Algebra, code 151139

Datum	:	19-08-2008
Zaal	:	SC 0
Tijd	:	9.00-12.00

Motiveer al uw antwoorden
Besteed niet te veel tijd aan een afzonderlijk onderdeel. Indien u een onderdeel niet kunt oplossen dan kunt het resultaat van dat onderdeel in latere onderdelen toch gebruiken.

1. Zij G een eindige groep met eenheidselement e.
   (a) Bewijs: als $e \neq x \in G$ dan $x^2 \neq x$.
   (b) Bewijs dat het aantal elementen x in G waarvoor $x^3 = e$ oneven is.

2. Zij G de verzameling matrices gegeven door:
$$G = \{\begin{bmatrix} \alpha & \beta \\ -\beta & \alpha \end{bmatrix} \mid \alpha, \beta \in \mathbb{R} \;\; \alpha^2 + \beta^2 \neq 0\}.$$
   Op G beschouwen we de bewerking matrixvermenigvuldiging.
   (a) Laat zien dat G met matrixvermenigvuldiging een groep is.
   (b) Laat zien dat G isomorf is met $(\mathbb{C}\backslash\{0\}, \cdot)$, de complexe getallen ongelijk nul met vermenigvuldiging.

3. Ga na of $\mathbb{Z}_3 \oplus \mathbb{Z}_9$ en $\mathbb{Z}_{27}$ ismorf zijn als optelgroepen.

4. Zij $R = \{a + b\mathrm{i} \mid a, b \in \mathbb{Z}\}$, hierbij is i de imaginaire eenheid.
   (a) Laat zien dat R met de gewone optelling en vermenigvuldiging een ring is.
   (b) Bepaal alle eenheden van R, dat wil zeggen alle elementen van R die een inverse met betrekking tot de vermenigvuldiging hebben. Geef van elk van de door u gevonden eenheid ook de inverse.

5. Gegeven is het polynoom $p(x) = 1 + x + x^3 + x^4 + x^5 \in \mathbb{Z}_2[x]$.
   (a) Laat zien dat er geen polynomen $a(x), b(x) \in \mathbb{Z}_2[x]$ bestaan zodanig dat $a(x)b(x) = p(x)$ en $\mathrm{gr}\, a(x) = 2$ en $\mathrm{gr}\, b(x) = 3$. Hint: Laat zien dat er slechts acht paren $(a(x), b(x))$ bestaan die in aanmerking komen en probeer ze alle acht uit en concludeer dat geen enkele combinatie tot $p(x)$ leidt.

(b) Beredeneer dat $p(x)$ irreducibel is.

Definieer $\mathbb{F} = \mathbb{Z}_2[x]/(p(x))$.

(c) Is $\mathbb{F}$ een lichaam?

(d) Hoeveel elementen heeft $\mathbb{F}$?

(e) Wat is de dimensie van $\mathbb{F}$ als vectorruimte over $\mathbb{Z}_2$?

(f) Laat $\mathbb{K}$ een lichaam zijn van dimensie d als vectorruimte over $\mathbb{Z}_2$ en $\mathbb{Z}_2 \subset \mathbb{K} \subset \mathbb{F}$.

Hoeveel elementen heeft $\mathbb{K}$? Wat is de dimensie van $\mathbb{F}$ opgevat als vectorruimte over $\mathbb{K}$? Concludeer dat er geen lichamen strikt tussen $\mathbb{Z}_2$ en $\mathbb{F}$ zitten.

(g) Stel $\mathbb{L}$ is een deellichaam van $\mathbb{M}$, i.e., $\mathbb{L} \subset \mathbb{M}$. Zij verder gegeven dat de dimensie van $\mathbb{M}$ opgevat als vectorruimte over $\mathbb{L}$ gelijk is aan n. Onder welke voorwaarde op n bestaat er geen lichaam $\mathbb{K}$ zodanig dat

$$\mathbb{L} \underset{\neq}{\subseteq} \mathbb{K} \underset{\neq}{\subseteq} \mathbb{M}?$$

6. $C \subset \mathbb{Z}_2^7$ is een lineaire code met *parity-check* matrix H gegeven door:

$$H = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

(a) Laat zien dat elk tweetal rijen van H lineair onafhankelijk is.

(b) Bevat C codewoorden van gewicht 3?

(c) Geef de definitie van *Hamming weight* van een lineaire code.

(d) Wat is de *Hamming weight* van C?

(e) Bepaal een *coset leader*, i.e., een woord w van minimaal gewicht zodanig dat $wH = 110$.

(f) Het woord $c = (0001111)$ wordt verstuurd, en het woord $w_{\mathrm{r}}(1101111)$ wordt ontvangen.

i. Decodeer wr met behulp van syndroom decodering.

ii. Wat valt u op?

iii. Geef een verklaring.

Puntenverdeling:

1		2		3	4		5							6					
a	b	a	b		a	b	a	b	c	d	e	f	g	a	b	c	d	e	f
8	8	9	9	7	7	7	3	2	3	2	3	3	4	4	4	2	5	3	6

Cijfer: $1 + \dfrac{\text{punten}}{11}$