Algebra I

Examenoefeningen

Deel I

Examens Algebra I – Leuven

1 14 januari 2004

Theorie

De theorievragen zijn verloren gegaan.

Oefeningen

1. Zij $G, *$ een groep en $A \triangleleft G$. Veronderstel dat A commutatief is.
   (a) Toon aan dat
   $$\sigma : \frac{G}{A} \times A \to A : (gA, a) \mapsto gag^{-1}$$
   een goed gedefinieerde afbeelding is en dat σ een groepsactie is van $\frac{G}{A}$ op A.
   (b) Zij $a \in A$. Bepaal $\mathrm{Or}(a)$ en $\mathrm{St}(a)$.

2. Zij $F, +, \cdot$ een veld. We definiëren de ring van de formele machtreeksen $F[[X]], +, \cdot$ als
   $$F[[X]] = \left\{ \sum_{i=0}^{\infty} a_i X^i \,\middle|\, a_i \in R \right\}.$$
   Hierop definiëren we volgende bewerkingen:
   $$+ \quad : \quad F[[X]] \times F[[X]] \to F[[X]] : \left(\sum_{i=0}^{\infty} a_i X^i\right) + \left(\sum_{i=0}^{\infty} b_i X^i\right) = \left(\sum_{i=0}^{\infty} (a_i + b_i) X^i\right),$$
   $$\cdot \quad : \quad F[[X]] \times F[[X]] \to F[[X]] : \left(\sum_{i=0}^{\infty} a_i X^i\right) \cdot \left(\sum_{i=0}^{\infty} b_i X^i\right) = \left(\sum_{i=0}^{\infty} \left(\sum_{k=0}^{i} a_k b_{i-k}\right) X^i\right).$$
   Herinner u dat de eenheden in deze ring de machtreeksen zijn waarvan de constante term verschillend van 0 is.
   (a) Toon aan dat het element X op een eenheid na het enige irreducibele element is in $F[[X]]$.
   (b) Bewijs dat $F[[X]]$ een UFD is.
   (c) Is $F[[X]]$ ook een HID? Bewijs of geef een tegenvoorbeeld.

3. Zij F een deelveld van een veld E en veronderstel dat K en L deelvelden van E zijn die F omvatten. Noteer met $K \cdot L$ het kleinste deelveld van E dat K en L omvat.
   Veronderstel dat $[K \cdot L : F]$ eindig is.
   (a) Toon aan dat $[K \cdot L : L] \leq [K : F]$.
   (b) Stel dat $[K : F] = 2$ en $K \not\subseteq L$, bewijs dan dat gelijkheid geldt in (a).
   (c) Stel dat ook als $[L : F] = 2$ en $L \not\subseteq K$ er gelijkheid geldt in (a).

4. Wat zijn de mogelijke Jordanvormen J over $\mathbb{C}$ van de volgende matrix A, afhankelijk van de waarde van de parameter $a \in \mathbb{C}$?
   $$A = \begin{pmatrix} 2 & a^2 - 1 & 0 & -1 \\ 0 & 2 & a^2 - 3a + 2 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & a \end{pmatrix}$$
   Een matrix P zo dat $P^{-1}AP = J$ hoe je niet te berekenen.

2 Ergens in januari 2005

Theorie

1. Zij R een commutatieve ring met een eenheidselement en zij I een ideaal van R. Bewijs dat R/I een veld is als en slechts als I een maximaal ideaal is.

2. Zij V een complexe vectorruimte. Bewijs dat een lineaire transformatie $\mathcal{A}$ van V normaal is als en slechts als V een orthonormale basis van eigenvectoren van $\mathcal{A}$ heeft. Je mag gebruiken dat de minimale veelterm van een normale transformatie splitst in lineaire factoren.

3. Zij G een groep en zij N een normaaldeler. Bewijs dat de afbeelding

$$\overline{*} : G/N \times G/N \to G/N : (x * N, y * N) \mapsto (x * N) \overline{*} (y * N) = (x * y) * N$$

goed gedefinieerd is.

Oefeningen

1. (a) Bewijs dat er slechts één groepsmorfisme $\varphi : \mathbb{Q}/\mathbb{Z}, + \to \mathbb{Q}, +$ bestaat.
   (b) Bewijs dat er oneindig veel groepsmorfismen $\varphi : \mathbb{Q}, + \to \mathbb{Q}/\mathbb{Z}, +$ bestaan.

2. Bewijs dat het aantal verschillende complexe $n \times n$ Jordanmatrices met slechts één eigenwaarde gelijk is aan het aantal conjugatieklassen van $\mathcal{S}_n$.

3. Een *Euclidisch domein* is een integriteitsdomein R, samen met een afbeelding $t : R \to \mathbb{N}$ die voldoet aan

   - voor alle $a, b \in R$ (verschillend van 0) volgt uit $a \mid b$ dat $t(a) \leq t(b)$;
   - voor alle $a, b \in R$ (met b verschillend van 0) bestaan er $r, q \in R$ zodat $a = bq + r$, met $r = 0$ of $t(r) < t(b)$.

   Een voorbeeld van een Euclidisch domein is de veeltermenring $F[X]$ over veld F met als afbeelding $\deg : F[X] \to \mathbb{N} : f \mapsto \deg(f)$.

   (a) Zoek een ander voorbeeld van een Euclidisch domein.
   (b) Bewijs dat een Euclidisch domein een hoofdideaaldomein is.
   (c) Bewijs dat $t(u) = t(1)$ als en slechts als $u \in R^{\times}$.

4. Zij $\mathcal{A} : \mathbb{C}_6 \to \mathbb{C}_6$ een nilpotente lineaire afbeelding met $\dim\left(\operatorname{Ker} \mathcal{A}^2\right) = 4$. Bepaal de mogelijke waarden voor $\dim(\operatorname{Ker} \mathcal{A})$ en illustreer telkens met een voorbeeld.

3 29 augustus 2005

Theorie

De theorievragen zijn verloren gegaan.

Oefeningen

1. Zij $G, *$ een groep en zijn M, N normaaldelers van G met $M \subset N$. Veronderstel dat G/N cyclisch is en $|N/M| = 2$.
   Toon aan dat G/M commutatief is.
   Hint: gebruik de opmerking op bladzijde 29:
   Stelling. *Zij G een groep. Indien $G/Z(G)$ cyclisch is, dan is G commutatief (en is $G/Z(G)$ dus eigenlijk de triviale groep).*
   Opmerking. Met hetzelfde bewijs kunnen we een nog iets beter resultaat verkrijgen: indien er een deelgroep H van $Z(G)$ bestaat zodat G/H cyclisch is, dan is G commutatief.

2. Beoordeel onderstaande redenering. Is ze juist of fout? Waarom?

   "Zij $R, +, \cdot$ een ring met $1 \neq 0$. Omdat R een groep is voor de optelling en $1 \in R$, bestaat er een invers element -1 van 1. Er geldt dan dat $(-1) \cdot (-1) = 1$ en dus is -1 een eenheid. Dus $|R^\times| \geq 2$."

3. Een ring $R, +, \cdot$ wordt *Artins* genoemd als elke dalende keten $I_0 \supseteq I_1 \supseteq I_2 \supseteq \cdots$ van idealen stabiliseert. Dit wil zeggen dat er een $n \in \mathbb{N}$ is zo dat $I_n = I_{n+1} = I_{n+2} = \ldots$.

   (a) Toon aan dat $\mathbb{Z}, +, \cdot$ geen Artinse ring is.

   (b) Bewijs dat de quotiëntring $\dfrac{\mathbb{Q}[X]}{(X^3)}, +, \cdot$ wel een Artinse ring is.

4. Zij E een veld met $\mathbb{Q} \subset E \subset \mathbb{C}$ en $[E : \mathbb{Q}] = 2$. Toon aan dat er een $d \in \mathbb{Z}$ bestaat met $E = \mathbb{Q}(\sqrt{d})$.

5. Veronderstel dat de matrix van een lineaire afbeelding $f : \mathbb{C}^3 \to \mathbb{C}^3$ ten opzichte van een goed gekozen basis $\{e_1, e_2, e_3\}$ volgende Jordanmatrix is

   $$J = \begin{pmatrix} 2 & 0 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

   We kunnen $\mathbb{C}^3$ echter ook als een zesdimensionale reële vectorruimte bekijken. Welke basis van $\mathbb{C}^3$als reële vectorruimte kan je kiezen opdat f ten opzichte van die basis in zijn Jordanvorm staat, en wat is die Jordanvorm?

4 Ergens in januari 2006

Theorie

1. Zij $G, *$ een groep en zij N een normaaldeler van G. Bewijs dat er een bijectie bestaat tussen de normaaldelers van G die N omvatten en de normaaldelers van G/N.
   Je mag hierbij het enkel feit gebruiken dat het beeld en het inverse beeld van een deelgroep onder een groepsmorfisme weer een deelgroep is, de andere beweringen moeten bewezen worden.

2. Veronderstel dat R een hoofdideaaldomein is en zij r een irreducibel element in R. Bewijs dat (r) dan een maximaal ideaal van R is.
   Geef een voorbeeld van een commutatieve ring R met eenheidselement en een irreducibel element $r \in R$ zo dat (r) geen maximaal ideaal van R is.

3. Bewijs de stelling van Kronecker.
   "Zij K een veld en zij f een niet-constante veelterm in $K[X]$, dan heeft f een wortel in een velduitbreiding van K."

Snelheidsvraagjes.

1. *Bestaat er een algebraïsch gesloten veld dat $\mathbb{C}$ strikt omvat?*

2. *Waar of fout?*
   "Een groep is eindig als en slechts als alle elementen eindige orde hebben."

Oefeningen

1. Zij $G, *$ een groep met precies twee niet-triviale deelgroepen.
   (a) Bewijs dat G cyclisch is.
   (b) Bewijs dat de orde van G van de vorm p^3 of pq is, voor zekere priemgetallen p en q.

2. Met welke "bekende" ring is

$$K = \frac{\mathbb{Z}_5[X, Y]}{(Y - X^2, XY + Y + 2)}$$

   isomorf? Bewijs je antwoord.

3. Zij $F \subset E$ velden. De Galoisgroep $\operatorname{Gal}(E, F)$ van E en F wordt gedefinieerd als de groep van alle veldautomorfismen $\sigma : E \to E$, dit zijn de ringautomorfismen van E waarvoor geldt dat $\sigma(1) = 1$, die voldoen aan $\sigma(f) = f$, voor alle $f \in F$. Hierbij beschouwen we als groepsbewerking de samenstelling van afbeeldingen.
   Toon aan dat $\operatorname{Gal}\left(\mathbb{Q}\left(\sqrt{2}\right), \mathbb{Q}\right) \cong \mathbb{Z}_2$.

4. (a) Kies een voorstelling van $\mathbb{F}_8$ als $\mathbb{F}_2[X]/(f)$, met $f \in \mathbb{F}_2[X]$ een irreducibele veelterm van graad 3. Bepaal een basis van $\mathbb{F}_8$ als $\mathbb{F}_2$-vectorruimte.
   Toon aan dat het Frobeniusmorfisme $\varphi : \mathbb{F}_8 \to \mathbb{F}_8 : x \mapsto x^2$ een lineaire transformatie van $\mathbb{F}_8$ is, bepaal de matrix van φ ten opzichte van de gekozen basis en bepaal de minimale veelterm van φ.
   (b) Zij p een priemgetal en zij r een natuurlijk getal verschillend van 0. Laat zien dat het Frobeniusmorfisme $\varphi : \mathbb{F}_{p^r} \to \mathbb{F}_{p^r} : x \mapsto x^p$ een lineaire transformatie is van $\mathbb{F}_{p^r}$ als vectorruimte over $\mathbb{F}_p$. Zoek de minimale veelterm van φ en bewijs je vermoeden.

5 25 januari 2006

Theorie

1. Zij $G, *$ een groep, zij K een deelgroep van G en zij N een normaaldeler van G.
   Bewijs dat $KN = \mathrm{grp}\,(K \cup N)$.

2. Zij R een ring en D een deelgroep van $R, +$. Bewijs dat

$$\bar{\cdot} : R/D \times R/D \to R/D : (x + D, y + D) \mapsto (x + D)\,\bar{\cdot}\,(y + D) = (x \cdot y) + D$$

   goed gedefinieerd is als en slechts als D een ideaal is.

3. Bewijs dat "algebraïsch zijn van velduitbreidingen" transitief is.
   Is "transcendent zijn" dat ook?

Snelheidsvraagje.
Geef alle 2×2–matrices over $\mathbb{C}$ die hermitisch en unitair zijn.

Oefeningen

1. (a) Zij H een deelgroep van $\mathcal{S}_n$. Toon aan dat H een normaaldeler is als en slechts als voor elke $\sigma \in H$ geldt dat alle elementen van $\mathcal{S}_n$ met dezelfde disjuncte cykel-schrijfwijze als σ ook tot H behoren.

   (b) Toon aan dat $\mathcal{S}_4$ een unieke deelgroep heeft van orde 12.

2. Zij $R, +, \cdot$ een ring. Het centrum $Z(R)$ van R is de verzameling

$$Z(R) = \{x \in R \big| \forall a \in R : ax = xa\}.$$

   Volgens oefening zeven uit de oefeningenbundel (deel III. Ringen) is $Z(R)$ een deelring is van R.

   (a) Geef een voorbeeld waaruit blijkt dat $Z(R)$ geen ideaal van R hoeft te zijn.

   (b) Het quotiënt $\frac{R}{Z(R)}$ zal dus in het algemeen geen ringstructuur hebben, maar slechts een additieve groepsstructuur. Bewijs dat als $\frac{R}{Z(R)}$ een cylische groep is, R dan een commutatieve ring is.

3. Noteer met N_r^p het aantal monische irreducibele polynomen van graad r over $\mathbb{Z}_p$. Gebruik de theorie van eindige velden om volgende recursieformule voor N_r^p te bewijzen:

$$N_r^p = \frac{1}{r}\left(p^r - \sum_{d|r,\, d\neq r} dN_d^p\right).$$

4. (a) Zij $\mathcal{A} : \mathbb{R}^2 \to \mathbb{R}^2$ een lineaire afbeelding met karakteristieke veelterm $f_A(X) = X^2 + aX + b$, waarbij de discriminant $a^2 - 4b < 0$. Toon aan dat er een basis $\mathcal{E}$ van $\mathbb{R}^2$ bestaat zodat $\mathcal{A}$ volgende matrix krijgt ten opzichte van $\mathcal{E}$:

$$\begin{pmatrix} 0 & -b \\ 1 & -a \end{pmatrix}.$$

   (b) Zij B de volgende 4×4-matrix over de complexe getallen:

$$\begin{pmatrix} 2 & 1 & 0 & -1 \\ 0 & 3 & 0 & 0 \\ -3 & 1 & 1 & -5 \\ 1 & -1 & 0 & 4 \end{pmatrix}.$$

   Bepaal de Jordanvorm J van B en een matrix P zodat $P^{-1}BP = J$.

6 15 januari 2007

Theorie

1. Zij $\sigma \in \mathcal{S}$. Geef en bewijs de formule voor de orde van σ in $\mathcal{S}, \circ$ in termen van de disjuncte cykelschrijfwijze van σ.
   Bijvraag: Wat is de grootst mogelijke orde van een element in $\mathcal{S}_8$?

2. Zij R een HID en $x \in R$ met $x \neq 0$ en x geen eenheid. Bewijs dat x te schrijven is als een product van irreducibele elementen.
   Hints:
   - *Een contradictie.*
   - *Een stijgende keten van idealen kan nuttig zijn.*

3. Zij $K \subset E$ een velduitbreiding en $a, b \in E$ algebraïsch over K.
   (a) Bewijs dat $a + b$ algebraïsch is over K.
   (b) Waar of niet?
   Zij $c, d \in E$ transcendent over K, dan is $c + d$ transcendent over K.

