# Toepassingen van Algebra oplossingen oefeningen

Pieter-Jan Coenen

December 2016

# Inhoudsopgave

# 1 Oefenzitting 1

## 1.1 Oefening 1

Op $\mathbb{R}$ definiëren we de samenstellingswet $a\tau b = a + b + a^2b^2$

(a) Deze wet heeft een neutraal element. Welk?

(b) Ze is niet associatief. Ga na!

(c) Ze is commutatief. Waarom?

**Oplossingsmethode**

Ga al deze eigenschappen na voor de gegeven samenstellingswet. De eigenschappen kunnen worden gevonden in de cursus deel I blz 79.

**Oplossing**

(a) Een snelle intuïtieve methode om dit op te lossen is door te testen of het neutraal element voor de optelling (0) of het neutraal element voor de vermenigvuldiging (1) een neutraal element is voor deze samenstellingswet.
We proberen eerst of het toepassen van de samenstellingswet op 0 en $x \in \mathbb{R}$ terug resulteert in $x$.

$$0\tau x = 0 + x + 0^2x^2 = x$$

$$x\tau 0 = x + 0 + x^20^2 = x$$

0 is dus het neutraal element.

Tweede manier om dit op te lossen is door de uitdrukking $e\tau x$ uit te werken en op zoek gaan naar een waarde van $e$ zodat het $e\tau x = x$

$$\begin{aligned} & e\tau x = x \\ \Leftrightarrow & e + x + e^2x^2 = x \\ \Leftrightarrow & e + e^2x^2 = 0 \\ \Leftrightarrow & e(1 + ex^2) = 0 \\ \Leftrightarrow & \begin{cases} e = 0 \\ e = \frac{-1}{x^2} \end{cases} \end{aligned}$$

Ook met deze mehode is dus duidelijk dat 0 het neutraal element is.

(b) Een samenstellingswet $\top$ is associatief $\Leftrightarrow \forall x, y \in A : x\top(y\top z) = (x\top y)\top z)$. (I blz 80).
We kunnen dus met een tegenvoorbeeld aantonen dat deze samenstellingswet niet associatief is.
Bijvoorbeeld:

$$1\tau(2\tau 3) = 1\tau(2+3+4*9) = 1\tau 41 = 1+41+1^2 41^2 = 1723$$

$$(1\tau 2)\tau 3 = (1+2+1*4)\tau 3 = 7\tau 3 = 7+3+7^2 3^2 = 451$$

(c) $\top$ is commutatief als $\Leftrightarrow \forall x, y \in A : x\top y = y\top x$ (I blz. 80).
Deze samenstellingswet maakt enkel gebruik van de operatoren "+" en "*". Aangezien dat deze beide commutatief zijn zal ook de samenstellingswet commutatief zijn.

$$\forall x, y \in \mathbb{R} : x\tau y = x+y+x^2y^2 = y+x+y^2x^2 = y\tau x$$

## 1.2 Oefening 2

Bewijs dat in $\mathbb{R}^2 \times \mathbb{R}^2$ volgende relaties equivalentierelaties zijn:

$$G = \{((a,b),(c,d))|a^2+b^2 = c^2+d^2\}$$

$$H = \{((a,b),(c,d))|b-a = d-c\}$$

$$J = \{((a,b),(c,d))|a+b = c+d\}$$

Welke zijn de partities die hierdoor gedefinieerd worden? Welke partitie definieert $H \cap J$?

### Oplossingsmethode

Een relatie $R \subseteq A \times A$ is een equivalentierelatie (I blz.58) $\Leftrightarrow$

1. $R$ is reflexief $\Leftrightarrow$ elk element staat in relatie met zichzelf (I blz 59) :

   $$\forall x \in A : (x,x) \in R \text{ of } \forall x \in A : xRx$$

   Voorbeeld hiervan is de "equals-relatie" elk element is gelijk aan zichzelf $x = x$.

