

Faculteit FEW 1e toets Inleiding Algebra
 (I Wisk.)
 Vrije Universiteit 23 november 2000

Als U een van de onderdelen niet kunt maken,
 dan mag U toch dergelijke onderdelen
 gebruiken bij Uw antwoord van andere onderdelen.

1

- V is een verzameling. Geef de definitie van R is een *equivalentie relatie* op V en
- van de *equivalentie klasse* van het element $v \in V$.
- Hoe definieer je tevens in deze situatie de verzameling V/R ?
- Geef de definitie van een *operatie* $*$ op de verzameling V en
- hoe definieer je dan: de equivalentie relatie R op V is een *congruentie relatie* voor de operatie $*$?
- Formuleer de stelling van het *delingsalgorithme*.
- Definieer: d is de *grootste gemene deler* van de gehele getallen $\{a_1, \dots, a_n\}$. Zijn deze gehele getallen nog aan beperkingen onderworpen?
- Hoe luidt de definitie van een *abelse groep*?
- Definieer een *restklasse* en een *priemrestklasse* modulo m , waarbij $m \geq 2$ in $\mathbb{Z}$.

2

- a. Bepaal de verzameling van gehele getallen (x, y) , die voldoen aan $3x + 21y \equiv 1 \pmod{7}$.
- b. Bepaal de verzameling van gehele getallen (x, y) , die voldoen aan $3x + 21y \equiv 1 \pmod{6}$.
- c. Bepaal gehele getallen a en b die de grootste gemene deler d van $x = 444$ en $y = 684$ schrijven in de vorm $d = ax + by$.

3

Maak 4 van de 6 onderdelen van deze opgave.

We gaan in deze opgave de gehele getallen $\mathbb{Z}$ maken vanuit de afspraak: we kennen de rekenregels voor de natuurlijke getallen en schrijven voor natuurlijke getallen $m, n \in \mathbb{N}$ tevens $m < n$ als er een natuurlijk getal u is met $m + u = n$. Zijn verder $m, n \in \mathbb{N}$ verschillende natuurlijke getallen, dan is òf $m < n$ òf $n < m$.

- a. Aan welke rekenregels voldoet de verzameling van de natuurlijke getallen $\mathbb{N} = \{1, 2, 3, \dots\}$ voor de optelling en de vermenigvuldiging? Is $\mathbb{N}$ voor een van deze operaties een abelse groep? Beargumenteer Uw antwoord bij deze laatste vraag.
- b. Beschouw op het cartesisch product $V = \mathbb{N} \times \mathbb{N} = \{(m, n) | m, n \in \mathbb{N}\}$ de relatie R , gegeven door

$$\forall m, n, u, v \in \mathbb{N} : (m, n)R(u, v) \Leftrightarrow m + v = u + n.$$

Bewijs dat R een equivalentie relatie op V is.

- c. Bewijs, dat U de elementen van V/R kunt representeren door de elementen van de volgende vorm: $(1, n)$ waarbij $1 < n$, van de vorm $(u, 1)$ waarbij $u > 1$ is, tesamen met het element $(1, 1)$.

Hint: laat zien: als $u \in \mathbb{N}$, dan $(m, n)R(m + u, n + u)$.

d. Bewijs dat R een congruentie relatie is voor de plaatsgewijze optelling

$$\forall m, n, m', n' : (m, n) + (m', n') := (m + m', n + n').$$

e. Schrijf nu de equivalentieklasse van (m, n) als $\overline{(m, n)}$. We weten dan uit de theorie, dat de verzameling V/R van equivalentieklassen een operatie $\oplus$ heeft, gedefinieerd door

$$\forall m, n, m', n' : \overline{(m, n)} \oplus \overline{(m', n')} := \overline{(m + m', n + n')}.$$

Laat zien, dat V/R voor de operatie $\oplus$ een abelse groep is, met neutraal element $\overline{(1, 1)}$ en dat de klassen $\overline{(1, m)}$ en $\overline{(m, 1)}$ elkaars tegengestelde zijn.

f. We maken een afbeelding $f : \mathbb{N} \rightarrow V/R$ door te definiëren

$$\forall n \in \mathbb{N} : f(n) := \overline{(1, n + 1)}.$$

Laat zien, dat f injectief is en voldoet aan

$$\forall m, n \in \mathbb{N} : f(m + n) = f(m) \oplus f(n).$$

Honorering:

voor opgave 1: 10 punten

voor opgave 2 en 3: elk onderdeel 5 punten.

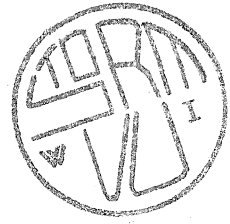
U kunt dus totaal $10 + (3 + 4) \times 5 = 45$ punten behalen

Het eencijfer E wordt berekend aan de hand van de formule

$$E = \frac{\text{behaald} + 5}{5},$$

gevolgd door afronden.

Faculteit FEW 1e toets Inleiding Algebra
(I Wisk.)
Vrije Universiteit 23 november 2000



Als U een van de onderdelen niet kunt maken,
dan mag U toch dergelijke onderdelen
gebruiken bij Uw antwoord van andere onderdelen.

4

- V is een verzameling. Geef de definitie van R is een *equivalentie relatie* op V en
- van de *equivalentie klasse* van het element $v \in V$.

R is een equivalentie relatie op V als $R \subset V \times V$ - in plaats van $(v, w) \in R$ schrijven we verder vRw - en als er voldaan is aan de volgende drie eigenschappen:

1. $\forall v \in V : vRv$.
2. $\forall v, w \in V : vRw \Rightarrow wRv$.
3. $\forall u, v, w \in V : uRv, vRw \Rightarrow uRw$.