Snelheidsvraagje.
Geef de maximale idealen in $\mathbb{C}[X]$.

Oefeningen

1. Zij $G, *$ een groep en zij H een deelgroep van G. Het aantal linkse nevenklassen van H in G noemen we de index van H in G. De index van H in G is dus een van 0 verschillend natuurlijk getal of oneindig.
   (a) Zij $G, *$ een groep. Zij H een deelgroep in G met eindige index in G en zij $g \in G$.
   Toon aan dat de deelgroep gHg^{-1} ook eindige index heeft in G.
   (b) Zij $G, *$ een groep en D de doorsnede van alle deelgroepen van G met eindige index in G. Toon aan dat D een normaaldeler is van G. Waarom is dit triviaal als G een eindige groep is?
   (c) Geef een voorbeeld van een oneindige groep $G, *$ waarvoor $\{eG\}$ de doorsnede is van alle deelgroepen van eindige index in G.

2. Zij $R, +, .$ een ring en zij I het ideaal voortgebracht door $\{ab - ba \mid a, b \in R\}$. Zij J een ideaal van R.
   Toon aan dat R/J commutatief is als en slechts als $I \subset J$.

3. Zij ω de primitieve derde eenheidswortel in $\mathbb{C}$.
   (a) Bepaal de relaties tussen de velden $\mathbb{Q}(\sqrt{3}\omega)$, $\mathbb{Q}(\sqrt{3} + \omega)$ en $\mathbb{Q}(\sqrt{3}, \omega)$.
   (b) Bereken de uitbreidingsgraad $\left[\mathbb{Q}(\sqrt{3}, \omega) : \mathbb{Q}\right]$.
   (c) Bepaal een minimale veelterm van $\sqrt{3} + \omega$ over $\mathbb{Q}$.

4. Stel
$$A = \begin{pmatrix} 0 & 1 & 2 & 0 \\ -2 & 4 & 1 & 0 \\ -2 & 1 & 4 & 0 \\ -2 & 0 & 3 & 3 \end{pmatrix}.$$
   Zoek een inverteerbare matrix P en een Jordanmatrix J zodat $P^{-1}AP = J$.

7 30 januari 2007

Theorie

1. Zij $G, *$ een eindige groep en $a \in G$.
   Definieer $C_G(a)$ en $Cl(a)$. Bewijs dat $|Cl(a)| = \dfrac{|G|}{|C_G(a)|}$.
   Bijvraag: Is $Cl(a)$ een deelgroep van G? Is $C_G(a)$ een deelgroep van G? Wat als G niet eindig is?

2. Vul aan en bewijs.
   "Het aantal elementen van een eindig veld is steeds..."

3. Zij V een $\mathbb{C}$-vectorruimte en $\mathcal{A}$ een lineaire afbeelding. Laat ons veronderstellen dat we weten hoe de decompositie van V over $\mathcal{A}$ ineen zit. Vul aan en bewijs.
   "$\mathcal{A}$ is diagonaliseerbaar als en slechts als de minimale veelterm van $\mathcal{A}$..."

Snelheidsvraagjes.

1. *Welke inclusies gelden er tussen $\mathbb{F}_2$, $\mathbb{F}_4$, $\mathbb{F}_6$ en $\mathbb{F}_8$?*
2. *Wat is $\mathbb{F}_{16} \cap \mathbb{F}_{64}$?*

Oefeningen

1. (a) Toon aan dat $G = \left\{ \begin{pmatrix} b & c \\ 0 & d \end{pmatrix} \middle| \, b, d \in \mathbb{Q}_0, c \in \mathbb{Q} \right\}$ met de gewone matrixvermenigvuldiging een groep is.
   (b) Toon aan dat $N = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \middle| \, a \in \mathbb{Q} \right\}$ een normaaldeler is van G.
   (c) Met welke "bekende" groep is G/N isomorf?

2. Beschouw de ring $\mathbb{R}[x, y]$.
   (a) Geef een ideaal dat geen priemideaal is, en leg uit waarom.
   (b) Geef een maximaal ideaal en toon dat aan.

3. (a) Toon aan dat $\sqrt[3]{5} \notin \mathbb{Q}(\sqrt[3]{2})$ door het probleem te herleiden tot de oplosbaarheid van een stelsel in $\mathbb{Q}$.
   Hint: Een stelsel moet niet lineair zijn.
   (b) Wat is $\left[\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{5}) : \mathbb{Q}\right]$?
   (c) Geef een basis van $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{5})$ over $\mathbb{Q}$

4. Stel
$$A = \begin{pmatrix} 2 & 1 & -1 \\ 3 & 4 & 1 \\ 3 & 2 & 3 \end{pmatrix}.$$
   Zoek een inverteerbare matrix P en een Jordanmatrix J zodat $P^{-1}AP = J$.

8 30 augustus 2007

Theorie

1. *Schriftelijk*
   Geef en bewijs de eerste morfismestelling van groepen.

2. Geef en bewijs de stelling van Kronecker.

3. Zij V een eindigdimensionale $\mathbb{C}$-vectorruimte met (Hermitisch) inproduct en $A : V \to V$ een lineaire transformatie. Bewijs dat $(A^*)^* = A$.

Snelheidsvraagjes.

1. *Gegeven $\mathbb{R}[X, Y]$, geef de grootste gemene deler van X en Y.*

2. *Zij $\mathbb{F}_q$ een eindig veld met q elementen. Bekijk dan de additieve en multiplicatieve groepen $\mathbb{F}_q, +$ en $\mathbb{F}_q^\times, \cdot$ Welke zijn cyclisch?*

Oefeningen

1. Zij $G, *$ een groep, N een normaaldeler en M een deelgroep van G die N omvat.
   (a) Bewijs dat als $M/N \subset Z(G/N)$ dan grp $\left\{ m * g * m^{-1} * g^{-1} \middle| \forall m \in M, \forall g \in G \right\} \subset N$.
   (b) Als nu $M/N = Z(G/N)$, geldt dan dat grp $\left\{ m * g * m^{-1} * g^{-1} \middle| \forall m \in M, \forall g \in G \right\} = N$? Bewijs of geef een tegenvoorbeeld.

2. Een ring $R, +, \cdot$ heeft een priemideaal P en twee idealen A en B.
   Bewijs dat als $A \cap B = P$ dat dan $A = P$ of $B = P$.

3. Zij ω de derde-eenheidswortel en zij ψ de wortel van $2 + \omega$.
   (a) Wat is de relatie tussen de velden $\mathbb{Q}(\omega)$ en $\mathbb{Q}(\xi)$?
   (b) Bereken $[\mathbb{Q}(\xi) : \mathbb{Q}]$.

4. Oefening over Jordanvorm.

9 15 januari 2008

Theorie

1. *Schriftelijk*
   Formuleer en bewijs de Factorisatiestelling voor groepen.

2. *Mondeling.*
   Zij V een complexe vectorruimte en $\mathcal{A}$ een lineaire transformatie van V. Op V rust het hermitisch inproduct.
   Veronderstel dat de decompositiestelling en een nuttig resultaat over minimale veeltermen en normale afbeeldingen $\mathcal{A}$ gegeven is. Bewijs nu dat $\mathcal{A}$ normaal is als en slechts als er een orthogonale basis van eigenvectoren van $\mathcal{A}$ bestaat.

3. *Mondeling.*
   Geef en bewijs de stelling van Bezout in een HID.

Snelheidsvraagjes.

1. *Gegeven $\mathbb{R}[X, Y]$, geef de grootste gemene deler van X en Y.*

2. *Zij $\mathbb{F}_q$ een eindig veld met q elementen. Bekijk dan de additieve en multiplicatieve groepen $\mathbb{F}_q, +$ en $\mathbb{F}_q^\times, \cdot$ Welke zijn cyclisch?*

Oefeningen

1. (a) Bewijs of geef een tegenvoorbeeld.
   "Er bestaat geen groep van orde 8 met maar één element van orde 4."

   (b) Zij $G, *$ een niet-cyclische groep van orde 8 met precies twee elementen van orde 4, toon aan dat G isomorf is met $\mathcal{D}_4$.

2. Waar of niet waar? Argumenteer!

   (a) $f : \mathbb{Z} \to \mathbb{Z}_6 : x \to \overline{4x}$ is een goed gedefinieerd ringmorfisme.

   (b) $\dfrac{\mathbb{Z}_2[X]}{(X^5 + X^4 + 1)}$ is een veld.

3. Bereken $\left[\mathbb{Q}(\sqrt[4]{2008}, \sqrt[6]{2008}) : \mathbb{Q}\right]$.

4. Oefening over Jordanvorm.

10 28 januari 2008

Theorie

1. *Schriftelijk*
   Formuleer en bewijs de tweede isomorfismestelling.

2. Bewijs dat

   (a) het aantal elementen van een eindig veld steeds van de vorm p^r, met p priem en $r \in \mathbb{N}_0$, is.

   (b) er een veld bestaat met p^r elementen, namelijk een ontbindingsveld van ... over $\mathbb{Z}_p$.

3. Bewijs dat diagonaliseerbaar zijn equivalent is met een minimale veelterm die volledig ontbindbaar is in onderling verschillende lineaire termen.

Snelheidsvraagje.
Waar of niet waar? Bespreek beide pijlen van de equivalentie.

> *"Zij R een ring met 1 dan geldt dat u en v een inverse hebben als en slechts als uv een inverse heeft."*

Wat als de ring nu commutatief is?

Oefeningen

1. De Stelling van Cauchy: "Zij G een groep van orde n, met n een veelvoud van een priemgetal p. Er bestaat dan een element in G dat orde p heeft."
   Bewijs deze stelling met het principe van volledige inductie op $\alpha = n/p$.

   (1) Bewijs de basistap, $\alpha = 1$.

   De inductiehypothese luidt nu dat er een zekere $k > 0$ is zo dat voor alle groepen met $\alpha \leq k$ geldt dat er een element met orde p is. We tonen nu vanuit het ongerijmde aan dat dit ook geldt voor $k+1$. Vanuit de oefenzittingen weten we alvast ook dat G geen commutatieve groep is.

   (2) Bewijs dat het aantal elementen van een niet-triviale conjugatieklasse een veelvoud is van p.

   (3) Bewijs dat het aantal elementen van $Z(G)$ een veelvoud is van p.

   (4) Beëindig je bewijs met een contradictie.

2. Zij $R = \dfrac{\mathbb{Z}[X,Y]}{(XY-1)}$.

   (a) Is $(\overline{1-X})$ een eenheid?

   (b) Is $(\overline{X})$ een maximale ideaal?

   (c) Bewijs dat R isomorf is met $\mathbb{Z}\left[X, \frac{1}{X}\right]$.
   Hint: je mag hierbij veronderstellen dat elke $f \in \mathbb{Z}[X,Y]$ te schrijven is als

   $$f = \sum_{n \in \mathbb{Z}} \sum_{\substack{(i,j) \in I \\ j = i+n}} a_{ij} X^i Y^j$$

   met $I \subset \mathbb{N}^2$ een eindig gebied.

   (d) Bepaal het breukenveld van R.

3. Zij $f(X) = X^4 + 4X^2 - 2 \in \mathbb{Z}[X]$.

(a) Bewijs dat f irreducibel is over $\mathbb{Q}$.

(b) Geef een ontbindingsveld $E \subset \mathbb{C}$ over $\mathbb{Q}$.

(c) Bereken $[E : \mathbb{Q}]$.

4. Oefening over Jordanvorm.

11 21 januari 2009

Theorie

1. *Mondeling.*
   Bewijs de Stelling van Cayley: “Elke groep is isomorf met een permutatiegroep.”

2. *Schriftelijk*
   Zij R een commutatieve ring met eenheidselement en I een ideaal van R. Bewijs dat R/I een veld is als en slechts als I maximaal is.

3. *Mondeling.*
   Gegeven is dat elk veld K een een algebraïsche uitbreiding K_1 heeft zo dat elke niet-constante veelterm $f \in K[X]$ een wortel heeft in K.
   Bewijs dat elk veld een algebraïsche sluiting heeft.

Oefeningen

1. x en y zijn voortbrengers van de groep G. Er geldt tevens dat $x^8 = y^2 = yxyx^3 = 1$.

   (a) Toon aan dat elk element van G van de vorm $x^i y^j$ is. Toon aan dat elk element maximaal orde 16 heeft.

   (b) Zij $|G| = 16$. Bepaal de orde van xy. Bepaal het centrum van G. Toon aan dat G oplosbaar is.

   (c) Toon aan dat elke groep van orde 4 dezelfde vorm als G heeft. Geldt ook voor elke groep van orde 8?

2. Waar of vals? Geef voldoende uitleg.

   (a) Zij $R = \mathbb{R}^{2\times 2}$. Voor elke $f, g \in R[X]$ geldt $\deg(f * g) = \deg(f) + \deg(g)$

   (b) Zij R de directe som van S en T. Als R een eenheidselement heeft, hebben S en T ook een eenheidselement.

3. (a) Hoeveel monische irreducibele veeltermen van graad 3 heeft $\mathbb{Z}_3[X]$?

   (b) Toon aan dat $f(X) = X^2 + 2X + 1$ irreducibel is. Wat is de orde van $F = \mathbb{Z}_3[X]/(f)$?

   (c) Zij $\mathcal{O} = \{\mathrm{Ord}(g) | g \text{ element van } F^\times\}$. Geef voor elke $n \in O$ een element g uit F met deze orde.

4. (a) Voor welke n bestaat er een matrix $M \in \mathbb{C}^{n\times n}$ zodat de minimale veelterm van M $(x-1)(x-2)^2(x-3)^3$ is?

   (b) Zij A een nilpotente matrix in $\mathbb{C}^{6\times 6}$. Zij $\dim(\mathrm{Ker}(A^2)) = 4$. Geef alle mogelijke invariante systemen van A.

12 27 januari 2009

Theorie

1. (a) Zij $G, *$ een groep en $N \lhd G$. Bewijs dat

$$\overline{*} : G/N \times G/N \to G/N : (x * N, y * N) \mapsto (x * N) \,\overline{*}\, (y * N)\, (x * y) * N$$

goed gedefinieerd is.

(b) Waar of niet?
"Als G cyclisch en N een deelgroep van G is, dan is G/N cyclisch."

2. Zij $K \subset E$ een velduitbreiding en $u \in E$ algebraïsch over K.

(a) Bewijs dat $K(u) \cong K[X]/(f)$ waarbij f de minimale veelterm van u over K is.

(b) Bewijs dat $1, u, u^2, \ldots, u^k$ lineair onafhankelijk zijn over K, waarbij je k zo groot mogelijk neemt.

3. Zij V een eindigdimensionale $\mathbb{C}$-vectorruimte met (Hermitisch) inproduct en $A : V \to V$ een lineaire transformatie. Bewijs dat $(A^*)^* = A$.

Snelheidsvraagjes.

1. *Geef alle idealen van* $\mathbb{Z}$.

2. *Als* $\mathbb{Z}$ *een HID is, is* $(4, 7)$ *dan ook een hoofdideaal?*

3. *Wat is de priemdeelring van* $\mathbb{Z}$*?*

4. *Wat is de doorsnede van alle deelringen van* $\mathbb{Z}$*?*

5. *Wat zijn de maximale idealen in* $\mathbb{Z}$*?*

Oefeningen

1. Waar of niet waar? Geef voldoende uitleg.

(a) Zij G_1, G_2, H_1, H_2 groepen zodat $G_1 \oplus G_2$ isomorf is met $H_1 \oplus H_2$. Dan is $G_1 \cong H_1$ en $G_2 \cong H_2$, of, $G_1 \cong H_2$ en $G_2 \cong H_1$.