2. $R$ is symmetrisch $\Leftrightarrow$ de relatie in twee richtingen geldt (I blz 59) :

   $$(x,y) \in R \Rightarrow (y,x) \in R \text{ of } xRy \Rightarrow yRx$$

   De "equals-relatie" is bijvoorbeeld symmetrisch want als $x = y \Rightarrow y = x$. De kleiner dan relatie is bijvoorbeeld niet symmetrisch wat als $x < y \nRightarrow y < x$.

3. $R$ is transitief $\Leftrightarrow$ de relatie kan doorgegeven worden (erfelijk is). (I blz 60) :

   $$(x, y) \in R \text{ en } (y, z) \in R \Rightarrow (x, z) \in R \text{ of } xRy \text{ en } yRz \Rightarrow xRz$$

   De kleiner dan relatie is bijvoorbeeld transitief want als $x < y$ en $y < z \Rightarrow x < z$.

**Oplossing voor G**

1. $G$ is reflexief want

   $$\forall (x, y) \in \mathbb{R}^2 \Rightarrow x^2 + y^2 = x^2 + y^2$$

   dus geldt dat

   $$\forall (x, y) \in \mathbb{R}^2 : (x, y)G(x, y)$$

2. $G$ is symmetrisch want

   $$\forall (x, y), (z, q) \in \mathbb{R}^2 : x^2 + y^2 = z^2 + q^2 \Rightarrow z^2 + q^2 = x^2 + y^2$$

   dus geldt dat

   $$(x, y)G(z, q) \Rightarrow (z, q)G(x, y)$$

3. $G$ is transitief want

   $$\forall (x, y), (z, q), (v, w) \in \mathbb{R}^2 : (x^2+y^2 = z^2+q^2 \ \& \ z^2+q^2 = v^2+w^2) \Rightarrow x^2+y^2 = v^2+w^2$$

   dus geldt dat

   $$(x, y)G(z, q) \ \& \ (z, q)G(v, w) \Rightarrow (x, y)G(v, w)$$

Elke equivalentie relatie definieert een partitie (stelling 9.1 deel I blz 62). Aangezien dat aan alle voorwaarden is voldaan, is $G$ een equivalentierelatie.

**Oplossing voor H**

1. $H$ is reflexief want

   $$\forall (x, y) \in \mathbb{R}^2 \Rightarrow y - x = y - x$$

   dus geldt dat

   $$\forall (x, y) \in \mathbb{R}^2 : (x, y)H(x, y)$$

2. $H$ is symmetrisch want

   $$\forall (x, y), (z, q) \in \mathbb{R}^2 : y - x = q - z \Rightarrow q - z = y - x$$

   dus geldt dat

   $$(x, y)H(z, q) \Rightarrow (z, q)H(x, y)$$

3. $H$ is transitief want

   $\forall(x,y),(z,q),(v,w) \in \mathbb{R}^2 : (y-x = q-z \ \& \ q-z = w-v) \Rightarrow y-x = w-v$

   dus geldt dat

   $$(x,y)H(z,q) \ \& \ (z,q)H(v,w) \Rightarrow (x,y)H(v,w)$$

Aangezien dat aan alle voorwaarden is voldaan, is $H$ een equivalentierelatie.

**Oplossing voor J**

1. $J$ is reflexief want

   $$\forall(x,y) \in \mathbb{R}^2 \Rightarrow x+y = x+y$$

   dus geldt dat

   $$\forall(x,y) \in \mathbb{R}^2 : (x,y)J(x,y)$$

2. $J$ is symmetrisch want

   $$\forall(x,y),(z,q) \in \mathbb{R}^2 : x+y = z+q \Rightarrow q+z = x+y$$

   dus geldt dat

   $$(x,y)J(z,q) \Rightarrow (z,q)J(x,y)$$

3. $J$ is transitief want

   $\forall(x,y),(z,q),(v,w) \in \mathbb{R}^2 : (x+y = z+q \ \& \ z+q = v+w) \Rightarrow x+y = v+w$

   dus geldt dat

   $$(x,y)J(z,q) \ \& \ (z,q)J(v,w) \Rightarrow (x,y)J(v,w)$$

Aangezien dat aan alle voorwaarden is voldaan, is $J$ een equivalentierelatie.

