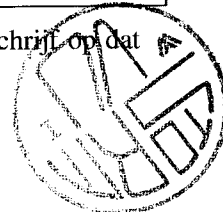


**Opgelet:** er is een apart multiple-choice gedeelte op de laatste bladzijde (vraag 4). Schrijf op dat blad je naam en lever het mee in met je overige tentamenkopij!



## 1. Groepswerkingen en symmetriegroepen.

(a) Algemene kennis. Bij een groepswerking van een groep  $G$  op een verzameling  $V$  gaat het om een functie  $G \times V \rightarrow V$ , waarbij  $(g, v) \mapsto gv$  voor  $g \in G$  en  $v \in V$ .

(i) Formuleer in deze notatie de twee axioma's voor een groepswerking.

**TG1.**  $(st)v = s(tv)$  voor alle  $s, t \in G$  en  $v \in V$ .

**TG2.**  $ev = v$  voor alle  $v \in V$ .

(ii) Wat verstaat men onder de stabilisator van een element  $v \in V$ ?

De stabilisator van  $v \in V$  is de deelverzameling van  $G$  gedefiniëerd door

$$S(v) := \{g : g \in G, gv = v\}.$$

Dit is de verzameling van alle groeps-elementen die  $v$  vasthouden.

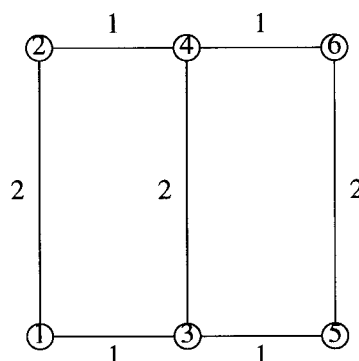
(iii) Wat verstaat men onder de baan van een element  $v \in V$ ?

De baan (orbit) van  $v \in V$  is de deelverzameling van  $V$  gedefiniëerd door

$$O(v) := \{gv : g \in G\}.$$

Dit is de verzameling van alle elementen van  $V$  waarop  $v$  kan worden afgebeeld door de actie van een groeps-element.

(b) Volgende figuur met 6 punten (genummerd 1 t/m 6) is gesitueerd in het platte vlak. De relevante afstanden zijn aangeduid, alle getekende hoeken zijn recht.



(i) Beschrijf de baan  $O(3)$  van het punt 3 onder de werking van de symmetriegroep.

Geen enkele symmetrie brengt het punt 3 naar 1, 2, 5, of 6, want deze punten hebben elk slechts één "buur" op afstand 1 en punt 3 heeft twee van dergelijke "buren". Een spiegeling in de horizontale as door het midden van de figuur (dit is de permutatie  $(1\ 2)(3\ 4)(5\ 6)$ ) verplaatst punt 3 naar punt 4. Dus is de baan  $O(3) = \{3, 4\}$ .

(ii) Beschrijf de baan  $O(2)$  van het punt 2 onder de werking van de symmetriegroep.

Je kan de figuur spiegelen in de horizontale as door het midden van de figuur en in de verticale as door het midden van de figuur. Deze symmetrieën en hun combinaties leveren vier mogelijke posities op voor het punt 2, namelijk 1, 2, 5, en 6. Geen enkele symmetrie brengt 2 naar 3 of 4, want deze punten hebben twee "buren" op afstand 1 en punt 2 heeft maar één dergelijke "buur". Dus is de baan  $O(2)=\{1,2,5,6\}$ .

Goede toelichting scoort.

(c) (Zelfde figuur)

(i) Beschrijf de stabilisator  $S(2)$  van het punt 2 onder de werking van de symmetriegroep.

Als punt 2 vastblijft, moet ook punt 1 vastblijven (enige "buur" op afstand 2). Als de punten 1 en 2 vastblijven, dan ook de punten 3 en 4, want dit zijn de unieke respectievelijke buren op afstand 1. Onder deze omstandigheden moeten ook punten 5 en 6 vast blijven. Dus  $S(2)=\{id\}$ .