(b) Zij G_1 en G_2 groepen met normaaldelers $N_1 \lhd G_1$ en $N_2 \lhd G_2$. Dan is $N_1 \oplus N_2$ een normaaldeler van $G_1 \oplus G_2$.

2. Zij F een veld.

(a) Toon aan dat $R = \{f \in F[X] \mid f'(0) = 0\}$ een deelring is van $F[X]$. Geef een ideaal $I \lhd R$ van de vorm (X^i, X^j) met $i, j \in \mathbb{N}$ dat geen hoofdideaal is. De ring R is dus geen HID. Toon aan dat R zelfs geen UFD is.

(b) Toon aan dat de ringen

$$R_0 = \{f \in F[X] \mid f(0) = 0\} \qquad \text{en} \qquad R_1 = \{f \in F[X] \mid f(1) = 0\}$$

isomorf zijn.

3. Zij $f(X) = X^2 + 2X + 4$.

(a) Zij E het ontbindingsveld van f over $\mathbb{Q}$. Bepaal $[E : \mathbb{Q}]$.

(b) Toon aan dat f irreducibel is over $\mathbb{Z}_5$. Beschouw het veld $F = \mathbb{Z}_5[T]/(f(T))$. Hoeveel elementen telt F? Geef de twee wortels van f in F. Schrijf $\overline{T+1}^{2009}$ als $\overline{aT+b}$ met $a, b \in \mathbb{Z}_5$.

4. Zij $A \in \mathbb{C}^{3\times 3}$ de volgende matrix:

$$A = \begin{pmatrix} i & 0 & -2 \\ 0 & i+1/2 & 1/2 \\ 0 & -1/2 & -1/2+i \end{pmatrix}.$$

Bepaal een inverteerbare matrix P en een Jordanmatrix J zodat $J = P^{-1}AP$.

13 2 september 2009

Theorie

1. Zij $\sigma \in \mathcal{S}_n, \sigma \neq \mathrm{Id}$, geef en bewijs een formule voor de orde van σ in termen van zijn disjuncte cykelnotatie.

2. Zij R een ring en D een deelgroep van $R, +$. Bewijs dat

$$\bar{\cdot} : R/D \times R/D \to R/D : (x + D, y + D) \mapsto (x + D) \,\bar{\cdot}\, (y + D) = (x \cdot y) + D$$

   goed gedefinieerd is als en slechts als D een ideaal is.

3. (a) Bewijs dat de orde van een eindig veld altijd de macht van een priemgetal is.

   (b) Bewijs dat als p een priemgetal en $r \in \mathbb{N}_0$, er dan een veld bestaat met p^r elementen, namelijk het ontbindingsveld van de veelterm … (vul in) over $\mathbb{Z}_p$.

Oefeningen

1. Zij $G, *$ een groep en $D = \{(g, g) \,|\, g \in G\}$ een deelgroep van $G \times G$.

   (a) Welke voorwaarde moet je op G opleggen opdat D een normaaldeler van $G \times G$ is?

   (b) Veronderstel nu dat D een normaaldeler is. Waarmee is $G \times G/D$ dan isomorf?

2. Een ring heet *lokaal* als de ring slechts 1 maximaal ideaal heeft.

   (a) Bewijs dat een ring lokaal is als en slechts als de niet-eenheden van de ring een ideaal vormen.

   (b) Zijn de ringen $\mathbb{Z}$, $\mathbb{Z}_9$, $\mathbb{Z}_{10}$, $\mathbb{Z}_{11}$ en $\mathbb{Z}[X]$ lokaal?

3. Zij $z = i\sqrt{1 + \sqrt{2009}}$. Bereken $[\mathbb{Q}(z) : \mathbb{Q}]$ en geef de minimale veelterm van z over $\mathbb{Q}$.

4. Zij $A \in \mathbb{C}^5 \times \mathbb{C}^5$:

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 2 & -1 & 1 & 1 \\ -2 & 0 & 3 & -1 & 0 \\ -1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 2 \end{pmatrix}.$$

   Bepaal een inverteerbare Jordanmatrix J zodat $J = P^{-1}AP$.

14 13 januari 2010

Theorie

1. *Mondeling.*
   Zij $G, *$ een eindige groep en X een verzameling. Veronderstel dat G werkt op X via de actie
   $$\cdot : G \times X \to X : (g, x) \mapsto g \cdot x.$$
   (a) Zij $x \in X$. Definieer de *baan* (ook orbiet genoemd) van x en de stabilisator van x.
   (b) Formuleer en bewijs de orbietstelling. Deze geeft voor een $x \in X$ een verband tussen de kardinaliteiten van G, van de baan van x en van de stabilisator van x.

2. *Schriftelijk.*
   (a) Definieer het begrip *hoofdideaaldomein.*
   (b) Zij F een veld. Toon aan dat $F[X]$ een hoofdideaaldomein is.

3. *Schriftelijk.*
   (a) Zij $F \subseteq E$ een eindige velduitbreiding. Toon aan dat E algebraïsch is over F.
   (b) Geef een voorbeeld van een oneindige velduitbreiding die algebraïsch is. Argumenteer!

Oefeningen

1. Zij $G, *$ een eindige groep en zij H en K twee verschillende deelgroepen van index 2 in G.
   (a) Toon aan dat $H \cap K \triangleleft G$.
   (b) Toon aan dat $\dfrac{G}{H \cap K}$ niet cyclisch is.

2. (a) Zij $a \in \mathbb{R}$.
   Hoeveel idealen heeft de ring $\dfrac{\mathbb{R}[X]}{X^2 - a}$? Leg uit.
   Hint: beschouw de gevallen $a < 0$, $a = 0$ en $a > 0$ apart.
   (b) Geef een voorbeeld van een ring met precies drie priemidealen. Argumenteer.

3. Zij $f = X^4 + X^2 + 1 \in \mathbb{Q}[X]$ en L het ontbindingsveld van f over $\mathbb{Q}$.
   (a) Toon aan dat er een wortel α van f bestaat zo dat $L = \mathbb{Q}(\alpha)$.
   (b) Geef de minimale veelterm van de gevonden α uit deel (a) en geef $[L : \mathbb{Q}]$.

4. Zij $A \in \mathbb{C}^{n \times n}$ en zij $f_A = (X - i)\,\phi_A$ en $\phi_A^2 = \left(X^2 + 1\right) f_A$.
   Bereken f_A en ϕ_A en geef de Jordanvorm van A. Leg uit.

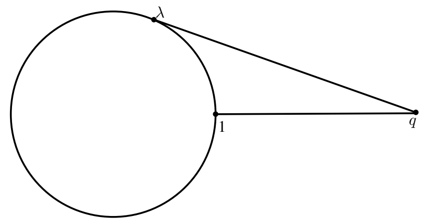
15 19 januari 2011

Theorie

1. *Schriftelijk.*
   (a) Formuleer de eerste ismorfismestelling voor groepen.
   (b) Forumuleer en bewijs de parallellogramismorfismestelling voor ringen.
   Hint: voor een ring R geeft deze stelling een verband tussen een ideaal I van R, een deelring S van R , $I+S$ en $I \cap S$.
2. *Mondeling.*
   Zij K een veld en G een eindige deelgroep van de multiplicatieve groep $K^{\times}, \cdot$. Bewijs in detail dat G cyclisch is.
3. *Schriftelijk.*
   (a) Zij V een eindig dimensionale vectorruimte over een veld K en zij A een nilpotente transformatie van V met index $k \geq 1$. Zij $v \in V$ gegeven met $A^{k-1}(v) \neq 0$. Bewijs dat $\{v, A(v), \ldots, A^{k-1}(v)\}$ lineair onafhankelijk zijn.
   (b) Veronderstel bovendien dat $k = \dim V$. Wat is dan de matrix A ten opzichte van de basis $\{v, A(v), \ldots, A^{k-1}(v)\}$?

Oefeningen

1. Toon aan dat $\mathcal{S}_4$ geen deelgroep heeft die isomorf is met de quaternionengroep.
2. We zullen in de volgende stappen de Stelling van Wedderburn (op bladzijde 45 in de cursus) aantonen. Zij R een eindig lichaam.
   (a) Zij $x \in R$. Definieer de ringcentralisator $C_R(x)$ van R als
   $$C_R(x) = \{r \in R | rx = xr\}.$$
   Toon aan dat $C_R(x)$ een deellichaam is van R.
   (b) Definieer het ringcentrum $Z(R)$ van R als
   $$Z(R) = \bigcap_{x \in R} C_R(x) = \{r \in R | rx = xr \text{ voor alle } x \in R\}.$$
   Stel dat $|Z(R)| = q$. Vermits $0 \neq 1$ in R en deze elementen beide behoren tot $Z(R)$ hebben we dat $q \geq 2$.
      i. Toon aan dat er een $n \in \mathbb{N}_0$ bestaat zodat $|R| = qn$.
      ii. Toon aan dat er voor alle $x \in R$ een $n_x \in \mathbb{N}$ bestaat zodat $|C_R(x)| = q^{n_x}$.
   (c) Veronderstel dat R geen veld is, dus er bestaat een $x \in R$ zodat $C_R(x) \neq R$. Leg uit waarom $n > 1$ en $nx < n$.
   Toon aan dat
   $$q^n - 1 = q - 1 + \sum_{k=1}^{m} \frac{q^n - 1}{q^{n_k} - 1}$$
   voor $m \in \mathbb{N}_0$ met elke $nk < n$ en $\frac{q^n-1}{q^{n_k}-1} \in \mathbb{Z}$ voor elke k.
   (d) Dan kan men makkelijk aantonen dat $nk|n$, maar dat hoef je hier niet te doen. Maak hiervan gebruik om aan te tonen dat $\Phi_n(q)\,|q-1$ in $\mathbb{Z}$, waarbij Φ_n de n-de cyclotome veelterm is.
   (e) Uit onderstaande tekening haal je meteen dat $|q - \lambda| > |q - 1|$ als $\lambda^n = 1$ en $\lambda \neq 1$. Maak gebruik van dit resultaatje om een contradictie uit te komen.



3. Beschouw de ring $\dfrac{\mathbb{Z}_2[X]}{X^2+1}$. Deze ring heeft 4 elementen. Is deze ring isomorf met $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, $\mathbb{Z}_4$, $\mathbb{F}_4$ of met geen van de drie? Leg uit.

4. Zij $A \in \mathbb{C}^{3\times 3}$ diagonaliseerbaar met 3 verschillende eigenwaarden λ_1, λ_2 en λ_3 en de bijhorende eigenvectoren v_1, v_2 en v_3. Beschouw de matrix $C \in \mathbb{C}^{6\times 6}$ waarbij

$$C = \begin{pmatrix} A & I \\ 0 & A \end{pmatrix}.$$

   (a) Vind de Jordanvorm J van C.

   (b) Vind een matrix P zodat $J = P^{-1}CP$.

16 21 januari 2011

Theorie

1. *Schriftelijk.*
   (a) Zij $G, *$ een groep en H een deelgroep van G van index 2.
   Toon aan dat H een normaaldeler is van G.
   (b) Zij $G, *$ een groep, $f : G \to H$ een groepsmorfisme en N een normaaldeler van H.
   Toon aan dat $f^{-1}(N)$ een normaaldeler is van G.

2. *Mondeling.*
   Zij R een ring en D een deelgroep van $R, +$. Bewijs dat
   $$\bar{\cdot} : R/D \times R/D \to R/D : (x + D, y + D) \mapsto (x + D) \,\bar{\cdot}\, (y + D) = (x \cdot y) + D$$
   goed gedefinieerd is als en slechts als D een ideaal is.

3. *Schriftelijk.*
   Zij V een eindigdimensionale vectorruimte en A een element van $\mathrm{Hom}(V, V)$.
   Bewijs in detail dat er een unieke A^* bestaat zodat $\langle A(v), w\rangle = \langle v, A^*(w)\rangle$.
   Duid aan waar je gebruikt dat V eindigdimensionaal is. Je hoeft geen tegenvoorbeeld te geven als V oneindigdimensionaal is.

Oefeningen

1. We bewijzen de eerste stelling van Sylow in verschillende stappen.
   Zij p een priemgetal en $G, *$ een groep.
   (a) Stel dat $p^k | \, |G|$ voor een $k \in \mathbb{N}_0$.
   Toon aan dat er een strikte deelgroep H van G bestaat zodat $p^k | \, |H|$ of dat $p| \, |Z(G)|$.
   (b) **Stelling van Gauss.**
   Toon aan dat wanneer $p| \, |G|$ er een element in G bestaat van orde p.
   Hint: toon dit eerst aan voor een commutatieve groep met de structuurstelling en pas dan in het algemeen.
   (c) **Eerste stelling van Sylow.**
   Als $p| \, |G|$ en k de grootste k is waarvoor $p^k | \, |G|$, dan heeft G een deelgroep S zodat $p^k = |S|$.

2. (a) Zij $R, +, \cdot$ een ring met eenheidselement en S een deelring zodat $1 \in S$. Beschouw de "equivalentie"
   "R is een domein als en slechts als S een domein is."
   Een van deze implicaties is foutief en de andere is juist. Bewijs de juiste implicatie en geef een tegenvoorbeeld voor de foutieve.
   (b) Zij $F \subseteq K$ een algebraïsche velduitbreiding en zij R een ring zodat $F \subseteq R \subseteq K$.
   Toon aan dat R een veld is.
   Geldt dit ook indien de uitbreiding niet algebraïsch is?

3. Zij F een veld en beschouw de veelterm f in $F[X]$ gegeven door $X^7 - 11$. Zij E het ontbindingsveld van f over F.
   Geef de uitbreidingsgraad van E over F met $F = \mathbb{Q}$, $F = \mathbb{R}$, $F = \mathbb{C}$ en $F = \mathbb{F}_2$.

4. Vind de Jordanvorm J van de matrix A.
   $$A = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 2 & 1 & -1 & -1 & -1 \\ 0 & 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 2 & 0 \\ -1 & 0 & 0 & 0 & 2 \end{pmatrix}$$
   Bereken de minimale veelterm en zoek een inverteerbare matrix P zo dat $A = P^{-1}JP$.

17 18 januari 2012

Theorie

1. *Schriftelijk.*
   Formuleer en bewijs de eerste isomorfismestelling voor groepen.

2. *Mondeling.*
   Geef en bewijs de stelling van Kronecker.

3. *Schriftelijk.*
   Waar of niet? Bewijs of geef een tegenvoorbeeld.

   "Als de ring R een domein is, dan is $(R[X])^{\times} = R^{\times}$."

Oefeningen

1. Gegeven is een groep G met $102\,(= 2 \cdot 3 \cdot 17)$ elementen, met $|Z(G)| = 2$.
   Toon aan dat
   (a) $|Z(G/Z(G))| = 1$.
   (b) $G/Z(G)$ heeft een deelgroep van orde 17.
   (c) G heeft een deelgroep van orde 34.

2. Stel dat R een HID is.
   (a) Bewijs dat elk priemideaal van R ook een maximaal ideaal is.
   (b) Zij f een surjectief ringmorfisme van R naar S met S een integriteitsdomein.
   Bewijs dat f ofwel een isomorfisme is ofwel S een veld.
   (c) Toon aan dat als de veeltermenring van R een HID is, R dan een veld moet zijn.

3. Zij p een priemgetal en $p \equiv 1 \bmod 3$. We beschouwen in deze oefening $\mathbb{F}_p$.
   (a) Toon aan dat er in $\mathbb{F}_p^{\times}$ een element van orde 3 bestaat.
   (b) Besluit dat $X^2 + X + 1$ een wortel heeft in $\mathbb{F}_p$.

4. Oefening over Jordanvorm met 6×6-matrix.

18 20 januari 2012

Theorie

1. *Schriftelijk.*
   Zij R een ring en D een deelgroep van $R, +$. Bewijs dat

   $$\bar{\cdot} : R/D \times R/D \to R/D : (x + D, y + D) \mapsto (x + D) \,\bar{\cdot}\, (y + D) = (x \cdot y) + D$$

   goed gedefinieerd is als en slechts als D een ideaal is.