**Oplossing bijvragen**

Aangezien G, H en J alle drie equivalentierelaties zijn definiëren ze ook alle drie een partitie (zie stelling 9.1 deel I blz 62).

$H \cap J$ zijn dus alle koppels uit $\mathbb{R}^2$ die behoren tot zowel H als J.
Dit geeft de volgende formele beschrijving:

$$H \cap J = \{((a,b),(c,d))|b-a = d-c \ \& \ a+b = c+d\}$$

We kunnen dit verder uitwerken door dit in een stelsel te gieten:

$$\begin{cases} b-a=d-c \\ a+b=c+d \end{cases}$$

Als we dit stelsel verder uitwerken krijgen we:

$$\begin{cases} b-a=d-c \\ a+b=c+d \end{cases} = \begin{cases} 2b=2d \\ a+b=c+d \end{cases} = \begin{cases} b=d \\ a=c \end{cases}$$

Nu kunnen we $H \cap J$ schrijven als:

$$H \cap J = \{((a,b),(c,d))|a=c \ \& \ b=d\}$$
$$= \{(x,y)|x \in \mathbb{R}^2, y \in \mathbb{R}^2, x=y\}$$
$$= \{(x,x)|x \in \mathbb{R}^2\}$$

## 1.3 Oefening 3

Los het volgende stelsel op in (mod 7):

$$\begin{cases} 3x_1-2x_2+6x_3=4 \\ 4x_1-x_2+x_3=0 \\ 2x_1-x_2+2x_3=-1 \end{cases}$$

### Oplossingsmethode

Zie volledig uitgewerkt voorbeeld in deel I blz. 85.
Je kan beter geen deling gebruiken, want in sommige omstandigheden zorgt dit voor fouten. In plaats van een getal $x$ dus te delen door $x$ om een 1 te bekomen moet je opzoek gaan naar een getal $y$ zodat $x*y=1$.
Bijvoorbeeld in modulo 5, om van 2 naar 1 te gaan doe je $2*3=6 \bmod 5=1$.

Let op als je een gelijkaardige opgave krijgt met (mod $k$) waarbij $k$ geen priemgetal is, meer info zie blz 86 voorbeeld 14.5.

### Oplossing

We zetten dit stelsel eerst om naar een matrix

$$\left[\begin{array}{ccc|c} 3 & -2 & 6 & 4 \\ 4 & 1 & 1 & 0 \\ 2 & 1 & 2 & -1 \end{array}\right] \xrightarrow{R_1=R_1*5} \left[\begin{array}{ccc|c} 15 & -10 & 30 & 20 \\ 4 & 1 & 1 & 0 \\ 2 & 1 & 2 & -1 \end{array}\right]$$

$$\xrightarrow{R_1=R_1 \bmod 7} \left[\begin{array}{ccc|c} 1 & 4 & 2 & 6 \\ 4 & 1 & 1 & 0 \\ 2 & 1 & 2 & -1 \end{array}\right] \xrightarrow[R_3=R_3-2*R_1]{R_2=R_2-4*R_1} \left[\begin{array}{ccc|c} 1 & 4 & 2 & 6 \\ 0 & -15 & -7 & -24 \\ 0 & -7 & -2 & -13 \end{array}\right]$$

$$\xrightarrow[R_3=R_3 \bmod 7]{R_2=R_2 \bmod 7} \left[\begin{array}{ccc|c} 1 & 4 & 2 & 6 \\ 0 & 6 & 0 & 4 \\ 0 & 0 & 5 & 1 \end{array}\right] \xrightarrow[R_3=R_3*3 \ (mod\ 7)]{R_2=R_2*6 \ (mod\ 7)} \left[\begin{array}{ccc|c} 1 & 4 & 2 & 6 \\ 0 & 1 & 0 & 3 \\ 0 & 0 & 1 & 3 \end{array}\right]$$

