ een wortel is van een monische veelterm $g(X) \in \mathbb{Z}[X]$, dan is de monische minimaal veelterm van α, $f_\alpha(X)$, ook een veelterm over $\mathbb{Z}$, i.e. $f_\alpha(X) \in \mathbb{Z}[X]$.

$X^2 - 2X + 1 = (X-1)^2$

$X^2 - 5 = 0$

(*) $\mathbb{Z}/6\mathbb{Z}$:

$3 + 4 = 1$

gn eenheid   eenheid.

$a^{p-1} = 1$