2. Geef en bewijs de Stelling van Cayley.

3. Zij $F \subseteq K \subseteq E$ velduitbreidingen. Bewijs dat als E algebraïsch is over K en K over F, dan E algebraïsch is over F.

Oefeningen

1. Zij G een groep waarvoor $[G : Z(G)] = 6$. Hoeveel deelgroepen en normaaldelers heeft G die $Z(G)$ omvatten?

2. Zij R een ring met een eenheidselement en zij $f \in R[X]$. Slechts één van de volgende beweringen is waar. Bewijs de juiste bewering en geef een tegenvoorbeeld voor de andere bewering en leg precies uit wat er misloopt.

   $$\exists g \in R[X] : g(X - a) = f \Leftrightarrow f(a) = 0$$
   $$\exists g \in R[X] : (X - a)\, g = f \Leftrightarrow f(a) = 0$$

3. (a) Hoeveel irreducibele veeltermen van graad 5 bestaan er over $\mathbb{F}_2$?

   (b) Bereken de ontbindingsvelden van volgende veeltermen over $\mathbb{Q}$ en geef ook de uitbreidingsgraad.

   i. $X^3 + 1$

   ii. $X^6 + 2X^3 - 3$

   iii. $X^4 - 6X^2 - 7$

4. Zij $f : \mathbb{Z}_p[X] \to \mathbb{Z}_p^{n\times n}$ met $n \geq 2$ een ringmorfisme, $f(1) = \mathrm{I}_n$ en $f(X) = M$.

   (a) Toon aan dat f volledig bepaald is door $f(X)$.

   (b) Toon aan dat f nooit injectief is.

   (c) Toon aan dat f nooit surjectief is.

   (d) Zij $p = 3$, $n = 6$, $f(X) = M$, met

   $$M = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

   Geef de minimale veelterm van M. Hoeveel elementen bevat $\mathrm{Im}(f)$?

19 28 augustus 2012

Theorie

1. *Schriftelijk.*
   Zij $G, *$ een groep en N een normaaldeler van G. Geef de definitie van de quotiëntbewerking $\overline{*}$ op G/N. Bewijs dat dit de goede definitie is en dat $G/N, \overline{*}$ een groep is.

2. *Mondeling.*
   Zij R een HID en $x \in R$ met $x \neq 0$ en x geen eenheid. Bewijs dat x te schrijven is als een product van irreducibele elementen.
   Hints:

   - *Een contradictie.*
   - *Een stijgende keten van idealen kan nuttig zijn.*

3. *Mondeling.*
   Zij $K \subset E$ een velduitbreiding en $a, b \in E$ algebraïsch over K. Bewijs dat $a \cdot b$ algebraïsch is over K.

Snelheidsvraagjes.

1. *Zij $K \subset E$ een velduitbreiding en $a, b \in E$ transcendent over K. Is $a \cdot b$ dan ook transcendent over K?*

2. *Bespreek de inclusies tussen de volgende verzamelingen van $\mathbb{C}^{n \times n}$-matrices:*

   diagonaliseerbaar unitair normaal Hermitisch.

Oefeningen

1. Zij p een priemgetal.
   (a) Zij H een abelse groep van orde n en p een priemfactor van n. Maak gebruik van de structuurstelling voor eindige groepen om aan te tonen dat H een element van orde p heeft.
   (b) Zij $G, *$ een groep met orde p^r, $r \neq 0$.
      i. Toon aan met behulp van (a) dat er een element $g \in G$ bestaat met $\mathit{orde}\,(g) = p$ en $\langle g \rangle \triangleleft G$.
      ii. Toon met inductie op r aan dat er voor alle s, met $0 \leq s \leq r$, er een normaaldeler N in G bestaat met $|N| = p^s$.

2. Zij R een commutatieve ring met $1 \neq 0$ zo dat voor alle $a \in R$ er een $b \in R$ bestaat zo dat $a^2 b = a$. Toon aan dat elk priemideaal van R ook een maximaal ideaal van R is.

3. (a) Bereken $[\mathbb{Q}\left(\sqrt{2}, \sqrt[3]{4}\right) : \mathbb{Q}]$.
   (b) Beschouw het veld $\mathbb{Q}\,(\omega_3, \omega_7)$. Volgens de stelling van het primitieve element bestaat er een $\alpha \in \mathbb{Q}\,(\omega_3, \omega_7)$ zo dat $\mathbb{Q}\,(\alpha) = \mathbb{Q}\,(\omega_3, \omega_7)$.
      i. Zoek zo'n α.
      ii. Bereken $[\mathbb{Q}\,(\omega_3, \omega_7) : \mathbb{Q}]$.
      iii. Wat is de minimale veelterm van ω_7 over $\mathbb{Q}\,(\omega_3)$?
   (c) Bereken $\mathbb{F}_2\,(\alpha, \beta)$, waarbij α en β elementen zijn van een uitbreiding L van $\mathbb{F}_2$ met $\alpha^3 + \alpha + 1 = 0$ en $\beta^2 + \beta + 1 = 0$.

4. Gegeven de lineaire afbeelding $\mathcal{A} : \mathbb{C}^6 \to \mathbb{C}^6$ met matrix

$$A = \begin{pmatrix} 2 & -1 & 0 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & 0 & 0 & 0 \\ -1 & 0 & 1 & 4 & 1 & 1 \\ 1 & 0 & -1 & -1 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$$

ten opzichte van de standaardbasis van $\mathbb{C}$.
Bepaal de Jordanvorm J van A en geef P zo dat $J = P^{-1}AP$. Geef ook de karakteristieke veelterm en de minimale veelterm van $\mathcal{A}$.

20 Voorbeeldexamen

Theorie

1. *Mondeling.*

   (a) Zij $G, \cdot$ een groep. Definieer de *commutatordeelgroep* G' van G.

   (b) Toon aan dat G' een normale deelgroep is van G.

   (c) Zij $N \lhd G$. Toon aan dat G/N commutatief is als en slechts als $G' \subset N$.

   Bijvragen.
   Je krijgt de verzameling van niet-triviale deelgroepen

   $$\{\{1, -1\}, \{1, -1, i, -i\}, \{1, -1, j, -j\}, \{1, -1, k, -k\}\}$$

   van $\mathcal{Q}, \cdot$ gegeven. Welke van deze deelgroepen zijn normale deelgroepen? Waarom?
   Kan je nu met behulp van puntje (c) snel de commutatordeelgroep van $\mathcal{Q}$ berekenen? Met welke "bekende" groep is het quotiënt $\mathcal{Q}/\mathcal{Q}'$ isomorf?

2. *Schriftelijk.*
   Bewijs in detail de fundamentele stelling van de veldentheorie: voor een veld K en een niet-constante veelterm $f \in K[X]$ bestaat er een uitbreiding E van K zodat f een wortel heeft in E. Is het mogelijk om voor E een algebraïsche uitbreiding te kiezen?

3. *Schriftelijk.*
   Zij K een veld en A een nilpotente transformatie van een K-vectorruimte van index k. Bewijs dat

   $$\{0\} \subsetneq \operatorname{Ker}(A) \subsetneq \operatorname{Ker}(A^2) \subsetneq \cdots \subsetneq \operatorname{Ker}(A^{k-1}) \subsetneq \operatorname{Ker}(A^k) = V.$$

Deel II

Examens Algebra I – Kortrijk

21 Ergens in januari 2006

Theorie

De theorievragen zijn verloren gegaan.

Oefeningen

1. Een ring $(R, +, \cdot, 1)$ wordt een *geordende ring* genoemd als en slechts als er een niet-lege deelverzameling P van R bestaat die voldoet aan de volgende twee voorwaarden:

   - voor alle $a, b \in P$ geldt: $a + b$ en ab behoren tot P, en
   - voor alle $a \in R$ is aan juist één van de volgende voorwaarden voldaan: a behoort tot P, $a = 0$, of $-a$ behoort tot P.

   Men noemt de elementen van P positief, en P zelf noemt men de *positieve verzameling.*

   (a) Kan P een deelring zijn? Welke van de verzamelingen $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$ en $\mathbb{C}$ zijn geordende ringen?

   (b) Zij $(R, +, \cdot, 1)$ een geordende ring. Toon aan dat alle kwadraten in R (verschillend van 0) positief zijn. Bewijs dat R geen echte nuldelers heeft en karakteristiek 0 heeft. Wat concludeer je bijgevolg voor eindige ringen?

   (c) Zij $(R, +, \cdot, 1)$ een geordende ring met positieve verzameling P. Beschouw de veelterming $(R[X], +, \cdot, 1)$ en definieer de verzamelingen

   $$\begin{aligned} P[l] &= \left\{p(X) \in R[X] \,\middle|\, \text{de coëfficiënt van de laagstegraadsterm van } p(X) \text{ behoort tot } P\right\}, \\ P[h] &= \left\{p(X) \in R[X] \,\middle|\, \text{de coëfficiënt van de hoogstegraadsterm van } p(X) \text{ behoort tot } P\right\}. \end{aligned}$$

   Toon aan dat $R[X]$ zowel met de verzameling $P[l]$ als met de verzameling $P[h]$ een geordende ring is.

   (d) Zij $(R, +, \cdot, 1)$ een geordende ring met positieve verzameling P. Definieer de relatie $\sim$ op R door te stellen dat voor alle $a, b \in R$ geldt dat $a \sim b$ als en slechts als $b - a$ tot P behoort of $a = b$). Bewijs dat deze relatie een totale orderelatie definieert op R. Toon aan dat deze orderelatie voldoet aan

   - voor alle $a, b, c \in R$ geldt: $b \sim c \Rightarrow a + b \sim a + c$
   - voor alle $a, b, c \in R$ geldt: $((b \sim c)$ en $(0 \sim a)) \Rightarrow ba \sim ca$.

   (e) Neem de veeltermring $\mathbb{Z}[X]$ en een positieve verzameling P uit de geordende ring $(\mathbb{Z}, +, \cdot)$. Rangschik de monomen $\pm 1, \pm X, \pm X^2, \ldots$ van klein naar groot (zo mogelijk) volgens de ordes die horen bij de positieve verzamelingen $P[l]$ en $P[h]$.

2. Oefening over Jordanvorm.

3. Zij $G, *$ een groep. We definiëren voor $x, y \in G$ de commutator van x en y als

   $$[x, y] = x^{-1} * y^{-1} * x * y.$$

   (a) De verzameling $\left\{[x, y] \,\middle|\, x, y \in G\right\} \subseteq G$ is niet noodzakelijk een deelgroep van $G, *$. Wat kan er fout lopen?
   Zoek geen tegenvoorbeeld: het loopt pas fout bij groepen met een hele hoge orde.

   (b) Definieer de commutatordeelgroep $[G, G], *$ van G als

   $$[G, G] = \operatorname{grp}\left\{[x, y] \,\middle|\, x, y \in G\right\}.$$

   Wat gebeurt er als G abels is? Geldt het omgekeerde ook?

(c) Bewijs volgende uitspraken.

   i. $[G, G]$ is een normaaldeler van G.
   ii. $G/[G, G]$ is Abels.
   iii. Als N een normaaldeler is van G, en G/N is Abels, dan is $[G, G]$ een deelverzameling van N.
   iv. Als H een deelgroep is van G en $[G, G]$ is een deelverzameling van H, dan is H een normaaldeler en G/H is Abels.

(d) De quotiëntgroep $G/[G, G]$ noemen we de abelianisatie van G. Bepaal de abelianisatie van $\mathcal{D}_4$. Met welke bekende groep is deze abelianisatie isomorf?

4. Beschouw de quotiëntring $\dfrac{\mathbb{Z}[i]}{(5)}, +, \cdot$.

   (a) Hoeveel elementen bevat deze ring? Verklaar.

   (b) De quotiëntring is isomorf met één van de volgende ringen:

   $$\mathbb{Z},\ \mathbb{Q},\ \mathbb{R},\ \mathbb{C},\ \mathbb{Z}_p,\ \mathbb{Z}_{p^2},\ \mathbb{Z}_p \oplus \mathbb{Z}_p,\ \mathbb{F}_{p^2}, \qquad \text{met } p \text{ priem.}$$

   Hou er door eliminatie nog één over.

   (c) Bewijs het isomorfisme uit (b).

   (d) Bereken de quotiëntring

   $$\frac{\mathbb{Z}_5[X, Y]}{(X^2 + Y + 1, Y - X)}.$$

   Is $\mathbb{Z}[i]/(5)$ hiermee isomorf?

Deel III

Examens Algebra I – Gent

22 21 februari 1992

Theorie

De theorievragen zijn verloren gegaan.

Oefeningen

1. Zij A een commutatieve ring met een eenheid. Zij $f \in A[X_1, \ldots, X_n]$. f bepaalt een (veelterm)functie
$$f : A \times \cdots \times A \to A : (a_1, \ldots, a_n) \mapsto f(a_1, \ldots, a_n).$$
Kan f de nulfunctie zijn als f niet de nulpolynoom is?
Anders geformuleerd wordt er gevraagd of de functie f de polynoom f volledig bepaalt.
Hint: neem $A = \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$. Bekijk polynomen in een veranderlijke.

2. Toon aan dat de volgende ringen isomorf zijn.
   (a) Gegeven twee families $(X_i)_{i \in I}$ en $(Y_i)_{i \in I}$ veranderlijken, dan is
$$A\left[(X_i)_{i \in I}\right] \cong A(Y_i)_{i \in I}$$
   (b) $A[X_1, \ldots, X_n] \cong A[X_1, \ldots, X_{n-1}][X_n]$.

3. Definieer “graad”functies
$$\begin{aligned} \deg &: A[X_1, \ldots, X_n] \to \mathbb{Z} \\ \deg_{X_i} &: A[X_1, \ldots, X_n] \to \mathbb{Z} \end{aligned}$$
Wat is de graad van het product van polynomen?
Toon aan dat als A een domein is, $A[X_1, \ldots, X_n]$ ook een domein is.

4. Zij $\mathcal{S} = \{f_i(X_1, \ldots, X_n) = 0\}_{i \in \mathcal{F}}$ een stelsel vergelijkingen over de complexe getallen, i.e. $f_i(X_1, \ldots, X_n) \in \mathbb{C}[X_1, \ldots, X_n]$. Zij I het ideaal voortgebracht door de polynomen f_i. Stel
$$\mathcal{V}(I) = \left\{(a_1, \ldots, a_n) \in \mathbb{C}^n \,\middle|\, (a_1, \ldots, a_n) \text{ is een nulpunt van het stelsel } \mathcal{S}\right\}.$$
Wordt I volledig bepaald door $\mathcal{V}(I)$?
Anders geformuleerd wordt er gevraagd of de verzameling van polynomen die nul worden in alle elementen van $\mathcal{V}(I)$ het ideaal I is.

23 6 maart 1992

Theorie

De theorievragen zijn verloren gegaan.

Oefeningen

1. Zij K een veld en $K[X,Y]$ de veeltermenring in twee veranderlijken over K. Beschouw het ideaal voortgebracht door X en Y, $I = (X,Y)$. Toon aan dat I^n/I^{n+1} en A/I^n eindig dimensionale K-vectorruimten zijn. Bepaal de dimensies.

2. Zij A een ring en $A[X_1,\ldots,X_n]$ de veeltermenring over A. Als $a_1,\ldots,a_n$ willekeurige eenheden zijn in A en $b_1,\ldots,b_n$ willekeurige elementen in A, dan geldt
$$A[X_1,\ldots,X_n] = A[a_1X_1+b_1,\ldots,a_nX_n+b_n].$$

3. Zij K een veld en $y_1,\ldots,y_n \in K$. Toon aan dat
   (a) Voor alle $x_1,\ldots,x_n \in K$ bestaat er een unieke veelterm $P(X) \in K[X]$ met $\deg(P(X)) \leq n-1$ zo dat
   $$\forall x_i \text{ is } P(x_i) = y_i.$$
   (b) Deze veelterm $P(X)$ is van de vorm
   $$u_0 + u_1(X-x_1) + \cdots + u_{n-1}(X-x_1)\cdots(X-x_{n-1})$$
   met $u_i \in K$.