Dit resulteert in

$$\begin{cases} x_1 + 4x_2 + 2x_3 = 6 \\ x_2 = 3 \\ x_3 = 3 \end{cases} \rightarrow \begin{cases} x_1 + 18 \ (\text{mod } 7) = x_1 + 4 = 6 \\ x_2 = 3 \\ x_3 = 3 \end{cases} \rightarrow \begin{cases} x_1 = 2 \\ x_2 = 3 \\ x_3 = 3 \end{cases}$$

## 1.4 Oefening 4

Bepaal de isometrieën van een gelijkzijdige driehoek. Stel voor deze isometrieën de bewerkingstabel op, onder de samenstellingswet $\circ$.

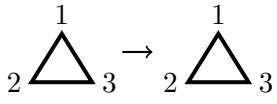
### Oplossingsmethode

Volledig uitgewerkt voorbeeld is te vinden in de cursus deel I op blz 94-95.
Als alle $n$ zijden dezelfde lengte hebben, dan geldt dat het aantal isometrieën gelijk is aan $2n$.

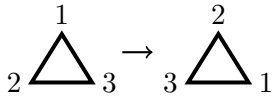
### Oplossing

Bij een gelijkzijdige driehoek hebben we dus $3 * 2 = 6$ isometrieën.

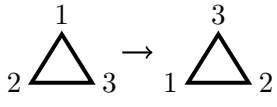
1. $e$ : de identieke afbeelding



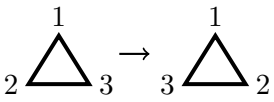

2. $r_1$ : rotatie om het middelpunt over 90° in wijzerzin



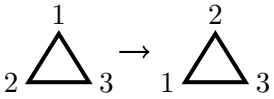

3. $r_2$ : rotatie om het middelpunt over 180° in wijzerzin



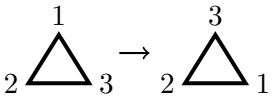
4. $m_1$ : spiegeling in de middellijn door bovenste hoekpunt




5. $m_2$ : spiegeling in de diagonaal door hoekpunt rechtsonder



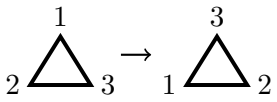

6. $m_3$ : spiegeling in de diagonaal door hoekpunt linksonder



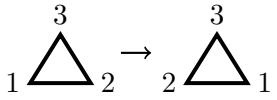

Dit geeft ons de volgende bewerkingstabel:

| $\circ$ | $e$ | $r_1$ | $r_2$ | $m_1$ | $m_2$ | $m_3$ |
|---|---|---|---|---|---|---|
| $e$ | $e$ | $r_1$ | $r_2$ | $m_1$ | $m_2$ | $m_3$ |
| $r_1$ | $r_1$ | $r_2$ | $e$ | $m_3$ | $m_1$ | $m_2$ |
| $r_2$ | $r_2$ | $e$ | $r_1$ | $m_2$ | $m_3$ | $m_1$ |
| $m_1$ | $m_1$ | $m_2$ | $m_3$ | $e$ | $r_1$ | $r_2$ |
| $m_2$ | $m_2$ | $m_3$ | $m_1$ | $r_2$ | $e$ | $r_1$ |
| $m_3$ | $m_3$ | $m_1$ | $m_2$ | $r_1$ | $r_2$ | $e$ |

$m_3$ wordt bijvoorbeeld bekomen door eerst $r_2$ toe te passen




op dit resultaat passen we nu $m_1$ toe




Het toepassen van "$m_1 \circ r_2$" is dus hetzelfde als het toepassen van $m_3$.