(ii) Beschrijf de stabilisator  $S(3)$  van het punt 3 onder de werking van de symmetriegroep.

Als punt 3 vast blijft, moet zijn enige buur op afstand 2 ook vast blijven. Verder kunnen de twee buren (1 en 5) van 3 op afstand 1 alleen onder elkaar verwisseld worden of vast blijven. In het laatste geval moeten alle punten vast blijven; in het eerste geval heb je de isometrie  $(15)(26)$ . Dus  $S(3)=\{id, (15)(26)\}$ .

Goede toelichting scoort.

(d) Hoeveel elementen heeft de symmetriegroep van de figuur in deze opgave? Wat is de link met de resultaten uit delen (b) en (c)?

De totale symmetriegroep heeft 4 elementen. Je kan dit aantal krijgen via de baanformule: voor ieder punt  $v$  is  $\#groep = \#S(v) \cdot \#O(v)$ . Bijvoorbeeld,  $v=2$  geeft  $\#S(v)=1$  en  $\#O(v)=4$ . Bijvoorbeeld,  $v=3$  geeft  $\#S(v)=2$  en  $\#O(v)=2$ .

**2. Groepshomomorfismen en deelgroepen.** In deze opgave bekijken we de kandidaat functie

$$f: \mathbb{Z}_{28} \rightarrow \mathbb{Z}_7, \quad \text{klas}_{28}(z) \mapsto \text{klas}_7(z).$$

(a) Controleer dat  $f$  een goed gedefiniëerde functie is, en controleer vervolgens dat  $f$  een (additief) homomorfisme is.

Goed gedefiniëerd: Het voorschrift hangt niet af van de keuze van een representant  $z$ . Stel  $z_1$  en  $z_2$  representeren dezelfde "modulo 28" klasse. Dan is  $z_1 \equiv z_2 \pmod{28}$ . M.a.w.,  $28 \mid z_2 - z_1$  en bijgevolg  $7 \mid z_2 - z_1$ . Conclusie:  $z_1 \equiv z_2 \pmod{7}$ .

Additief homomorfisme:

| context $\mathbb{Z}_{28}$     |           | context $\mathbb{Z}_7$  |
|-------------------------------|-----------|-------------------------|
| $klas_{28}(x)$                | $\mapsto$ | $klas_7(x)$             |
| $klas_{28}(y)$                | $\mapsto$ | $klas_7(y)$             |
| +                             |           | +                       |
| $klas_{28}(x) + klas_{28}(y)$ |           | $klas_7(x) + klas_7(y)$ |
| $= klas_{28}(x+y)$            | $\mapsto$ | $= klas_7(x+y)$         |

In de rechterkolom (context  $\mathbb{Z}_7$ ) is de berekende som gelijk aan de functiewaarde op grond van de definitie van "som modulo 7".

- (b) Bepaal de kern  $H$  van  $f$ .

De kern bestaat uit precies die elementen  $klas_{28}(z)$  waarvoor  $klas_7(z) = klas_7(0)$ . Om in aanmerking te komen, moet de gekozen representant  $z$  van  $klas_{28}(z)$  dus voldoen aan  $z \equiv 0 \pmod{7}$ : een 7-voud. Bijgevolg ("modulo 28" notatie):  $ker(f) = \{\bar{0}, \bar{7}, \bar{14}, \bar{21}\}$  (4 elementen).

- (c) Hoeveel nevenklassen heeft de deelgroep  $H$ ?

Stelling 8.§11 van Lagrange:  $\#\mathbb{Z}_{28}/\#H = 28/4 = 7$ . Dit wordt ook de index genoemd van  $H$  in  $\mathbb{Z}_{28}$ , genoteerd  $[\mathbb{Z}_{28}:H]$ .

- (d) Geef, met de nodige argumentatie, een volledig representantensysteem voor de equivalentierelatie ' $\equiv$ ' in  $\mathbb{Z}_{28}$  met voorschrift

$$x \equiv y \text{ betekent } y - x \in H.$$

Uit de theorie halen we de volgende wetenswaardigheden:

1) De equivalentieklassen van de equivalentierelatie ' $\equiv$ ' corresponderen aan de linker nevenklassen van  $H$  in  $\mathbb{Z}_{28}$  (stelling 8.§7).