4. Zij K een veld en $A = K[X,Y,Z]$. Beschouw het ideaal $I = \left(X^2-Y^3, Y^2-Z^3\right)$. Toon volgende zaken aan.
   (a) Zij $B = A/I$ een elk element $\alpha \in B$ de klasse is van een veelterm $F(X,Y,Z)$ met $\deg_X(F) \leq 1$ en $\deg_Y(F) \leq 1$.
   (b) Definieer het ringhomomorfisme φ door
   $$\varphi : K[X,Y,Z] \to K[T] : \begin{cases} \lambda & \mapsto \lambda \quad \text{als } \lambda \in K \\ X & \mapsto T^9 \\ Y & \mapsto T^6 \\ Z & \mapsto T^4 \end{cases}$$
   Bepaal $\operatorname{Ker}\varphi$. Toon aan dat I een priemideaal is.
   (c) Zij $L = \mathcal{Q}(B)$ het breukenveld van B, dan geldt $L \cong K(T)$.

5. Zij A een domein. Een kleinste gemeen veelvoud $\operatorname{kgv}(a,b)$ van $a,b \in A$ is een element k zo dat
   - $a|k$ en $b|k$,
   - als er $l \in A$ bestaat met $a|l$ en $b|l$, dan volgt $k|l$.

   (a) Toon aan dat twee elementen een kgv in A bezitten als en slechts als $(a)\cap(b)$ een hoofdideaal is.
   (b) Stel dat a en b irreducibel zijn en $(a) \neq (b)$. Toon aan dat als a en b een kgv hebben, dan $(a)\cap(b) = (ab)$.
   (c) Toon aan dat A een UFD is als en slechts als voor alle $a \in A \setminus \{0\}$ en $a \neq A^\times$, a het product is van irreducibele elementen en elk koppel $a,b \in A$ een kgv heeft in A.
   (d) Toon aan dat een UFD waarin elk eindig voortgebracht ideaal een hoofdideaal is noodzakelijk een HID is.

24 27 april 1992

Theorie

De theorievragen zijn verloren gegaan.

Oefeningen

1. Zij A een domein. Als a een eenheid is in A bestaat er een uniek automorfisme $\sigma A[X] \to A[X]$ zo dat $\sigma|_A = \mathrm{Id}$ en $\sigma(X) = aX + b$.
   Bepaal σ^{-1}.

2. (a) Zij $\mathbb{F}_p(t)$ het breukenveld van $\mathbb{F}_p[t]$. Zij $f(t), g(t) \in \mathbb{F}_p[t]$ met $\deg(f(t)) > 1$, $g(t) \neq 0$, $\deg(f(t)) > \deg(g(t))$ en $f(t)$ en $g(t)$ relatief priem.
   Toon aan dat $\mathbb{F}_p(t)$ een algebraïsche uitbreiding is van $\mathbb{F}_p\left(\dfrac{f(t)}{g(t)}\right)$.
   Toon aan dat de minimale veelterm $p_t(X)$ van t over $\mathbb{F}_p\left(\frac{f(t)}{g(t)}\right)$ gelijk is aan
   $$p_t(X) = f(X) - \frac{f(t)}{g(t)} g(X) \in \mathbb{F}_p\left(\frac{f(t)}{g(t)}\right)[X].$$
   Hint: stel $\frac{f(t)}{g(t)} = Y$, Y is transcendent over $\mathbb{F}_p$. Bewijs dat $p_t(X)$ ($= p_t(Y,X)$) als veelterm in $\mathbb{F}_p[Y,X] \cong \mathbb{F}_p[Y][X] \cong \mathbb{F}_p[X][Y]$ irreducibel is. Merk op dat $p_t(Y,X)$ irreducibel is in $\mathbb{F}_p(X)[Y]$.

   (b) Geef een voorbeeld van $\alpha = \frac{f(X)}{g(X)} \in \mathbb{F}_p(t)$ zodat $\mathbb{F}_p(t)/\mathbb{F}_p(\alpha)$ een inseperabele uitbreiding is en zo dat $\mathbb{F}_p(t)/\mathbb{F}_p(\alpha)$ een seperabele uitbreiding is.

3. Toon aan dat voor alle $n \in \mathbb{N}$, $n > 1$, er een veelterm $f \in \mathbb{F}_p[X]$ bestaat met $\deg(f(X))$ en f irreducibel.

4. Welke velden treden op als quotiënten (daarmee bedoelen we als homomorfe beelden) van de ring $\mathbb{F}_p[X]$?

5. Zij K een veld en L/K een Galoisuitbreiding met Galoisgroep G. Beschouw een stelsel vergelijkingen over K:
   $$f_i(X_1, \ldots, X_n) = 0, \qquad \text{met } i \in \{1, \ldots, m\}.$$
   Zij $I = (f_1, \ldots, f_m)$ het ideaal in $K[X_1, \ldots, X_n]$ voortgebracht door de f_i's. Definieer
   $$\mathcal{V}(I) = \left\{g : K[X_1, \ldots, X_n] \to L \middle| g \text{ is een } K\text{-algebrahomomorfisme met } I \subset \operatorname{Ker} g\right\}.$$
   Interpreteer $\mathcal{V}(I)$ als de verzameling van oplossingen (nulpunten) van het stelsel $\{f_i\}$ in L. Toon aan dat de Galoisgroep G op een natuurlijke manier werkt op $\mathcal{V}(I)$, dus dat elke $\sigma \in G$ een afbeelding $\sigma : \mathcal{V}(I) \to \mathcal{V}(I)$. Is deze σ injectief, surjectief?
   Interpreteer σ ook als afbeelding op de nulpunten. Wat zijn de vaste punten van de actie van σ op $\mathcal{V}(I)$, bepaal dus $(\mathcal{V}(I))^G$.

6. Zij K een veld, $n \in \mathbb{N}$ met $n > 1$ en $\mathrm{ggd}(n, \mathrm{char}(K)) = 1$.
   Toon aan dat het ontbindingsveld van de veelterm $X^n - 1$ een abelse uitbreiding is van K.
   Wat weet je over de uitbreidingsgraad?

7. Toon aan dat $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$ als en slechts als $n|m$.

25 Ergens in juni 1992

Theorie

De theorievragen zijn verloren gegaan.

Oefeningen

1. Zij A een domein. Een kleinste gemeen veelvoud $\operatorname{kgv}(a,b)$ van $a,b \in A$ is een element k zo dat
   - $a|k$ en $b|k$,
   - als er $l \in A$ bestaat met $a|l$ en $b|l$, dan volgt $k|l$.

   (a) Stel dat a en b irreducibel zijn en $(a) \neq (b)$. Toon aan dat als a en b een kgv hebben, dan $(a) \cap (b) = (ab)$.

   (b) Toon aan dat A een UFD is als en slechts als voor alle $a \in A \setminus \{0\}$ en $a \neq A^{\times}$, a het product is van irreducibele elementen en elk koppel $a,b \in A$ een kgv heeft in A.

   (c) Toon aan dat een UFD waarin elk eindig voortgebracht ideaal een hoofdideaal is, noodzakelijk een HID is.

2. Zij $\mathbb{F}_p(t)$ het breukenveld van $\mathbb{F}_p[t]$. Zij $f(t), g(t) \in \mathbb{F}_p[t]$ met $\deg(f(t)) > 1$, $g(t) \neq 0$, $\deg(f(t)) > \deg(g(t))$ en $f(t)$ en $g(t)$ relatief priem.

   (a) Toon aan dat $\mathbb{F}_p(t)$ een algebraïsche uitbreiding is van $\mathbb{F}_p\left(\dfrac{f(t)}{g(t)}\right)$.

   (b) Toon aan dat de minimale veelterm $p_t(X)$ van t over $\mathbb{F}_p\left(\frac{f(t)}{g(t)}\right)$ gelijk is aan
   $$p_t(X) = f(X) - \frac{f(t)}{g(t)} g(X) \in \mathbb{F}_p\left(\frac{f(t)}{g(t)}\right)[X].$$

3. Zij p een oneven priemgetal, ω een primitieve p-de eenheidswortel en $K = \mathbb{Q}(\omega)$ het p-de cyclotomisch veld.

   (a) Beschrijf de deelvelden van K.

   (b) Geef alle deelvelden van $\mathbb{Q}(\omega)$ met ω de elfde primitieve eenheidswortel.

4. Zij $A = \dfrac{\mathbb{Q}[X,Y,Z]}{(X^3+2)}$. Toon aan dat A een UFD is. *Hint: toon aan dat A isomorf is met een UFD.*

5. Zij K een veld en I een ideaal in $A = K[X_1, \ldots, X_n]$. Beschouw de verzameling van de nulpunten van I:
   $$\mathcal{V}(I) = \left\{(a_1, \ldots, a_n) \in K^n \middle| f(a_1, \ldots, a_n) = 0 \text{ voor alle } f \in I\right\}.$$
   Toon aan dat

   (a) als I en J idealen in A zijn, dan geldt dat $\mathcal{V}(IJ) = \mathcal{V}(I) \cup \mathcal{V}(J)$.

   (b) als $\{I_n\}_n$ een familie idealen in A is, dan is $\mathcal{V}\sum_n I_n = \bigcap_n \mathcal{V}(I_n)$.

   (c) $\mathcal{V}(I) \subset \mathcal{V}(J)$ als en slechts als $\operatorname{Rad}(J) \subset \operatorname{Rad}(I)$. Het radicaal van I is per definitie
   $$\operatorname{Rad}(I) = \left\{x \in A \middle| \text{er bestaat een } n \in \mathbb{N} \text{ zodat } x^n \in I\right\}.$$

   (d) er een bijectie is tussen de verzameling $\mathcal{V}(I)$ en de verzameling van K-homomorfismen $\operatorname{Hom}_K(A/I, K)$.

6. Zij $K = \mathbb{Q}(\sqrt{a})$ met $a \in \mathbb{Z}_0^-$. Toon aan dat er geen inbedding van K in een cyclische uitbreiding over $\mathbb{Q}$ van graad vier bestaat.

7. Zij $\overline{\mathbb{Q}}$ de algebraïsche sluiting van $\mathbb{Q}$. Zij E een maximaal deelveld van $\overline{\mathbb{Q}}$ dat $\sqrt{2}$ niet bevat. Leg uit waarom zo'n veld al dan niet bestaat. Toon aan dat elke eindige uitbreiding van E een cyclische uitbreiding is.

8. Zij E een algebraïsche uitbreiding van een veld K van karakteristiek 0, waarin elke veelterm $f \in K[X]$ met de graad $\deg(f) \geq 1$ minstens één wortel heeft. Toon aan dat E algebraïsch gesloten is.

26 Ergens in september 1992

Theorie

De theorievragen zijn verloren gegaan.

Oefeningen

1. Zij R een hoofdideaaldomein. Stel I en J idealen van R. Toon aan dat er een bijectie $f : I \to J$ bestaat waarvoor geldt dat
   - $f(u+v) = f(u) + f(v)$ voor alle $u, v \in I$
   - $f(ru) = rf(u)$ voor alle $r \in R$ en voor alle $u \in u$.
2. Geef een voorbeeld van een inseperabele uitbreiding L/K zo dat $\mathrm{Aut}_K(L) \cong \mathbb{Z}/3\mathbb{Z}$.
3. Toon aan dat als L/K een Galoisuitbreiding is, L het ontbindingsveld is van één polynoom.

27 11 februari 1993

Theorie

De theorievragen zijn verloren gegaan.

Oefeningen

1. Zij V een eindigdimensionale K-vectorruimte en zij $\mathrm{End}_K(V)$ de ring van endomorfismen van V. Zij $\varphi \in \mathrm{End}_K(V)$ en M het $K[X]$-moduul bepaald door (V, φ), dit wil dus zeggen dat $M, + = V, +$ en dat scalaire vermenigvuldiging wordt gegeven door

$$K[X] \times V \to V; (f(X), v) \mapsto f(X) \cdot = f(\varphi)(v).$$

   Toon aan dat volgende eigenschappen equivalent zijn:

   - $K[X] / \mathrm{Ann}(M)$ is een domein
   - $K[X] / \mathrm{Ann}(M)$ is een veld

   Toon aan dat als deze eigenschappen gelden, φ dan een isomorfisme is. Geldt het omgekeerde ook?

2. Bepaal een irreducibele veelterm $f(X, Y)$ in $\mathbb{F}_q[X, Y]$ zo dat het breukenveld van $\dfrac{\mathbb{F}_q[X, Y]}{f(X, Y)}$

   - een inseperabele uitbreiding van $\mathbb{F}_p(Y)$ is,
   - een Galoisuitbreiding is met Galoisgroep V, de Viergroep van Klein.

28 9 februari 1994

Theorie

De theorievragen zijn verloren gegaan.

Oefeningen

1. Stel dat $K = \mathbb{F}_9(t)$, met t transcendent over $\mathbb{F}_9$ en dat $f(X) = X^4 - t \in K[X]$.
   (a) Bewijs dat f irreducibel is over K.
   (b) Bewijs dat $X^2 + 1$ irreducibel is over K.
   (c) Stel dat α een wortel is van f in een algebraïsche sluiting van K. Bewijs dat $L = K(\alpha)$ het ontbindigsveld van f is.
   (d) Bepaal de Galoisgroep $G = \mathrm{Gal}(L/K)$.
   (e) Geef alle deelgroepen van G en de corresponderende tussenvelden.
   (f) Geef voor elk tussenveld E van K en L de minimale veelterm van de uitbreiding L/E en E/K.

2. Stel dat R een commutatieve ring is. Een ideaal I in R wordt *primair* genoemd als

$$ab \in I \text{ en } a \notin I \Rightarrow \text{er bestaat een } m \in \mathbb{N} \text{ zodat } b^m \in I.$$

   Het *radicaal* van I is het ideaal gedefinieerd als

$$\mathrm{Rad}(I) = \left\{ r \in R \middle| \text{er bestaat een } m \in \mathbb{N} \text{ zodat } r^m \in I \right\}.$$

   (a) Bewijs dat het radicaal van een primair ideaal priem is.
   (b) Bewijs dat als I en J idealen van R zijn zodat
   - $I \subseteq J$,
   - $b \in J \Rightarrow \exists m \in \mathbb{N} : b^m \in I$,
   - $ab \in I, a \notin I \Rightarrow b \in J$,

   dan is I primair en $J = \mathrm{Rad}(I)$.

29 30 augustus 1994

Theorie

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

1. De kern van een ringmorfisme naar een veld is een priemideaal.
2. Als E/F een transcendente velduitbreiding is, dan is elk element in E/F transcendent over F.
3. Elke eindige uitbreiding is algebraïsch, maar niet elke algebraïsche uitbreiding is eindig.
4. Als $E/K/F$ velduitbreidingen zijn en E/F is Galois, dan ook E/K en K/F.
5. $\mathbb{Z}[i, X]$ is een UFD, maar geen HID.