De equivalentie klasse $\bar{v}$ van het element v is de verzameling

$$\bar{v} = \{w \in V \mid wRv\}.$$

- Hoe definieer je tevens in deze situatie de verzameling V/R ?

V/R is de verzameling, waarvan de elementen bestaan uit de equivalentie klassen.

- Geef de definitie van een *operatie* $*$ op de verzameling V en
- hoe definieer je dan: de equivalentie relatie R op V is een *congruentie relatie voor de operatie* $*$

Een operatie $*$ op een verzameling V is een afbeelding $* : V \times V \rightarrow V$. (We schrijven dan het beeld $*((v, w))$ dan meestal $v * w$. De equivalentie relatie R is dan een congruentie relatie voor de operatie $*$ als

$$\forall u, v, x, y \in V : uRv \text{ en } xRy \Rightarrow (u * x)R(v * y).$$

- Formuleer de stelling van de *delingsalgorithme*.

Zij $a, b \in \mathbb{Z}$ met $b \neq 0$, dan zijn er unieke $q, r \in \mathbb{Z}$ zodat

$$a = bq + r \text{ en } 0 \leq r < |b|.$$

- Definieer: d is de *grootste gemene deler* van de gehele getallen $\{a_1, \dots, a_n\}$.

d is een natuurlijk getal met de eigenschappen

$$\forall i : d \mid a_i$$

en

$$e \in \mathbb{Z}, \forall i : e \mid a_i \Rightarrow e \mid d.$$

- Hoe luidt de definitie van een *abelse groep*?

Een abelse groep is een verzameling met een operatie, die associatief is, een neutraal element heeft, elk element heeft een inverse voor deze operatie en de operatie is abels. (U mag natuurlijk ook de definitie in formule vorm geven: een abelse groep is een verzameling A met een operatie $*$, zodat

a1. $\forall a, b, c \in A : a * (b * c) = (a * b) * c.$

a2. $\exists e \in A : \forall a \in A : e * a = a * e = a.$

3. $a \in A \Rightarrow \exists a' \in A : a * a' = a' * a = e.$

4. $\forall a, b \in A : a * b = b * a.$

- Definieer een *restklasse* en een *priemrestklasse* modulo m , waarbij $m \geq 2$ in $\mathbb{Z}$.

Een restklasse modulo m is een equivalentie klasse voor de relatie R op $\mathbb{Z}$, gedefinieerd door $xRy \Leftrightarrow m|x - y$. Schrijven we dan de equivalentie klasse van x als $\bar{x}$, dan is deze klasse een priemrestklasse (enkel) wanneer $\text{ggd}(x, m) = 1$, (of: enkel, wanneer x en m relatief priem zijn.)

5

- Bepaal de verzameling van gehele getallen (x, y) , die voldoen aan $3x + 21y \equiv 1 \pmod{7}$.
- Bepaal de verzameling van gehele getallen (x, y) , die voldoen aan $3x + 21y \equiv 1 \pmod{6}$.
- Bepaal gehele getallen a en b die de grootste gemene deler d van $x = 444$ en $y = 684$ schrijven in de vorm $d = ax + by$.

- Als er een oplossing voor dit stelsel, (1) is, dan is er een $k \in \mathbb{Z}$ met $3x + 21y = 1 + 7k \Rightarrow 3x \equiv 1 \pmod{7} \Rightarrow \exists m \in \mathbb{Z} : x = 5 + 7m$ (2). Vul (2) in het stelsel (1) in:

$$3(5 + 7m) + 21y = 1 + 7k \Rightarrow 21m + 21y = -14 + 7k \Rightarrow 3(m + y) = k - 2.$$

Dan is $k - 2$ een 3-voud, dus $\exists n \in \mathbb{Z} : k - 2 = 3n = 3(m + y) \Rightarrow y = m - n$ (3). Vullen we nu (3) en (2) in het stelsel (1) in, dan zien we dat dit het stelsel oplost. Ergo: Als het stelsel (1) oplosbaar is, dan gelden (2) en (3), terwijl omgekeerd (2) en (3) het stelsel oplossen.

- Als er een oplossing (x, y) zou zijn met gehele getallen (x, y) dan zou er een $k \in \mathbb{Z}$ zijn zodat $3x + 21y = 1 + 6k$. Het linkerlid ervan zou dan deelbaar zijn door 3, maar het rechterlid niet. Dit kan niet, dus er is geen oplossing voor dit stelsel.

- We passen het Euclidisch delingsalgorithme toe:

684	1	0	-
444	0	1	1
240	1	-1	1
204	-1	2	1
36	2	-3	6

Nu blijkt $36|204$, dus het algorithme eindigt hier en hebben we

$$2 \cdot 684 + (-3) \cdot 444 = 36,$$

dus $b = 2$ en $a = -3$.

6

We gaan in deze opgave de gehele getallen $\mathbb{Z}$ maken vanuit de afspraak: we kennen de rekenregels voor de natuurlijke getallen en schrijven voor natuurlijke getallen $m, n \in \mathbb{N}$ $m < n$ als er een natuurlijk getal u is met $m + u = n$. Zijn verder $m, n \in \mathbb{N}$ verschillende natuurlijke getallen, dan is $\text{of } m < n \text{ of } n < m$.

- Aan welke rekenregels voldoet de verzameling van de natuurlijke getallen $\mathbb{N} = \{1, 2, 3, \dots\}$ voor de optelling en de vermenigvuldiging? Is $\mathbb{N}$ voor een van deze operaties een abelse groep?