2) Volgens onderdeel (a) is de verzameling  $H$  precies de kern van het homomorfisme  $f: \mathbb{Z}_{28} \rightarrow \mathbb{Z}_7$  met voorschrift  $klas_{28}(z) \mapsto klas_7(z)$ . Je krijgt dan de partitie in nevenklassen direct uit het homomorfisme  $f$  op de volgende manier:

$$\{ f^{-1}(x) : x \in \mathbb{Z}_7 \}.$$

(opgave 8.6). Voor een volledig representantensysteem kies je (bijvoorbeeld) uit elke verzameling  $f^{-1}(x)$  (met  $x \in \mathbb{Z}_7$ ) die klasse modulo 28 met de kleinste standaard representant. Dat geeft:

Voor  $x = klas_7(0)$ :  $klas_{28}(0)$ .

Voor  $x = klas_7(1)$ :  $klas_{28}(1)$ .

Voor  $x = klas_7(2)$ :  $klas_{28}(2)$ .

Voor  $x = klas_7(3)$ :  $klas_{28}(3)$ .

Voor  $x = klas_7(4)$ :  $klas_{28}(4)$ .

Voor  $x = klas_7(5)$ :  $klas_{28}(5)$ .

Voor  $x = klas_7(6)$ :  $klas_{28}(6)$ .

Conclusie: de verzameling

$$\{ klas_{28}(x) : 0 \leq x < 7 \}$$

is een volledig representantensysteem voor de relatie ' $\equiv$ '.

### 3. Veeltermringen en modulorekenen met veeltermen.

(a) Algemene kennis.

(i) Formuleer het delingsalgoritme in een veeltermring  $K[X]$  (waar  $K$  een lichaam is).

Gegeven  $A, B \in K[X]$  met  $B \neq 0$ , bestaat een uniek stel veeltermen  $Q, R \in K[X]$  met

$$A = B \cdot Q + R \quad \text{en hetzij} \quad R = 0, \quad \text{hetzij} \quad 0 \leq \deg(R) < \deg(B).$$

De term " $\deg(F)$ " staat hier voor de graad van de veelterm  $F$ .

(ii) Een veelterm  $F \in K[X]$  is niet hetzelfde als de veeltermfunctie

$$K \rightarrow K, \quad x \mapsto F(x).$$

Leg dit bondig uit.

Een veelterm  $F$  die niet de "nulveelterm" is, kan wel aanleiding geven tot een veeltermfunctie die identiek nul is. Bijvoorbeeld, in  $\mathbb{Z}_p$  (met  $p$  priem) is  $x^p = x$  voor alle  $x \in \mathbb{Z}_p$ . Voor  $x=0$  is dit evident ( $0=0$ ) en voor  $x \neq 0$  is dit in essentie de Stelling van Euler, 5.§11. Dus de veelterm  $X^p - X$  is niet de nulveelterm (hij is van graad  $p$ ) maar de bijhorende veeltermfunctie is wel de nulfunctie.

(iii) In  $\mathbb{Z}[X]$  hebben we de volgende twee veeltermen:

$$F := X^4 + 2X^3 + 3X^2 + 4X + 5, \quad G := 5X^4 + 4X^3 + 3X^2 + 2X + 1.$$

Bereken de coëfficiënt van  $X^4$  in het veeltermproduct  $F \cdot G$ .