Oefeningen

1. Stel dat j een wortel is van de veelterm
$$X^2 + X - 1 \in \mathbb{F}_3[X]$$
in een algebraïsche sluiting van $\mathbb{F}_3$. Noteer $K = \mathbb{F}_3(j)$ en beschouw de veelterm
$$f(X) = X^4 + jX - j \in K[X].$$
Voor vraag 1 tot en met 5 mag je veronderstellen dat f irreducibel is over K.
   (a) Bewijs dat $K \cong \mathbb{F}_9$.
   (b) Stel de vermenigvuldigingstabel op voor K.
   (c) Stel dat α een wortel is van f in een algebraïsche sluiting van K.
      i. Bewijs dat $L = K(\alpha)$ het ontbindingsveld is van f.
      ii. Bepaal het aantal elementen van L.
      iii. Bepaal de Galoisgroep van f over K.
   (d) Bewijs dat er uniek echt tussenveld E bestaat tussen K en L en bepaal er een primitief element voor over K. Hierbij kunnen volgende gegevens van pas komen
$$\begin{aligned}\alpha^{81} &= (1-j)\alpha^3 + \alpha^2 + (j-1)\alpha,\\ \alpha^{162} &= \alpha^3 + (j+1)\alpha^2 + (j+1)\alpha,\\ \alpha^{243} &= (1-j)\alpha^3 + (j+1)\alpha^2 + \alpha.\end{aligned}$$
   (e) Bepaal de minimale veelterm van de uitbreiding E/K.
   (f) Bewijs dat f irreducibel is over K.
2. Stel dat R een commutatieve ring met 1 is.
   (a) Bewijs dat voor alle $a \in R$ de verzameling
$$\mathrm{Ann}(a) = \{ r \in R |\, ar = 0\}$$
een ideaal is in R.
   (b) Bewijs dat als additieve groepen $R/\mathrm{Ann}(a) \cong (a)$.
   (c) Veronderstel verder dat
      - R oneindig veel elementen heeft,
      - voor elk niet-nul ideaal I in R geldt dat R/I een eindige verzameling is.

      Bewijs volgende zaken onder deze gegeven voorwaarden.
      i. Elk niet-nul ideaal in R is oneindig.
      ii. Alle priemidealen in R zijn maximaal.
      iii. R is een domein.

      Geef voorbeelden van ringen R van elke mogelijke karakteristiek die geen velden zijn en aan de gegeven voorwaarden voldoen.

30 18 november 1994

Theorie

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

1. Zij $R, +, \cdot$ een ring, $I \triangleleft R$ en $I \neq R$. Er bestaat dan een ideaal $J \triangleleft R$, $J \neq R$ zo dat R/J een veld is en voor alle $r \in I$ geldt dat $r \bmod J = 0$.
2. Zij R een hoofdideaal domein en $P \triangleleft R$ een priemideaal, $P \neq 0$, dan is R/P een veld.
3. Alle domeinen R zijn hoofdideaal domeinen.
4. Stel $f(X), g(X) \in \mathbb{Z}[X]$ en $g(X) \neq 0$. Er bestaan polynomen $q(X), r(X) \in \mathbb{Z}[X]$ zo dat
$$f(X) = g(X)q(X) + r(X)$$
waarbij $\deg(r(X)) < \deg(g(X))$ of $r(X) = 0$.
5. Als I en J idealen zijn in een ring R geldt steeds $I \cap J = IJ$.
6. De volgende ringen zijn isomorf:
$$\frac{\mathbb{Z}[X]}{(2, X)(3, X^2 - X)} \cong \frac{\mathbb{Z}[X]}{(2, X)} \times \frac{\mathbb{Z}[X]}{(3, X^2 - X)} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$
7. Er zijn geen surjectieve morfismen van een veld naar een ring met echte nuldelers.
8. Zij $\varphi : R \to S$ en $\psi : R \to S'$ ringmorfismen.
   (a) Als $\operatorname{Ker}\varphi = \operatorname{Ker}\psi$, hebben $\varphi = \psi$ isomorfe beelden.
   (b) Als $\operatorname{Ker}\varphi \cong \operatorname{Ker}\psi$, hebben $\varphi = \psi$ 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 hoef je niet te verklaren of verifiëren).
Als $a, b \in R$ en $a \neq b$ geldt $\operatorname{Ker}\varphi_a \neq \operatorname{Ker}\varphi_b$.

Oefeningen

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 $\left(2X^3 + 2X^2 + 2X + 4\right)\mathbb{Z}[X]$ een priemideaal in $\mathbb{Z}[X]$?
2. Zij $f(X) \in \mathbb{F}_p[X]$ en stel $f(a) = 0$ voor alle $a \in \mathbb{F}_p$. Toon aan dat
$$f(X) = (X^p - X)\, h(X)$$
met $h(X) \in \mathbb{F}_p[X]$.
3. Zij K een veld, $K[X]$ een veeltermring in één variabele over K. Zij I een echt ideaal in $K[X]$.
   (a) Bewijs dat er een polynoom $f(X) \in K[X]$ bestaat zo dat $I = (f(X))$.
   (b) Zij $A = K[X]/I$. Bewijs dat er een inbedding van K in A bestaat.
   (c) Bewijs dat A een K-vectorruimte is.

(d) Stel $I = (f(X))$, $d = \deg(f(X))$ en $\bar{X}$ is de klasse van X in de quotiëntring A. Bewijs dat
$$\{1, \bar{X}, \bar{X}^2, \bar{X}^3, \ldots, \bar{X}^{d-1}\}$$
een lineair voortbrengend deel is voor de K-vectorruimte A.

(e) Bewijs dat $\dim_K A = d$.

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

   (a) Bewijs dat R een commutatieve ring is van karakteristiek 2.

   (b) Bewijs dat alle priemidealen van R maximale idealen zijn.

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

   (d) Bewijs dat R een $\mathbb{F}_2$-vectorruimte is.

   (e) Bewijs dat als R een eindige dimensionale $\mathbb{F}_2$-vectorruimte is dan geldt dat R ringisomorf is met
   $$\underbrace{\mathbb{F}_2 \times \mathbb{F}_2 \times \cdots \times \mathbb{F}_2}_{n},$$
   waarbij $n = \dim_{\mathbb{F}_2} R$.
   Hint: Inductie op de dimensie van R over $\mathbb{F}_2$. Beschouw elementen $e, e-1 \in R$, met $e \neq 0$, $e \neq 1$. Gebruik de Chinese Reststelling.

31 20 december 1994

Theorie

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

1. Zij R een UFD en K het breukenveld van R.
   (a) Zij $r \in R$ een irreducibel element. Rr is dan 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.
2. Zij K een veld en L een velduitbreiding van K. Zij
   $$\varphi : K[X,Y] \to L$$
   een K-algebra homomorfisme met $\operatorname{Ker}\varphi = P$. We veronderstellen dat P een niet-nul priemideaal in $K[X,Y]$ is dat niet maximaal is. Er geldt nu
   (a) $\varphi(X)$ of $\varphi(Y)$ is transcedent over K.
   (b) de verzameling $\{\varphi(X), \varphi(Y)\}$ is algebraïsch onafhankelijk over K.
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 wortel van $f(X)$ zijn elementen van $K(\alpha)$.
   (c) $K(\alpha^2) = K(\alpha)$.

Oefeningen

1. Zij $\alpha \in \mathbb{C}$ een wortel van de veelterm $X^3 + 26X + (3+2i)$ over $\mathbb{Q}(i)$.
   Bepaal het minimale polynoom van α over $\mathbb{Q}$.
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 $X^3 + X + 1$.
   (b) Factoriseer $X^2 + X + \alpha$ over het veld $\mathbb{F}_8$.
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 $\operatorname{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha))$, $\operatorname{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha, i))$, $\operatorname{Hom}_{\mathbb{Q}}(\mathbb{Q}(\alpha), \mathbb{C})$ en $\operatorname{Hom}_{\mathbb{Q}}(\mathbb{Q}(\alpha, i), \mathbb{C})$.
   (e) Bepaal de minimale polynoom van $(1+i)\alpha$ over $\mathbb{Q}$.
   (f) Van welke deelgroep $H < \operatorname{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha, i))$ is $\mathbb{Q}((1+i)\alpha)$ het fixveld?

32 14 november 1995

Theorie

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

   (b) Beschouw volgende redenering. Toon met een tegenvoorbeeld aan dat dit besluit fout is. Waar loopt de redenering mis?
   Zij $N = \{a \in R | a$ *is een nuldeler*$\} \cup \{0\}$.
   Zij $a \in N$. *Elk veelvoud* ab, *met* $b \in R$ *is een element van* N. *Namelijk, neem* $r \in R$ *met* $r \neq 0$ *zo dat* $ra = 0$ *en dan volgt* $r(ab) = (ra)b = 0$, *wat impliceert dat* $ab = 0$ *of dat* ab *een nuldeler is.*
   N *is eveneens gesloten onder de optelling. Stel* $c, d \in N$ *en kies* $r, s \in R$ *met* $r \neq 0$ *en* $s \neq 0$ *zodat* $rc = 0$ *en* $sd = 0$. *Er geldt op die manier* $rs(c+d) = src + rsd = 0$, *waardoor* $c + d$ *ofwel nul is ofwel een nuldeler. We besluiten dat* N *een ideaal is in* R.

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

   (a) Definieer de quotiëntring R/I en formuleer de isomofismestelling.

   (b) Zij $\varphi : R \to S$ een surjectief ringmorfisme. Veronderstel dat $\operatorname{Ker}\varphi \subset I$. Bewijs dan dat $\varphi^{-1}(\varphi(I)) = I$.

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

   $$\begin{aligned} \pi_I &: R \to R/I \\ \pi_J &: R \to R/J. \end{aligned}$$

   Er bestaat dan een uniek morfisme

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

   zo dat $\beta \circ \pi_J = \pi_I$ als en slechts als...
   Vul aan en verklaar!

Oefeningen

1. Factoriseer de polynoom
   $$X^5 + X^4 + X^3 + X^2 - X - 1$$
   in irreducibele factoren respectievelijk over de velden
   $$\mathbb{Q}, \mathbb{F}_2, \mathbb{F}_3 \text{ en } \mathbb{F}_4.$$

2. Bepaal $r, s \in R$ zo dat
   $$ra + sb = \operatorname{ggd}(a, b)$$
   met

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

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

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

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

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

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 met M een maximaal ideaal in R.

   (c) Beschrijf de canonische surjectie

$$\theta : R \to R/M.$$

33 12 december 1995

Theorie

1. Bepaal alle deelringen van het eindig veld $\mathbb{F}_{p^n}$ met p priem.
2. (a) Zij R een UFD. Toon aan dat elk element in $R[X]$ een product is van priemelementen.
   (b) Geef een voorbeeld van een niet-Noethers UFD.
3. Zij A een eindig voortgebrachte K-algebra en φ een K-homomorfisme ($\varphi/K = \mathrm{Id}_K$)
$$\varphi : A \to K[X],$$
zo dat $X \in \mathrm{Im}\varphi$.
   (a) Toon aan dat A niet algebraïsch is over K.
   (b) Toon aan dat A een deelalgebra B bevat zo dat
$$\varphi/B : B \to K[X]$$
   een isomorfisme is.

Oefeningen

1. (a) Toon aan dat $f(X) = X^4 + X + 1$ irreducibel is over $\mathbb{F}_2$.
   (b) Zij $\alpha \in \mathbb{F}_2^\alpha$ 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 zo dat
$$T(\beta) = \beta + \beta^2 + \beta^4 + \beta^8 = 1.$$
   Bepaal dit element.
   (d) Bepaal de wortels van
$$\alpha^4 X^3 + \alpha X^2 + 1$$
   in $\mathbb{F}_2^\alpha$.
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
   (a) $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$
   (b) $[\mathbb{Q}(\alpha, \beta, \gamma) : \mathbb{Q}(\alpha)]$
   (c) $[\mathbb{Q}(\alpha, \beta, \gamma) : \mathbb{Q}]$
3. Zij d een kwadraatvrij getal. Bewijs dat alle getallen in $\mathbb{Z}[\omega_d]$ in het complexe vlak construeerbaar zijn met passer en liniaal.
4. Bepaal de minimale veelterm 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) $\sqrt[3]{5} \cdot \sqrt{2}$ over $\mathbb{Q}$.
5. (a) Hoeveel deelvelden in $\mathbb{Q}^a$ bestaan er die isomorf zijn met $\mathbb{Q}\left(\sqrt[4]{3}\right)$.
   (b) Zij α een algebraïsch element over $\mathbb{Q}$. Toon aan dat het aantal deelvelden van $\mathbb{Q}(\alpha)$ eindig is.

34 Ergens in februari 1996 (1)

Theorie

1. Zij R een uniek factorisatie domein (UFD) en 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 $a_i \equiv \mathrm{mod} p$. Als $f(X) = g(X)h(X)$, $g(X), h(X) \in R[X]$, dan is

$$\begin{aligned} g(X) &= X^d + \sum_{i=0}^{d-1} b_i X^i, \qquad \text{met } b_i \bmod p, \\ h(X) &= X^f + \sum_{i=0}^{f-1} c_i X^i, \qquad \text{met } c_i \bmod p. \end{aligned}$$

   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 een injectief K-morfisme van $K[\alpha, \beta]$ naar de veeltermring $K[X]$.
   (a) Bewijs dat $\{\alpha, \beta\}$ een algebraïsch afhankelijke verzameling is.
   (b) Bewijs dat α transcendent is over K.
   (c) Bewijs dat β transcendent is over K.
   (d) Bewijs dat α algebraïsch is over $K(\beta)$.
   (e) Bewijs dat β algebraïsch is over $K(\alpha)$.

Oefeningen

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

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

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

3. Zij $f(X)$ een irreducibele polynoom over een veld K van karakteristiek nul. Stel dat $\alpha \in K^a$ een wortel is van f en er een $b \in K$ bestaat zo dat $K(\sqrt{b}) \subset K(\alpha)$.
   (a) Bewijs dat $\deg(f(X))$ even is.
   (b) Bewijs dat $f(X) = g(X)^2 + bh(X)^2$, met $g(X), h(X) \in K[X]$.

35 Ergens in februari 1996 (2)

Theorie

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

1. Alle maximale idealen in een ring zijn priem.
2. Als I en J twee comaxiale idealen zijn in een ring R, dan zijn I^n en J^n ook comaximaal in R.
3. Het ontbindingsveld van een eindige verzameling veeltermen over een veld K is een eindige uitbreiding van K.
4. Zij $\sigma : K \to K$ een automorfisme van velden. Zij $f(X) = \sum_i a_i X^i \in K[X]$ een irreducibele veelterm over K. Definieer
$$\sigma(f)(X) = \sum_i \sigma(a_i) X^i \in K[X].$$
Het aantal verschillende wortels van $\sigma(f)(X)$ in de algebraïsche sluiting van K is gelijk aan het aantal verschillende wortels van $f(X)$ in de algebraïsche sluiting van K.
5. Als $\alpha \in \mathbb{C}$ een wortel is van een monische veelterm $g(X) \in \mathbb{Z}[X]$, dan is de monische minimale veelterm van α, $f_\alpha(X)$, ook een veelterm over $\mathbb{Z}$, dus $f_\alpha(X) \in \mathbb{Z}[X]$.

Oefeningen

1. Factoriseer de volgende veeltermen.
   (a) $X^4 - X^2 - 1$ over $\mathbb{Q}$
   (b) $X^6 - X^3 - 1$ over $\mathbb{F}_3$
2. Bepaal de wortels van de veelterm
$$X^2 + X + \beta^2$$
in $\mathbb{F}_2^a$. Hierbij is $\beta \in \mathbb{F}_2^a$ zo dat $\beta^3 + \beta + 1 = 0$.
3. Zij d een kwadraatvrij geheel getal. Toon aan dat de niet-nul priemidealen in de ring $\mathbb{Z}\left[\sqrt{d}\right]$ maximale idealen zijn.
4. 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.

36 Ergens in augustus 1996

Theorie

1. Zij K een veld en L/K een velduitbreiding. Stel $X \subset L$ zo dat $L = K(X)$.
   Toon aan aan dat als elk element in X algebraïsch is over K, dan L/K een algebraïsche velduitbreiding is.