De verkregen tabel is duidelijk niet symetrisch, dit betekend dat niet alle samenstellingen commutatief zijn en dus dat $\circ$ niet commutatief is.

## 1.5 Oefening 5

Een latijns vierkant is een n×n tabel waarin slechts n verschillende elementen voorkomen.
In elke rij en elke kolom komt namelijk elk element juist eenmaal voor.

(a) Bewijs dat de bewerkingstabel voor een eindige groep steeds een Latijns vierkant is.

(b) Is dit ook een voldoende voorwaarde om een groep te hebben? Bepaal of volgend Latijns vierkant de bewerkingstabel van een groep is:

| $\tau$ | a | b | c | d | e | f |
|---|---|---|---|---|---|---|
| a | c | e | a | b | f | d |
| b | f | c | b | a | d | e |
| c | a | b | c | d | e | f |
| d | e | a | d | f | c | b |
| e | d | f | e | c | b | a |
| f | b | d | f | e | a | c |

**Oplossingsmethode**

Definitie 2.1 (deel I blz. 93) : Een groep is een monoïde waarvoor elk element symmetriseerbaar is. Dus $\langle A, * \rangle$ is een groep asa :

- $*$ is overal bepaald
- $x * (y * z) = (x * y) * z$ (associatief)
- $\exists e \in A : \forall x \in A : x * e = e * x = x$ (neutraal element)
- $\forall x : \exists x^{-1} \in A : x * x^{-1} = x^{-1} * x = e$ (symmetriseerbaar)

**Oplossing**

(a) Een groep is overal bepaald, dus de tabel is volledig ingevuld.

Nu bewijzen we dat elk element maar één keer voorkomt op elke rij. Dit doen we door te veronderstellen dat een element twee keer voorkomt op één rij en zo een contradictie te bekomen.

*Bewijs.* Een element komt twee keer voor op één rij als er een rij bestaat met rij element $a$ en er twee verschillende kolommen bestaan met elementen $x$ en $y$ waarbij $x$ en $y$ verschillend zijn zodat $a \tau x = a \tau y$

Nu vinden we :

$$\begin{aligned} & a\tau x = a\tau y \\ \Leftrightarrow\, & a^{-1}\tau(a\tau x) = a^{-1}\tau(a\tau y) \\ \Leftrightarrow\, & (a^{-1}\tau a)\tau x = (a^{-1}\tau a)\tau y \\ \Leftrightarrow\, & e\tau x = e\tau y \\ \Leftrightarrow\, & x = y \end{aligned}$$

Aangezien dat $x$ verschillend is van $y$ kan dit dus niet en hebben we een contradictie. □

Merk op dat we in het bovenstaande bewijs gebruik maken van het feit dat een groep associatief en symmetrisch is en neutraal element heeft.
Om te bewijzen dat er geen element twee keer voorkomt in een kolom is het bewijs analoog.

(b) We kijken of deze tabel voldoet aan alle eigenschappen van een groep:

- Deze bewerking is duidelijk overal bepaald, want de tabel is volledig ingevuld.
- Associativiteit is niet zo heel eenvoudig om na te kijken. Daarom proberen we dit systematisch rij per rij te doen.
  We gaan altijd $x\tau(y\tau[a,b,c,d,e,f])$ berekenen en kijken of dit gelijk is aan $(x\tau y)\tau[a,b,c,d,e,f]$.
  Op die manier vinden we het volgende tegenvoorbeeld:
  $a\tau(b\tau b) = a$ en $(a\tau b)\tau b = f$

- Om het neutraal element te zoeken in deze tabel zijn we dus opzoek naar een rij en kolom waar elk element opzichzelf wordt afgebeeld.
  Het is duidelijk dat voor "c" elk element op zichzelf wordt afgebeeld. "c" is dus het neutraal element.
- Deze bewerking is duidelijk symmetriseerbaar want voor elk element kunnen we een symmetrisch element vinden.
  "a", "b","c" en "f" zijn zelf het symmetrisch element voor zichzelf. Want bijvoorbeeld $b\tau b = b\tau b = c$, dit klopt want "c" is het neutraal element.
  Het symmetrisch element voor "d" is "e" en het symmetrisch element voor "e" is dus "d" want $d\tau e = e\tau d = c$.

