

400002 Tentamen Algebra en Discrete Wiskunde 21-12-2005

1 Groepen, cyclische groepen en restklassen.

- a) Geef de definitie van de *orde* van een groep, en geef ook aan wat het betekent dat een groep *cyclisch* is. Wat is een *generator* (of *voortbrenger*) van een cyclische groep?
- b) Geef aan waarom een groep G waarvan de orde o een priemgetal is, *cyclisch* moet zijn.
- c) Wat is een *eenheid* in een restklassenring? Geef de *eenheden* van $\mathbb{Z}_8$ en van $\mathbb{Z}_9$.
- d) Vormen de *eenheden* van $\mathbb{Z}_8$ een cyclische groep? Zo ja, geef een *voortbrenger* aan. Hoe ligt dat bij $\mathbb{Z}_9$, en zo ja, geef een *voortbrenger*?

2 Ringen, Lichamen, Veeltermen(polynomen).

- a) Wat bedoelt men met een *nuldeler* in een ring R ? Geef een voorbeeld van een nuldeler in $\mathbb{Z}/24$
- b) Geef de juiste, meest aangepaste, benaming of bijbehorende afkorting: Een veeltermring (of polynoomring) over een lichaam is een
(Unitaire Ring--UR, Commutatieve Unitaire Ring--CUR, Integriteitsgebied--ITG, Lichaam--L).
- c) Laat zien dat de veelterm $F = X^3 + X + 1$ reducibel is over het lichaam $\mathbb{Z}/3$ maar irreducibel over het lichaam $\mathbb{Z}/7$.
- d) Hoeveel elementen heeft de ring $K[X]/F$ voor het geval dat met K het lichaam $\mathbb{Z}/3$ wordt bedoeld, en voor het geval dat met K het lichaam $\mathbb{Z}/7$ wordt bedoeld. Bedoeld wordt de F uit onderdeel b).
- e) Is de ring $K[X]/F$ zelf een lichaam, in het geval dat met K het lichaam $\mathbb{Z}/3$ wordt bedoeld, en in het geval dat met K het lichaam $\mathbb{Z}/7$ wordt bedoeld. Bedoeld wordt de F uit onderdeel b).

3 Veeltermen over $\mathbb{Z}_{10}$.

- a) Bepaal de *nuldelers*, en de *eenheden* van $\mathbb{Z}_{10}$.
- b) Een *idempotent* in een semigroep is een element a zodat $a \cdot a = a$. Bepaal alle *idempotenten* in de multiplicatieve semigroep van $\mathbb{Z}_{10}$.
- c) Bepaal het aantal elementen van de *veeltermring* $\mathbb{Z}_{10}[X]$ modulo $X^2 - 1$.
- d) Zoek een paar nuldelers in de *veeltermring* $\mathbb{Z}_{10}[X]$ modulo $X^2 - 1$ die beiden de graad 1 hebben.

4 Vectorruimten.

a) Algemene kennis :

- (i) Wat bedoelt men met een *lineaire deelruimte* W van een lineaire ruimte V over een lichaam $\mathbb{F}$?
- (ii) In de *dimensie stelling* voor een lineaire afbeelding $f: V \rightarrow W$ tussen twee lineaire ruimten V en W over een lichaam $\mathbb{F}$ is sprake van de *kern* van f en het *beeld* van f . Formuleer deze stelling.
- (iii) Als V een lineaire ruimte van dimensie 5 over $GF(5)$ is, hoeveel elementen heeft V in dat geval? En hoeveel elementen heeft een *basis* voor V dan?

b) Op de gebruikelijke wijze wordt een afbeelding $f: V \rightarrow W$ tussen de lineaire ruimten V en W over $GF(5)$ gegeven door de hiernaast gegeven matrix. Hoe groot is nu de dimensie van V ? Hoe groot is de dimensie van W ? Hoeveel elementen heeft V ? En hoeveel W ?

1	2	3	0	0
0	2	1	1	0
0	1	3	2	4
1	0	2	3	4

- c) Bepaal de dimensie van de *kern* en van het *beeld* van de afbeelding f . Is de gegeven afbeelding *injectief*? Is de gegeven afbeelding *surjectief*? Licht je antwoorden toe.
N.B. $GF(5) = \mathbb{Z}/5 = \{0, 1, 2, 3, 4\}$.