2. Zij K een veld en A, B K-algebra's. Met $\sigma : A \to B$ noteren we een K-algebra morfisme.
   Zijn volgende uitspraken juist of fout? Indien juist geef je een bewijs, indien fout geef je een tegenvoorbeeld.

   (a) Als $\alpha \in A$ met α K-algebraïsch, dan is $\sigma(\alpha)$ K-algebraïsch.

   (b) Als $\alpha \in A$ met α transcendent over K, dan is $\sigma(\alpha)$ transcendent over K.

   (c) Als $X \subset A$ met X K-algebraïsch afhankelijk, dan is $\sigma(X)$ (als verzameling) K-algebraïsch afhankelijk.

   (d) Als $X \subset A$ met X K-algebraïsch onafhankelijk, dan is $\sigma(X)$ (als verzameling) K-algebraïsch onafhankelijk.

Oefeningen

1. (a) Bewijs dat de veelterm $f(X) = X^3 - 3X - 1$ irreducibel is over $\mathbb{Q}$.

   (b) Zij $u \in \mathbb{R}$ met u een wortel van $f(X)$. Druk $u^4 + 2u^3 + 3$ uit als een lineaire combinatie van $1, u, u^2$. Gebruik hierbij het algoritme van Euclides in $\mathbb{Q}[X]$.

   (c) Bepaal de inverse van $3u^2 + 7u + 5$ in $\mathbb{Q}(u)$. Gebruik de stelling van Bezout in $\mathbb{Q}[X]$.

2. Zij K een veld en $f, g \in K[X]$ met $\deg(g) \geq 1$.
   Toon aan dat er unieke polynomen $f_0, \ldots, f_r \in K[X]$ bestaan zo dat
   $$f = f_0 + f_1 g + f_2 g^2 + \ldots + f_r g^r.$$

3. Zij R een ring, A een R-algebra en $\alpha \in A$.

   (a) Toon aan dat
   $$R[\alpha] \cong R[X]/I$$
   met I een ideaal in R.

   (b) Stel dat er een monische veelterm $g(X) \in R[X]$ zo dat $g(\alpha) = 0$. Bewijs dat het ideaal I uit punt (a) een hoofdideaal is dat voortgebracht wordt door een monische veelterm in $R[X]$.

37 12 november 1996

Theorie

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

1. Zij H, I, J idealen in R. Dan is
$$H \cap (I + J) = (H \cap I) + (H \cap J).$$
2. Zij R een Noethers domein waarin elk ideaal dat voortgebracht is door twee elementen een hoofdideaal. R is dan een hoofdideaaldomein (HID).
3. Zij $\sigma : \mathbb{C} \to \mathbb{C}$ een ringmorfisme en $\alpha \in \mathbb{C}$ een algebraïsch element over $\mathbb{Q}$. $\sigma(\alpha)$ is dan algebraïsch over $\mathbb{Q}$.
4. Elk rationaal getal $a \in \mathbb{Q}$ is algebraïsch over $\mathbb{Z}$.
5. Zij $f(X)$ een irreducibele veelterm over $\mathbb{Q}$ en $a, b \in \mathbb{C}$ wortels van $f(X)$.
   (a) $\mathbb{Q}[a]$ is dan een veld.
   (b) $\mathbb{Q}[a] \cong \mathbb{Q}[b]$.

Oefeningen

1. Zij $a = 1-7i \in \mathbb{Z}[i]$ en $b = 2-2i \in \mathbb{Z}[i]$. Bepaal $\mathrm{ggd}(a, b)$ en $s, t \in \mathbb{Z}[i]$ zo dat $\mathrm{ggd}(a, b) = sa+tb$ (gebruik recursie).
2. Factoriseer $X^4 + 2X^3 + X^2 + 1$ over $\mathbb{F}_5$.
3. Zij R een ring en $I, I_1, I_2, \ldots, I_n$ idealen in R. Definieer het radicaal van I als
$$\mathrm{Rad}(I) = \{r \in R \,|\, r^n \in I \text{ voor een zekere } n > 0\}.$$
   (a) Toon aan dat
      i. $\mathrm{Rad}(\mathrm{Rad}(I)) = \mathrm{Rad}(I)$
      ii. $\mathrm{Rad}(I_1 I_2 \cdots I_n) = \mathrm{Rad}\left(\bigcap_{j=1}^{n} I_j\right) = \bigcap_{j=1}^{n} \mathrm{Rad}(I_j)$
      iii. $\mathrm{Rad}(I^m) = \mathrm{Rad}(I)$
   (b) Stel $J \subset \mathrm{Rad}(I)$ is een eindig voortgebracht ideaal in R. Bewijs dat er dan een $n > 0$ bestaat zo dat $J^n \subset I$.
4. 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 $M = 0$.

38 17 december 1996

Theorie

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

1. Zij L/K een eindige velduitbreiding 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.
2. Zij $\alpha \in K^a$ een algebraïsch element over een veld K. Zij $K \subset L$ een velduitbreiding.
   (a) De minimale veelterm $f_{\alpha,K}(X)$ van α over K is een veelvoud van de minimaalveelterm $g_{\alpha,L}(X)$ van α over L.
   (b) Zij $f_{\alpha,K}(X)$ en $g_{\alpha,L}(X)$ zoals in (a). Dan is $\deg\left(f_{\alpha,K}(X)\right) > \deg\left(g_{\alpha,L}(X)\right)$.
3. Zij $f(X)$ een irreducibele veelterm over een veld K en $g(X)$ een willekeurige veelterm over K zo dat $f(X)$ en $g(X)$ een wortel $\alpha \in K^a$ gemeen hebben. Dan zijn alle wortels van $f(X)$ ook wortels van $g(X)$.
4. Zij $f(X)$ een primitieve veelterm over $\mathbb{Z}$. Dan is $f(X)$ irreducibel over $\mathbb{Z}$ als en slechts als $f(X)$ irreducibel is over $\mathbb{Q}$.
5. Zij R een ring en I een ideaal in R.
   (a) Als I het product is van verschillende maximale idealen in R, dan is R/I isomorf met het direct product van velden.
   (b) Als I het product is van maximale idealen in R, dan is R/I isomorf met het direct product van velden.
6. Een velduitbreiding is algebraïsch als en slechts als het een eindige uitbreiding is.
7. (a) Zij $\sigma : K \to K$ een automorfisme van velden. Zij $f(X) = \sum_i a_i X^i \in K[X]$ een irreducibele veelterm over K. Definieer $\sigma(f)(X) = \sum_i \sigma(a_i) X^i \in K[X]$. Dan is $\sigma(f)(X)$ ook irreducibel over K.
   (b) Zij $\sigma : K \to K$ een morfisme van velden. Zij $f(X) = \sum_i a_i X^i \in K[X]$ een irreducibele veelterm over K. Definieer $\sigma(f)(X) = \sum_i \sigma(a_i) X^i \in L[X]$. Dan is $\sigma(f)(X)$ ook irreducibel over L.
8. 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 $\deg(f(X)) = 2$. Zij $\alpha \in \mathbb{F}_p^a$ een wortel van $f(X)$ en $\beta \in \mathbb{F}_p^a$ een wortel van $g(X)$. Er geldt dan $\beta \in \mathbb{F}_p(\alpha)$.

Oefeningen

1. Beschrijf systematisch alle deelvelden van
   (a) $\mathbb{F}_{2^{12}}$
   (b) $\mathbb{F}_{3^{12}}$
2. Factoriseer 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 $\mathbb{Z}[i]$.
3. Zij $\alpha \in \mathbb{C}$ een wortel van $X^4 + (2+i)X + 5$. Bepaal de minimale veelterm van α 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 $\beta \in \mathbb{F}_2^a$ zo dat $\beta^3 + \beta + 1 = 0$.

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

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

39 Ergens in februari 2002

Theorie

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

1. Zij p, q verschillende priemgetallen in $\mathbb{Z}$. Zij $a, b \in \mathbb{Z}$ met $\text{ggd}\,(a-b, pq) = 1$. Het aantal oplossingen van $(X-a)\,(X-b) = 0$ in de ring $\mathbb{Z}/pq\mathbb{Z}$ is gelijk aan 2^2?
2. $((\mathbb{Z}/4\mathbb{Z})[X])^* = (\mathbb{Z}/4\mathbb{Z})^* = \{1 \bmod 4, 3 \bmod 4\}$.
3. De functie $\sin x$ is transcendent over $\mathbb{C}(\cos(45x))$.
4. Zij L het ontbindinsveld van een irreducibele veelterm van graad 3 over $\mathbb{Q}$. Dan is L ook het ontbindingsveld van een veelterm van graad 6 over $\mathbb{Q}$.
5. Zij $\alpha \in \mathbb{R}$ de wortel van een veelterm van graad 4 over $\mathbb{Q}$. α is dan construeerbaar.
6. Zij $f(X) \in \mathbb{Q}[X]$, $\deg f(X) = n \geq 1$. Zij L het ontbindingsveld van $f(X)$ en $\text{Gal}(L/\mathbb{Q}) \cong \mathcal{A}_n$, $n \geq 5$. Dan is $f(X)$ irreducibel en de enige deelvelden $E \subset L$ die galois zijn over $\mathbb{Q}$ zijn L en $\mathbb{Q}$.
7. Zij K een veld en I, J idealen in $\mathbb{C}\,[X_1, \ldots, X_n]$. Zij $V(T)$ de oplossingsverzameling van het stelsel vergelijkingen bepaald door een ideaal $T \subset \mathbb{C}\,[X_1, \ldots, X_n]$ en dan is $V\,(IJ) = V\,(I) \cup V\,(J)$.
8. Zij R een ring en M een uniek maximaal ideaal in R. Dan is $R^* = R \setminus M$.
9. Zij K een veld en $\bar{K}$ de algebraïsche sluiting van K. Zij $\alpha \in \bar{K}$ zo dat de minimale veelterm van α over K een meervoudige wortel heeft. Dan is $\text{Kar}(K) = p \neq 0$.
10. Zij $z \in \mathbb{Z}[i]$, z een irreducibel element. Dan is $\mathbb{Z}[i]/\,(z)$ een eindig veld.
11. $\mathbb{C}\,(\sin(x))$ is een velduitbreiding van $\mathbb{C}\,(\sin(45x))$ met $[\mathbb{C}\,(\sin(x)) : \mathbb{C}\,(\sin(45x))] = 45$.

Oefeningen

1. (a) Toon aan dat $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}, \sqrt{5}\right)$ een galoisuitbreiding van $\mathbb{Q}$ is. Bepaal de galoisgroep.
   (b) Zij $f(X) = X^3 + X^2 - 2X - 1 \in \mathbb{Q}[X]$. De disciminant van deze veelterm is 49. Toon aan dat het ontbindingsveld van $f\,(X)$ gelijk is aan $\mathbb{Q}(\alpha)$ met α een wortel van $f\,(X)$ in $\mathbb{C}$.
   Bepaal de andere wortels in functie van α.
   Bepaal de minimale veelterm van α^{-1} over $\mathbb{Q}$.
   (c) Bepaal de galoisgroep van $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}, \sqrt{5}, \alpha\right)$ over $\mathbb{Q}$.
   (d) Bestaat er een cyclotome uitbreiding $\mathbb{Q}(\zeta_n)$ met ζ_n de n-de primitieve eenheidswortel die $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}, \sqrt{5}, \alpha\right)$ bevat?
2. Zij $\zeta_{19} = e^{\frac{2\pi i}{19}} \in \mathbb{C}$.
   (a) Bepaal $[\mathbb{Q}(\zeta_{19}) : \mathbb{Q}]$.
   (b) Bepaal $\text{Gal}\,(\mathbb{Q}(\zeta_{19})/\mathbb{Q})$.
   (c) Bepaal alle reële deelvelden van $\mathbb{Q}(\zeta_{19})$. Dit betekent dus alle deelvelden in $\mathbb{Q}(\zeta_{19}) \cap \mathbb{R}$.
   (d) Met een passer en een geijkt liniaal kan men de wortels constureren van alle derde graadsvergelijkingen (met construeerbare coëfficiënten) met drie reële wortels.
   Een complex getal heet construeerbaar met passen en geijkt liniaal als het reël en imaginair deel beide construeerbaar zijn met passer en geijkt liniaal.
   Toon aan dat alle getall $\mathbb{Q}(\zeta_{19})$ construeerbaar zijn met passer en geijkt liniaal.

(e) Zij $f(\zeta_{19})$ een willekeurig element van $\mathbb{Z}[\zeta_{19}]$. Toon aan dat

$$N(f(\zeta_{19})) = \prod_{i=1}^{18} \zeta_{19}^{i} \in \mathbb{N}.$$

Men kan aantonen dat de ring $\mathbb{Z}[\zeta_{19}]$ een Euclidisch domein is met als norm N. Zij α een irreducibel element in $\mathbb{Z}[\zeta_{19}]$. Toon aan dat

$$\alpha\mathbb{Z}[\zeta_{19}] \cap \mathbb{Z} = p\mathbb{Z} \qquad \text{met } p \text{ een priemgetal in } \mathbb{Z}.$$

Toon aan dat de quotiënring $\dfrac{\mathbb{Z}[\zeta_{19}]}{\alpha\mathbb{Z}[\zeta_{19}]}$ een eindig veld is.
Welke eindige velden kunnen we op deze manier bekomen als quotiënt van $\mathbb{Z}[\zeta_{19}]$ naar $\alpha\mathbb{Z}[\zeta_{19}]$ als we aannemen dat $\alpha\mathbb{Z}[\zeta_{19}] \cap \mathbb{Z} \neq 19\mathbb{Z}$.

40 17 januari 2011

Theorie

De theorievragen zijn verloren gegaan.

Oefeningen

1. Zij G een eindige groep, P een Sylow p-deelgroep van G, en H een deelgroep van G zodat $N_G(P) \leq H \leq G$. Toon aan dat $N_G(H) = H$.

2. Zij G een eindige groep, $N \triangleleft G$, en A een klasse van toegevoegde elementen in G zodat $A \subseteq N$.

   (a) Toon aan dat A een unie is van een aantal klassen van toegevoegde elementen in N die allemaal dezelfde grootte hebben.

   (b) Noem dit aantal klassen k en toon aan dat dan $k = [G : C_G(x) N]$ voor elke $x \in A$.

3. Zij $R, +, \cdot$ een noetherse ring en zij $\varphi : R \to R$ een surjectief ringmorfisme. Toon aan dat φ een isomorfisme is.
   Hint: beschouw $\mathrm{Ker}(\varphi^n)$, *waarbij* $\varphi^n = \underbrace{\varphi \circ \cdots \circ \varphi}_{n \text{ keer}}$.

4. Een moduul wordt enkelvoudig genoemd als het niet het nul-moduul is en geen eigenlijke deelmodulen heeft. Zij R een ring, M een R-moduul en J een ideaal in R. Onderstel dat M en J enkelvoudige R-modulen zijn. Stel verder

$$JM = \left\{ \sum_{i=1}^{n} j_i m_i \,\middle|\, j_i \in J,\ m_i \in M \text{ en } n \in \mathbb{N} \right\}.$$

   (a) Bewijs dat ofwel $JM = M$, ofwel $JM = 0$.

   (b) Veronderstel nu dat $JM = M$. Bewijs dat J en M dan isomorfe R-modulen zijn.

41 17 januari 2012

Theorie

De theorievragen zijn verloren gegaan.

Oefeningen

1. Zij G een eindige groep die werkt op een verzameling A. Veronderstel dat voor elke twee paren (a_1, a_2) en (b_1, b_2) van elementen $a_1, a_2, b_1, b_2 \in A$ waarbij $a_1 \neq a_2$ en $b_1 \neq b_2$, er een element $g \in G$ bestaat zodat $a_1^g = b_1$ en $a_2^g = b_2$.
   Toon aan dat als $|A| = n$, dat dan $|G|$ deelbaar is door $n\,(n-1)$.