Het Latijns vierkant kan dus geen bewerkingstabel zijn van een groep, want het is niet associatief.

# 2 Oefenzitting 2

## 2.1 Oefening 1

Bewijs dat $\mathbb{R}_0 \times \mathbb{R}$ voorzien van de samenstellingswet $((a,b),(c,d)) \mapsto (ac, bc+d)$ een groep is. Is hij abels ?

### Oplossingsmethode

Definitie 2.1 (deel I blz. 93) : Een groep is een monoïde waarvoor elk element symmetriseerbaar is. Dus $\langle A, * \rangle$ is een groep asa :

- $*$ is overal bepaald
- $x * (y * z) = (x * y) * z$ (associatief)
- $\exists e \in A : \forall x \in A : x * e = e * x = x$ (neutraal element)
- $\forall x : \exists x^{-1} \in A : x * x^{-1} = x^{-1} * x = e$ (symmetriseerbaar)

Als $*$ commutatief is, dan is de groep abels.

### Oplossing

- $*$ is overal bepaald in $\mathbb{R}_0$, dus $ac \in \mathbb{R}_0$
  $*$ en $+$ zijn ook overal bepaald in $\mathbb{R}$, dus $bc + d \in \mathbb{R}$.

  De bewerking is dus overal bepaald.

- Associatief want

  $$((x,y),((i,j),(u,v))) = ((x,y),(iu, ju+v)) = (xiu, yiu + ju + v)$$

  en

  $$(((x,y),(i,j)),(u,v)) = ((xi, yi+j),(u,v)) = (xiu, yiu + ju + v)$$

- Voor het neutraal element $(e_1, e_2)$ moet gelden dat :

  $$\begin{cases} ((x,y),(e_1,e_2)) = (x,y) \\ ((e_1,e_2),(x,y)) = (x,y) \end{cases}$$

  Dus moet gelden dat

  $$\begin{cases} ((x,y),(e_1,e_2)) = (xe_1, ye_1 + e_2) = (x,y) \\ ((e_1,e_2),(x,y)) = (e_1 x, e_2 x + y) = (x,y) \end{cases}$$

$$= \begin{cases} xe_1 = x \\ e_1 x = x \\ ye_1 + e_2 = y \\ e_2 x + y = y \end{cases}$$

Dus dan zal

$$\begin{cases} e_1 = 1 \\ e_2 = 0 \end{cases}$$

$(1, 0)$ is dus het neutraal element.

- Symmetriseerbaarheid:

$$((x, y), (x^{-1}, y^{-1})) = (1, 0) \Leftrightarrow \begin{cases} xx^{-1} = 1 \\ yx^{-1} + y^{-1} = 0 \end{cases}$$

$$\Leftrightarrow \begin{cases} x^{-1} = \frac{1}{x} \\ y^{-1} = -\frac{y}{x} \end{cases}$$

Het symmetrisch element voor $(x, y)$ is dus $(\frac{1}{x}, -\frac{y}{x})$

Aangezien dat aan alle eigenschappen van een groep zijn voldaan, is dit dus duidelijk een groep.

Een groep is abels als de bewerking commutatief is, we testen dit even uit:

$$((x, y), (v, w)) = (xv, yv + w)$$

$$((v, w), (x, y)) = (vx, wx + y)$$

Het is duidelijk dat de bovenstaande bewerkingen niet aan elkaar gelijk zijn en de groep dus niet commutatief (of abels) is.

## 2.2 Oefening 2

$\langle S_n, \circ \rangle$ is de groep van permutaties van een verzameling van n elementen. Stel de samenstellingstabel op voor $\langle S_3, \circ \rangle$. Zijn er deelgroepen? Normaaldelers?