5 De Euler totient functie en primitieve elementen.

- a) Wat bedoelt men met de *Euler totient functie* $\phi(m)$?
- b) Welke formule is er voor $\phi(m_1 \cdot m_2)$ en voor welke voorwaarde(n) op m_1 en m_2 is die geldig?
- c) Een stelling zegt, dat $n = \sum_{d|n} \phi(d)$, waarin $d|n$ staat voor alle d die deler zijn van n , inclusief 1 en n zelf. Laat met behulp van een rij van breuken zien, hoe de restklassen modulo n kunnen worden ingedeeld zodat de stelling duidelijk wordt.
- d) Gegeven een eindig lichaam L met m elementen. Aan welke vergelijking voldoen alle elementen behalve de 0 van L ? Geef de definitie van een *primitief element* van L . Wat voor eigenschap heeft zo'n element met betrekking tot de gevonden vergelijking?

NORMERING

1a 2 pt	2b 1 pt	3b 2 pt	4c 3 pt	
1b 2 pt	2c 2 pt	3c 2 pt	5a 1 pt	Multiple Choice
1c 1 pt	2d 2 pt	3d 2 pt	5b 1 pt	7 pt
1d 2 pt	2e 2 pt	4a 3 pt	5c 3 pt	
2a 1 pt	3a 2 pt	4b 2 pt	5d 2 pt	$CIJFER = \frac{SOM}{5} + 1.$

6. Multiple-choice gedeelte

- Bij iedere vraag is precies één van de onderdelen juist en (meest) volledig.
- Het antwoord van een aangekruist bolletje hoeft niet te worden toegelicht.

6.1. Gegeven twee onderling ondeelbare natuurlijke getallen $m > n$. De Chinese Reststelling zegt dan dat :

- o er twee unieke natuurlijke getallen q en r bestaan met $m = q \cdot n + r$.
- o voor de totient functie geldt $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$.
- o als $q < m$ en $r < n$ natuurlijke getallen, dan is er een unieke oplossing voor het stelsel vergelijkingen $x \equiv q \pmod{m}$ en $x \equiv r \pmod{n}$ beneden $m \cdot n$.
- o het getal $m \cdot n$ kan worden gebruikt als de modulus voor een RSA code.

6.2. Een monoïde is:

- o een semigroep met een neutraal element.
- o een vectorruimte met dimensie 1.
- o een alternatieve benaming voor een unitaire ring.
- o een veeltermring met uitsluitend veeltermen van graad 1.

6.3. De formule van Bezout in $\mathbb{Z}$ stelt dat:

- o bij iedere $a, b \neq 0$ een uniek stel getallen q, r bestaat met $b = a \cdot q + r$ en $0 \leq r < a$.
- o bij iedere $a, b \neq 0$ een stel getallen x, y bestaat met $x \cdot a + y \cdot b = \text{ggd}(a, b)$.
- o bij iedere $a, b \neq 0$ een stel getallen x, y bestaat met $x \cdot a + y \cdot b = 1$.
- o bij iedere $a, b \neq 0$ geldt: als $\text{ggd}(a, b) = 1$ en a deelt $b \cdot c$ dan a deelt c .

6.4. Een ideaal van een commutatieve unitaire ring R is een deelverzameling van R die:

- o stabiel is onder optelling $x + y$ en vermenigvuldiging $x \cdot y$ van R .
- o stabiel is onder aftrekking $x - y$ en vermenigvuldiging $x \cdot y$ van R die het eenheidselement van R bevat.
- o stabiel is onder optelling $x + y$ en "superstabiel" is onder de vermenigvuldiging $x \cdot y$ van R .
- o stabiel is onder aftrekking $x - y$ en "superstabiel" onder de vermenigvuldiging $x \cdot y$ van R die het eenheidselement van R bevat.

N.B. Een verzameling $A \subset R$ is "stabiel" onder een bewerking $x \# y$ in R wanneer geldt:

als $x \in A$ en $y \in A$ dan $x \# y \in A$.

Een verzameling $A \subset R$ is "superstabiel" onder een bewerking $x \# y$ in R wanneer geldt:

als $x \in R$ en $y \in A$ dan $x \# y \in A$.

6.5. Een vectorruimte van dimensie 3 over het lichaam $\mathbb{Z}(2)$ heeft :

- o $2 + 3 = 5$ elementen.
- o $2 \cdot 3 = 6$ elementen.
- o $2^3 = 8$ elementen.
- o $3^2 = 9$ elementen.

6.6. Als R een UR (unitaire ring) is, dan staat R^* voor :

- o de veeltermring voor alle veeltermen (polynomen) over R .
- o de groep van eenheden van R .
- o de verzameling van nuldelers van R .
- o de structuur die uit R ontstaat na weglating van de optelling.

6.7. Er bestaat géén lichaam met :

- o 16 elementen
- o 17 elementen
- o 18 elementen
- o 19 elementen