2. Zij G een enkelvoudige groep met $|G| = 60$.

   (a) Bewijs dat $n_2\,(G) = 5$, $n_3\,(G) = 10$ en $n_5\,(G) = 6$.

   (b) Toon aan dat G juist een deelgroep H van orde 12 heeft.

   (c) Toon aan dat H juist 5 conjugatieklassen heeft.

3. Zij R een Euclidisch domein met een Euclidische functie d zodanig dat voor alle $a, b \in R \setminus \{0\}$ geldt

   - $d\,(a) \leq d\,(ab)$,
   - $d\,(a+b) \leq \max\{d\,(a) + d\,(b)\}$.

   (a) Zij $a, b \in R \setminus \{0\}$. Toon aan dat $d\,(a) = d\,(ab)$ als en slechts als $b \in R^\times$.

   (b) Toon aan dat
   $$K = \left\{a \in R \setminus \{0\} \,\middle|\, d\,(a) \leq (1)\right\} \cup \{0\}$$
   een veld is.

   (c) Toon aan dat voor alle $a, b \in R$, met $a \neq 0$, er unieke elementen $q, r \in R$ bestaan zodat $b = aq + r$ en ofwel $r = 0$, ofwel $d\,(r) < d\,(a)$

   (d) Toon aan dat $R = K$ of $R \cong K\,[X]$.

4. Zij R een domein en $M \neq 0$ een R-moduul. Stel
   $$M_t = \left\{m \in M \,\middle|\, \text{er bestaat een } a \in R \text{ zodat } am = 0\right\}.$$
   De elementen van M_t worden *torsie-elementen* genoemd.

   (a) Bewijs dat M_t een deelmoduul is van M.

   (b) Zij M, N R-modulen, toon aan dat $(M \oplus N)_t = M_t \oplus N_t$.

   (c) Zij R een HID en M een eindig voortgebracht R-moduul. Toon aan dat M een vrij R-moduul is als en slechts als $M_t = 0$.

   (d) Zij R een HID en M een eindig voortgebracht projectief R-moduul. Toon aan dat M een vrij R-moduul is.

Deel IV

Examens Algebra I – Antwerpen

42 Ergens in januari 1995

Theorie

De theorievragen zijn verloren gegaan.

Oefeningen

1. Zij G een abelse groep en zij $a, b \in G$ met eindige orde. Veronderstel dat de orden van a en b onderling ondeelbaar zijn.
   (a) Toon aan dat $\langle a, b\rangle \cong \langle a\rangle \times \langle b\rangle$.
   (b) Toon aan dat $\langle a, b\rangle = \langle ab\rangle$.
2. Zij $\varphi : G_1 \to G_2$ een homomorfisme van groepen.
   (a) Toon aan dat voor alle $g \in G_1$ geldt dat de orde van $\varphi(g)$ de orde van g deelt.
   (b) Toon aan dat φ injectief is als en slechts als voor alle $g \in G_1$ de orde van $\varphi(g)$ gelijk is aan de orde van g.
3. Zij $\theta = \mathbb{Q}[X] \to \mathbb{C}$ een ringmorfisme. Toon aan dat
   (a) voor alle $a \in \mathbb{Q}$ geldt dat $\theta(a) = a$,
   (b) $\mathrm{Ker}(\theta)$ altijd een priemideaal is in $\mathbb{Q}[X]$.
4. Zij R een commutatieve ring met eenheidselement. Als I een ideaal in R is, definiëren we het radicaal als
$$\mathrm{Rad}\,(I) = \{a \in R\, | \text{er bestaat een } n \in \mathbb{N}_0 \text{ zodat } a^n \in I\}\,.$$
   (a) Toon aan dat $\mathrm{Rad}\,(I)$ een ideaal in R is en $I \subset \mathrm{Rad}\,(I)$.
   (b) Toon aan dat $\mathrm{Rad}\,(\mathrm{Rad}\,(I)) = \mathrm{Rad}\,(I)$.
5. Zij M een R-moduul en zij $I \subset R$ een ideaal. Stel
$$IM = \{\, a_1m_1 + a_2m_2 + \cdots + a_km_k |\, k \in \mathbb{N},\, a_i \in I \text{ en } m_i \in M\}\,.$$
   (a) Toon aan dat IM een deelmoduul is van M.
   (b) Definieer op M/IM een scalair product met elementen uit R/I door $\overline{a} \cdot \overline{m} = \overline{a \cdot m}$. Toon aan dat dit scalair product goed gedefinieerd is en dat de abelse groep $M/IM, /$ een R/I-moduul is voor dit scalair product.

43 Ergens in september 1995

Theorie

De theorievragen zijn verloren gegaan.

Oefeningen

1. Zij A een cyclische groep met orde n. Toon aan dat $3|n$ als en slechts als A juist twee elementen heeft met orde 3.

2. Zij X een verzameling en zij $S \subset X$ een deelverzameling. Stel

$$\begin{aligned} A &= \{\sigma \in \mathcal{S}(X) \,|\, \sigma(S) = S\} \qquad \text{en} \\ B &= \{\sigma \in \mathcal{S}(X) \,|\, \text{voor alle } s \in S \text{ geldt dat } \sigma(s) = s\} \end{aligned}$$

   Toon aan dat

   (a) A en B deelgroepen zijn van $\mathcal{S}(X)$,

   (b) B is een normaaldeler van A.

3. Zij K een lichaam. Stel $R = K \times K$ en definieer R een optelling "+" en een vermenigvuldiging "$*$" door

$$\begin{aligned} + &: K \times K \to K : (a,b) + (a',b') = (a+a', b+b') \\ * &: K \times K \to K : (a,b) \cdot (a',b') = (aa', ab' + a'b). \end{aligned}$$

   (a) Toon aan dat $R, +, *$ een ring is.
   Wat is het neutraal element voor $*$?

   (b) Definieer de afbeelding

$$\varphi : K[X] \to R : F(X) \mapsto \varphi\left(F(X)\right) = \left(F(0), DF(0)\right).$$

   Toon aan dat φ een surjectief ringhomomorfisme is met $\operatorname{Ker}(\varphi) = (X_2)$.

   (c) Toon aan dat $0 \cdot R$ en $((0,1))$ de enige idealen zijn in R.

   (d) Toon aan dat $R^* = K^* \times K$.

4. Stel

$$\begin{aligned} \theta &= \frac{1+\sqrt{3}}{2}, \\ A &= \{a + b\theta \,|\, a, b \in \mathbb{Z}\}, \\ N &: A \to \mathbb{Z} : a + b\theta \mapsto N\left(a + b\theta\right) = a^2 - b^2 + ab. \end{aligned}$$

   Toon aan dat

   (a) A een deelring is van $\mathbb{R}$,

   (b) dat voor alle $x, y \in A$ geldt dat $N(x \cdot y) = N(x) \cdot N(y)$,

   (c) $x \in A^*$ als en slechts als $N(x) = \pm 1$.

44 Ergens in januari 1996

Theorie

De theorievragen zijn verloren gegaan.

Oefeningen

1. Zij $H \subseteq G$ een echte deelgroep van een cyclische groep $G, *$. Bewijs dat $[G : H] < \infty$.
2. Zij G_1 en G_2 groepen, $N_1 \lhd G_1$ en $N_2 \lhd G_2$ normaaldelers. Toon aan dat
   (a) $N_1 \times N_2 \lhd G_1 \times G_2$,
   (b) $\dfrac{G_1 \times G_2}{N_1 \times N_2} \cong \dfrac{G_1}{N_1} \times \dfrac{G_2}{N_2}$.
3. Zij R een commutatieve ring zo dat voor elke $x \in R$ er een geheel getal $n \geq 2$ bestaat met de eigenschap dat $x^n = x$. Bewijs dat elk priemideaal van R een maximaal ideaal is.
4. Als R een commutatieve ring is en K en L idealen in R. Definieer

$$(K : L) := \{x \in R \,|\, xL \subseteq K\}.$$

   Bewijs volgende beweringen.
   (a) $(K : L)$ is een ideaal.
   (b) $K \subseteq (K : L)$.
   (c) $(K : L)\, L \subseteq K$.
   (d) Als $\{K_i \,|\, i \in I\}$ een familie van idealen in R is. Er geldt dat

$$\left(\bigcap_{i \in I} K_i : L \right) = \bigcup_{i \in I} (K_i : L).$$

5. Geef alle idealen en maximale idealen van de ring $R \times R$ als R een commutatieve ring is. Bewijs uw bewering.

45 Ergens in september 1996

Theorie

De theorievragen zijn verloren gegaan.

Oefeningen

1. Toon aan dat het aantal elementen van orde 2 in een eindige groep G ofwel nul ofwel oneven is.

2. Zij $G, *$ een groep en zij $\mathrm{Aut}(G)$ de groep van automorfismen, beschouwd met de samenstelling van functies. Noteer

$$I = \left\{ \varphi \in \mathrm{Aut}(G) \left| \text{er bestaat een element } g \in G \text{ zo dat voor alle } x \in G \ \varphi(x) = gxg^{-1} \right. \right\}.$$

   Als $H \subseteq G$ een deelgroep is, stel dan

$$H_0 = \bigcap_{\varphi \in \mathrm{Aut}(G)} \varphi(H).$$

   Toon volgende beweringen aan.

   (a) I is een normaaldeler van $\mathrm{Aut}(G)$.

   (b) Voor alle $\varphi \in \mathrm{Aut}(G)$ geldt dat $\varphi(H_0) = H_0$.

   (c) H_0 is een normaaldeler in G.

3. Zij R is een commutatieve ring zo dat

$$\bigcap_{P \text{ is een priemideaal in } R} P = \{0\}$$

   en zij $x \in R$ zo dat $x^n = 0$ voor een zekere $n > 0$. Toon aan dat dan $x = 0$.

4. Een R-moduul voortgebracht door één element noemen we *cyclisch*. Toon aan dat een R-moduul cyclisch is als en slechts als er een ideaal I van R bestaat zo dat $M \cong R/I$.

5. Zij R een commutatieve ring en $S \subseteq R$ een deelverzameling met de eigenschap dat voor alle $s, s' \in S$ geldt dat $ss' \in S$. Definieer voor elk R-moduul M de verzameling

$$T(M) = \{ m \in M \,|\text{er bestaat een } s \in S \text{ waarvoor geldt dat } sm = 0 \}.$$

   Bewijs dat

   (a) $T(M)$ is een deelmoduul van M,

   (b) $T(M/T(M)) = 0$.

46 Ergens in januari 2000

Theorie

De theorievragen zijn verloren gegaan.

Oefeningen

1. Zij $G, *$ een groep met $|G| = p^3$ met p een priemgetal. Toon aan dat als

$$|Z(G)| \geq p^2,$$

   G abels is.
   Hint: bekijk $G/Z(G)$.

2. Zij $\theta : G_1 \to G_2$ een groepshomomorfisme. Bewijs dat
   (a) voor elke $g \in G_1$ de orde van g deelbaar is door de orde van $\theta(g)$,
   (b) θ injectief is als en slechts als voor alle $g \in G_1$ de orde van g gelijk is aan de orde van $\theta(g)$.

3. Zij $a_i, m_i \in \mathbb{Z}$ voor $i = 1, 2$. Bewijs dat het stelsel

$$\begin{cases} x & = & a_1 \bmod m_1 \\ x & = & a_2 \bmod m_2 \end{cases}$$

   heeft een oplossing als en slechts als $\mathrm{ggd}(m_1, m_2) \mid (a_1 - a_2)$.

4. Is het ideaal $\left(2, 1 + \sqrt{-5}\right)$ een priemideaal of maximaal ideaal in $\mathbb{Z}\left[\sqrt{-5}\right]$? Toon aan je bewering aan!

47 Ergens in januari 2001

Theorie

De theorievragen zijn verloren gegaan.

Oefeningen

1. Zij $f : G \to G'$ een groepsmorfisme tussen eindige groepen en zij $H \subset G$ een deelgroep. Noteer met $f' = f|_H$ de beperking van f tot H.
   (a) Bewijs dat $\mathrm{Ker}(f')$ een deelgroep is van $\mathrm{Ker}(f)$ en $\mathrm{Im}(f')$ een deelgroep is van $\mathrm{Im}(f)$.
   (b) Toon aan dat
   $$[G : H] = [\mathrm{Ker}(f) : \mathrm{Ker}(f')] \cdot [\mathrm{Im}(f) : \mathrm{Im}(f')] .$$
2. Zij $G, *$ een eindige groep van orde p^m met $m > 0$ en p een priemgetal.
   Toon aan dat het centrum van G dan orde p^k heeft voor $0 < k < m$.
   Hint: schrijf G als unie van conjugatieklassen.
3. Zij R een ring en $a \in R$ is irreducibel.
   (a) Toon aan dat als (a) een priemideaal is in R, a dan irreducibel is.
   (b) Toon met een voorbeeld aan dar de omgekeerde implicatie niet hoeft te gelden.
   Hint: gebruik bijvoorbeeld als ring $R = \mathbb{Z}\left[\sqrt{-5}\right]$.
4. Zij M een R-moduul en L, M deelmodulen van M zo dat $L \subseteq N$. Toon aan dat
   $$\frac{M}{N} \cong \frac{M/L}{N/L}.$$

48 Ergens in september 2002

Theorie

De theorievragen zijn verloren gegaan.

Oefeningen

1. Zij $G, *$ een groep van orde pq waarbij p en q priemgetallen zijn.
   Bewijs dat elke deelgroep van G cyclisch is.

2. Zij H een deelgroep van een groep $G, *$ en $N \triangleleft G$.

   (a) Toon aan dat $NH := \{nh \,|\, n \in N \text{ en } h \in H\}$ een deelgroep is van G.

   (b) Bewijs dat als bovendien $H \triangleleft G$, dan is $NH \triangleleft G$.

   (c) Als H en N eindige deelgroepen zijn van G, zo dat $\operatorname{ggd}(|H|, |N|) = 1$. Bewijs dat NH dan exact $|N| \cdot |H|$ elementen heeft.

3. Zij $F \in \mathbb{Z}[X]$ een monische veelterm. Toon aan dat als $F \bmod p$ irreducibel is in $\mathbb{F}_p[X]$, dan F irreducibel is in $\mathbb{Q}[X]$.
   Geef een voorbeeld van een irreducibele vierdegraadsveelterm in $\mathbb{Q}[X]$.

4. Is het ideaal $(5, 2 + i)$ een maximaal ideaal in de ring $\mathbb{Z}[i]$? Is het een hoofdideaal? Bewijs je antwoorden.

49 Ergens in januari 2003

Theorie

De theorievragen zijn verloren gegaan.

Oefeningen

1. Zij $f : G \to G'$ een groepsmorfisme. Toon aan dat f injectief is als en slechts als voor alle $x \in G$ de orde van x gelijk is aan de orde van $f(g)$.

2. Zij $G, *$ een groep en $N \triangleleft G$ van eindige index. Zij H een eindige deelgroep van G zo dat de orde van H relatief priem is met index van N in G. Dit betekent dus dat $\text{ggd}(|H|, [G : H]) = 1$. Toon aan dat $H \subseteq N$.

3. Een element a in een ring R is irreducibel als a geen eenheid is en als uit $a = bc$ volgt dat b of c eenheden zijn in R.

   (a) Toon aan dat als (a) een priemideaal is in R, a dan irreducibel is.

   (b) Toon met een tegenvoorbeeld aan dat de omgekeerde implicatie in het algemeen niet geldt. Gebruik bijvoorbeeld $\mathbb{Z}\left[\sqrt{-5}\right]$.

4. Is het ideaal $(12, i - 5)$ een maximaal ideaal in $\mathbb{Z}[i]$? Is het een hoofdideaal? Toon uw antwoorden aan.