Noem de  $F$ -coëfficiënt van  $X^i$  even  $a_i$ , en noem de  $G$ -coëfficiënt van  $X^j$  even  $b_j$ . De formule voor de coëfficiënt van  $X^4$  is dan:  $\sum_{i+j=4} a_i \cdot b_j$ . We berekenen dit via een tabelletje:

| $i$                 | 4 | 3 | 2 | 1  | 0  |
|---------------------|---|---|---|----|----|
| $a_i$               | 1 | 2 | 3 | 4  | 5  |
| $j=4-i$             | 0 | 1 | 2 | 3  | 4  |
| $b_j$               | 1 | 2 | 3 | 4  | 5  |
| $a_i \cdot b_{4-i}$ | 1 | 4 | 9 | 16 | 25 |

Het gezochte resultaat is de som van de getallen, berekend in de laatste rij van de tabel:  
 $1+4+9+16+25=55$ .

(b) We werken in dit onderdeel met het lichaam  $\mathbb{Z}_{11}$ . Bereken met de "klassieke" staartdelingsalgoritme quotiënt en rest van  $A$  bij deling door  $B$  als

$$A := X^3 + \bar{4}X^2 - \bar{4}X + \bar{5}, \quad B := X^2 + \bar{2}X + \bar{3}.$$

Welke graad hebben dit quotiënt en deze rest?

We voeren de staartdeling uit.

$$\begin{array}{r}
 \begin{array}{cccc}
 X^2 & +\bar{2}X & +\bar{3} & / \\
 - & & & \\
 \hline
 & & & 
 \end{array}
 \begin{array}{cccc}
 X^3 & +\bar{4}X^2 & -\bar{4}X & +\bar{5} \\
 X^3 & +\bar{2}X^2 & +\bar{3}X & \\
 \hline
 & \bar{2}X^2 & -\bar{7}X & +\bar{5} \\
 & \bar{2}X^2 & +\bar{4}X & +\bar{6} \\
 \hline
 & & \bar{0}X & -\bar{1}
 \end{array}
 \end{array}
 \quad \backslash \quad X \quad + \quad \bar{2}$$

Dus:  $Q = X + \bar{2}$  van graad 1 en  $R = -\bar{1}$  van graad 0.

(c) Neem  $M := X^3 - X - \bar{1} \in \mathbb{Z}_3[X]$  als modulus en reduceer de veelterm  $F := X^5 + X^2 + \bar{1}$  mo-

dulo  $M$ .

Uit de gelijkheid  $M \equiv \bar{0}$  halen we  $X^3 \equiv X + \bar{1}$ . Dit geeft  $X^5 \equiv X^3 + X^2 \equiv X^2 + X + \bar{1}$ . Invullen in  $F$  geeft:

$$F \equiv (X^2 + X + \bar{1}) + X^2 + \bar{1} = -X^2 + X - \bar{1}.$$

Je kan deze uitkomst ook krijgen als de rest bij (staart)deling van  $F$  door  $M$ , maar dat kost meer rekenwerk.

**Normering:**

|       |   |       |   |       |   |       |    |
|-------|---|-------|---|-------|---|-------|----|
| 1a    | 6 | 2a    | 5 | 3a    | 9 | 4     | 24 |
| 1b    | 6 | 2b    | 5 | 3b    | 7 |       |    |
| 1c    | 6 | 2c    | 4 | 3c    | 7 |       |    |
| 1d    | 4 | 2d    | 7 |       |   |       |    |
| <hr/> |   | <hr/> |   | <hr/> |   | <hr/> |    |
| 22    |   | 21    |   | 23    |   | 24    |    |

**Totaal = 90**

**Cijfer = Totaal/10 + 1**

**Multiple choice gedeelte:** -5 ptn per foute keuze.

#### 4. Multiple-choice gedeelte

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

**4.1.** De stelling van Lagrange gaat over een eindige groep  $G$  en een deelgroep  $H$  van  $G$ . De conclusie van de stelling is, dat de orde van  $H$  een deler is van de orde van  $G$ . Wat zijn de verdere voorwaarden?

- ☐ Er zijn geen verdere voorwaarden. ☒ JA
- ☐ De groep  $G$  moet abels zijn.
- ☐ De groep  $H$  moet een normale deelgroep zijn van  $G$ .
- ☐ De groep  $H$  moet voortgebracht zijn door een element (i.e., een cyclische groep).

