

Tentamen Algebra en Discrete Wiskunde I 8-2-2005

1 Groepen.

- a) Algemene kennis :
- (i) In een groep van orde 29 is x niet het eenheidselement. Wat weet je van de orde van x ?
 - (ii) Wat wordt aangegeven met de *Euler Totient functie* $\phi(m)$ voor gehele getallen $m \geq 2$?
 - (iii) Formuleer de *Chinese Reststelling* in een situatie waarbij we precies twee moduli m_1 en m_2 hebben.
- b) Zoek een geheel getal x dat tegelijk voldoet aan $x \equiv 11 \pmod{14}$ en $x \equiv 8 \pmod{15}$. (Goede toelichting scoort).
- c) Bereken $10^{74} \pmod{51}$ op een economisch zuinige manier. Geef daarbij nauwkeurig aan welke stappen je daarbij neemt.

2 Groepen, deelgroepen en nevenklassen.

- a) Gegeven een groep G en een deelverzameling D van G . Waaraan moet D voldoen om een deelgroep van G te zijn? Gegeven dat N een nevenklasse is van D binnen G . Wat betekent dat voor N ?
- b) Laat zien dat een (echte) nevenklasse N en de ondergroep D disjunct zijn. Laat ook zien dat twee verschillende nevenklassen N_1 en N_2 disjunct zijn.
- c) Laat zien dat elke nevenklasse N precies evenveel elementen heeft als D .

3 Ringen en idempotenten.

Een *idempotent element* van een ring is een element $x \neq 0$ met $x \cdot x = x$.

- a) Toon aan dat in een ITG precies één idempotent element is. Welk?
- b) Geef een voorbeeld van een CUR (niet ITG) waar nog andere idempotente elementen voorkomen. Welke?
- c) Zij p een priemgetal en $k > 1$. Toon aan dat $\bar{1}$ het enige idempotente element is van $\mathbb{Z}/(p^2)$, en dat deze restklassenring toch géén ITG is.

Unitaire Ring--UR, Commutatieve Unitaire Ring--CUR, Integriteitsgebied--ITG, Lichaam--L.

Z.O.Z

4 *Veeltermringen.*

- a) Algemene kennis :
- (i) Wat verstaat men onder de *graad* van een veelterm over een commutatieve unitaire ring?
 - (ii) Is de graad van de som van twee veeltermen over een CUR steeds gelijk aan het maximum van de twee graden?
 - (iii) Is de graad van een product van twee veeltermen over een CUR steeds gelijk aan de som van de twee graden?
- b) Gegeven het lichaam $\mathbb{Z}/(2)$ met daarover de polynomen (veeltermen) $F(X) := X^6 + X^5 + X^4 + X^2 + X + 1$ en $G(X) := X^6 + X^5 + X^2 + X + 1$. Bepaal de grootste gemene deler $D(X)$ van deze twee veeltermen.
- c) Er is een formule van Bezout voor $D(X)$ vanuit $F(X)$ en $G(X)$. Bepaal deze formule via de gebruikelijke algoritme.

5 *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. $GF(5) = \mathbb{Z}/5 = \{1, 2, 3, 4, 5\}$.

NORMERING

1a 3 pt	2a 2 pt	3a 2 pt	4a 3 pt	5a 3 pt
1b 2 pt	2b 3 pt	3b 2 pt	4b 3 pt	5b 2 pt
1c 2 pt	2c 3 pt	3c 3 pt	4c 3 pt	5c 2 pt

$$CIJFER = \frac{SOM}{5} + 1.$$

Multiple choice: 1 punt per vraag.

6. Multiple-choice gedeelte Algebra en Discrete Wiskunde I

- 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. Over priemrestklassen.

- o Er zijn geen priemrestklassen modulo **26** want **26** is niet priem.
- o $\overline{13}$ is een priemrestklasse modulo **26**.
- o De som van twee priemrestklassen is weer een priemrestklasse modulo **26**.
- o Het product van twee priemrestklassen is weer een priemrestklasse modulo **26**.

6.2. Een deelgroep H van een groep $(G, *)$ is

- o een deelverzameling H van G die stabiel is onder de operatie $x*y^{-1}$ van G waarin y^{-1} de inverse is van y onder $*$.
- o een deelverzameling H van G die stabiel is onder de operatie $*$ van G .
- o een deelverzameling H van G die stabiel is onder de "inverse" van G .
- o een deelverzameling H van G met een operatie $\#$ zo dat $(H, \#)$ een groep is.

6.3. Een cyclische groep is

- o een groep die een generator (voortbrenger) heeft.
- o een groep die géén generator (voortbrenger) heeft.
- o een groep bestaande uit cyclische permutaties.
- o een deelgroep van de cirkelgroep, (dit is de complexe getallen met modulus 1).

6.4. Een nuldeeler in een ring is

- o een element a met $a \cdot b = 0$ voor zekere b .
- o een synoniem voor 0 .
- o een element $a \neq 0$ met $a \cdot b = 0$ voor zekere $b \neq 0$.
- o een element a dat 0 deelt.

6.5. De volgende verzameling is een ideaal in de ring $(\mathbb{Z}, +, \cdot)$

- o de verzameling van alle oneven getallen.
- o de verzameling $\{0, 1, -1\}$.
- o de verzameling van alle niet-priemgetallen.
- o de verzameling van alle drievouden.

6.6. Een basis in een vectorruimte (lineaire ruimte) V is:

- o een lineair onafhankelijke deelverzameling die heel V voortbrengt.
- o een zo groot mogelijke lineaire deelruimte.
- o een zo klein mogelijke lineaire deelruimte.
- o een verzameling van eenheidsvectoren.

6.7. Een primitief element van een lichaam K is:

- o een element van K^* zonder multiplicatieve inverse.
- o een generator van de multiplicatieve groep K^* .
- o een irreducibele veelterm in $K[X]$.
- o een generator van de additieve groep van K .