

1

V is een verzameling, "+" en "." zijn operaties op V en $0, 1$ zijn twee elementen van V . We herhalen de rekenregels van het college: voor elk drietal, niet perse verschillende elementen a, b, c van V geldt:

A1. $a + (b + c) = (a + b) + c$.

A2. $a + 0 = 0 + a = a$.

A3. Bij a is er een $a' \in V$ zodat $a + a' = a' + a = 0$.

A4. $a + b = b + a$.

A5. $a(b + c) = ab + ac$ en $(b + c)a = ba + ca$.

A6. $a(bc) = (ab)c$.

A7. $1a = a1 = a$.

A8. $ab = ba$.

A9. $ab = 0$ impliceert $a = 0$ of $b = 0$.

A10. Als $a \neq 0$ dan is er een $a' \in V$ zodat $aa' = a'a = 1$.

N.B. Als gebruikelijk laten we de "." in formules weg.

a. Welke van de bovenstaande regels zijn nodig om de volgende begrippen te definiëren:

a1. $(V, +)$ is een abelse groep.

a2. $(V, +, \cdot)$ is een CUR.

a3. $(V, +, \cdot)$ is een ITG.

a4. $(V, +, \cdot)$ is een lichaam.

b. Als k een lichaam is, geef de definitie van: $(V, +)$ is een vectorruimte over k .

2

Zij $d(X) = X^3 + X + \bar{1} \in \mathbb{Z}/2\mathbb{Z}[X]$.

a. Laat zien, dat $d(X)$ irreducibel is in $\mathbb{Z}/2\mathbb{Z}[X]$.

b. Laat zien, dat de verzameling

$$\mathcal{R} = \{a + bX + cX^2 \mid a, b, c \in \mathbb{Z}/2\mathbb{Z}\}$$

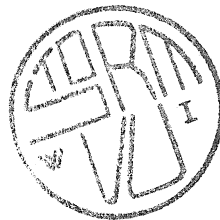
een volledig stelsel representanten is voor het lichaam $K := \mathbb{Z}/2\mathbb{Z}[X]/(d(X)\mathbb{Z}/2\mathbb{Z}[X])$.

c. Hoeveel elementen heeft K ?

d. Elk element $X^n, (0 \leq n \leq 7)$ heeft een representant in $\mathcal{R}$. Bepaal deze representant.

e. Heeft de klasse van X^{17} een inverse in K ? Zo ja, bepaal de representant hiervan in $\mathcal{R}$.

f. Algemener: heeft de klasse van $X^n, (n > 7)$ een inverse in K ? Zo ja, bepaal de representant hiervan in $\mathcal{R}$.



3

Zij $a = \frac{t}{n}$ een wortel van de veelterm $F(X) = a_0 + a_1X + \dots + a_dX^d \in \mathbb{Q}[X]$. We nemen aan, dat de graad van F gelijk aan d en $d \geq 1$ is. Door de breuk a zover mogelijk te vereenvoudigen nemen we aan, dat $\gcd(t, n) = 1$.

- a. Leid af, door $F(a) = 0$ uit te schrijven en noemers weg te werken, dat

$$a_0n^d = -t(a_1n^{d-1} + \dots + a_dt^{d-1}).$$

Gebruik dit, om te bewijzen, dat $t|a_0$. (1).

- b. Laat op een analoge wijze zien, dat $n|a_d$. (2). Gebruik de resultaten (1) en (2) om aan te tonen, dat $X^3 + X + 1$ irreducibel is in $\mathbb{Q}[X]$.

4

- a. Bepaal de grootste gemene deler d van de getallen 325 en 234 en schrijf d in de vorm $d = 325x + 234y$ met gehele getallen x en y .
- b. Bepaal alle oplossingen (x, y) van $d = 325x + 234y$ met $x, y \in \mathbb{Z}$.
- c. Voor welke waarde(n) van $x \in \mathbb{Z}$ met $0 \leq x \leq 1000$ geldt

$$x \cong 1 \pmod{129} \quad \text{en} \quad x \cong 4 \pmod{5}?$$

Honorering: voor elk onderdeel is maximaal 5 punten haalbaar. Bij 13 onderdelen derhalve 65 punten. Het eindcijfer E wordt berekend naar:

$$E = \frac{\text{totaal behaald} + 5}{7},$$

gevolgd door afronden.