Lees de Lagrange stelling 8.11 erop na: de voorwaarden genoemd in opties 2, 3, en 4, zijn niet nodig.

**4.2.** Van volgende uitspraken over elementen in een permutatiegroep is er één die altijd waar is. Welke?

- ☐ Elke permutatie is (op de volgorde van de factoren na) op unieke wijze te schrijven als een product van verwisselingen.
- ☐ Elke permutatie is op diverse manieren te schrijven als een product van verwisselingen. Daarbij is het aantal benodigde verwisselingen modulo twee hetzelfde. ☒ JA
- ☐ Elke permutatie is (op de volgorde van de factoren na) op unieke wijze te schrijven als een product van cykels.
- ☐ Elke permutatie is op diverse manieren te schrijven als een product van disjuncte cykels (verschil in de volgorde van de factoren niet meegerekend).

(Een leesopdracht!) Bij optie 1 is "uniek" niet terecht: je kan erg creatief omgaan met zulke producten; bijvoorbeeld kun je  $(12)(12)$  aan een product toevoegen zonder dat de uitkomst wijzigt. Optie 3 is om dezelfde reden niet goed. Bij optie 4 ontbreekt juist de toevoeging "uniek". Optie 2 ligt aan de basis van de "tekenfunctie" voor permutaties, en is correct.

**4.3.** Zij  $(G, *)$  een (multiplicatief geschreven) groep. Onder een normale deelgroep  $H \subseteq G$  verstaat men:

- ☐ Een deelgroep  $H$  van  $G$  die commutatief is.
- ☐ Een deelgroep  $H$  van  $G$  waarvan de rechternevenklassen even groot zijn als de linkernevenklassen.
- ☐ Een deelgroep  $H$  van  $G$  zo dat  $gHg^{-1} \subseteq H$  voor alle  $g \in G$ . ☒ JA
- ☐ Een deelgroep  $H$  van  $G$  zo dat  $hGh^{-1} \subseteq H$  voor alle  $h \in H$ .

Optie 1 geeft geen garantie op normaliteit: in opgave 8.13(c) werd een niet-normale deelgroep van  $S_3$  gevonden. Die groep is  $\{(1), (12)\}$ , en die is abels. Optie 2 is voor alle deelgroepen waar, en heeft dus evenmin met normaliteit te maken. Optie 4 is een foute variant op de juiste optie: 3.

**4.4.** De kern van een ringhomomorfisme  $R \rightarrow S$  is:

- o een additieve deelgroep van  $R$ .
- o een multiplicatieve deelsemigroep van  $R$ .
- o een deelring van  $R$ .
- o een ideaal van  $R$ . ☒ JA

Opties 1 en 2 zijn waar, maar nogal beperkt. Optie 3 is fout: een deelring bevat het eenheidselement van de gegeven ring. Dat zou hier betekenen dat het eenheidselement op nul wordt afgebeeld. Maar dan wordt de hele ring naar nul afgebeeld! Optie 4 is perfect.

**4.5.** Een lichaam is een commutatieve unitaire ring ...

- o .. die onder optelling een groep is.
- o .. die onder vermenigvuldiging een groep is.
- o .. waarin elk element  $\neq 0$  een inverse heeft. ☒ JA
- o .. zonder nuldelers.

Optie 1 is waar voor alle ringen. Optie 2 is zwaar fout, want 0 heeft geen inverse (tenzij in de "nulring"). Optie 4 is waar maar te beperkt: dit geeft ITGs. Optie 3 geeft precies de vereiste voorwaarde aan.

**4.6.** Een primitief element van een lichaam  $K$  is

- o een generator (voortbrenger) van  $(K, +)$ .
- o een generator (voortbrenger) van  $(K^*, \cdot)$ . ☒ JA
- o een nulpunt ongelijk 0 van  $X^m - X$ , waar  $m = \#K$ .
- o een eenheid van  $K$ .

Optie 1: foute groepskeuze, het is de groep uit optie 2. Optie 3 is volkomen uit de lucht gegrepen. Optie 4 laat alle elementen behalve nul meedoen.