### Oplossingsmethode

Voorbeelden voor het opstellen van een bewerkingstabel kan je vinden in deel I blz. 94-95.

In oefenzitting 1 is oefening 4 gelijkaardig.

De elementen van een deelgroep zijn een deelverzameling van de elementen van een groep en de deelgroep voldoet aan alle eigenschappen van een groep. Zie definitie 2.1 deel I blz 93 en stelling 2.1 deel I blz 94.

Een groep $S$, die een deelgroep is van $G$ is een normaaldeler van $G \Leftrightarrow$

$$\forall g \in G : g^{-1}Sg = g$$

of

$$\forall x \in G : Sx = xS \quad \text{met } xS = \{x\tau s | s \in S\}$$

Zie definitie 4.2 en stelling 4.2 deel I blz 105. Voorbeeld zie voorbeeld 4.1 blz 107.

**Oplossing**

Voor een rij van 3 elementen zijn er $3! = 6$ permutaties mogelijk. We zoeken eerst deze permutaties.

1. $e$ : de identieke afbeelding

$$[1, 2, 3] \rightarrow [1, 2, 3]$$

2. $r_1$ : we schuiven alle elementen één positie naar rechts

$$[1, 2, 3] \rightarrow [3, 1, 2]$$

3. $r_2$ : we schuiven alle elementen twee posities naar rechts

$$[1, 2, 3] \rightarrow [2, 3, 1]$$

4. $m_1$ : verwissel het laatste en eerste element

$$[1, 2, 3] \rightarrow [3, 2, 1]$$

5. $m_2$ : verwissel de eerste twee elementen

$$[1, 2, 3] \rightarrow [2, 1, 3]$$

6. $m_3$ :verwissel de laatste twee elementen

$$[1, 2, 3] \rightarrow [1, 3, 2]$$

Dit geeft ons de volgende samenstellingstabel:

| $\circ$ | $e$ | $r_1$ | $r_2$ | $m_1$ | $m_2$ | $m_3$ |
|---|---|---|---|---|---|---|
| $e$ | $e$ | $r_1$ | $r_2$ | $m_1$ | $m_2$ | $m_3$ |
| $r_1$ | $r_1$ | $r_2$ | $e$ | $m_3$ | $m_1$ | $m_2$ |
| $r_2$ | $r_2$ | $e$ | $r_1$ | $m_2$ | $m_3$ | $m_1$ |
| $m_1$ | $m_1$ | $m_2$ | $m_3$ | $e$ | $r_1$ | $r_2$ |
| $m_2$ | $m_2$ | $m_3$ | $m_1$ | $r_2$ | $e$ | $r_1$ |
| $m_3$ | $m_3$ | $m_1$ | $m_2$ | $r_1$ | $r_2$ | $e$ |

Aangezien dat een deelgroep zelf ook een groep is, moet deze dus altijd het neutraal element van de groep bevatten. Daarnaast moet de deelgroep ook overal bepaald zijn. Als de groep associatief is dan is de deelgroep dat normaal gezien ook.

We hebben sowieso de triviale deelgroep die enkel het neutraal element bevat en de triviale deelgroep die de volledige groep bevat.
We zien nu in de tabel dat er één niet-triviale deelgroep is, dit is de deelgroep die enkel de rotaties bevat $R = \{e, r_1, r_2\}$.
Tot slot vinden we ook nog de volgende deelgroepen: $M_1 = \{e, m_1\}, M_2 = \{e, m_2\}, M_3 = \{e, m_3\}$.
Merk op dat $\{e, r_1\}$ bijvoorbeeld geen deelgroep is want $r_1 \circ r_1 = r_2$ en $r_2$ behoort niet tot die deelgroep.

We moeten nu enkel nog de normaal delers zoeken. We kijken eerst na of de deelgroep van de rotaties $R$ een normaaldeler is. Dit doen we door te kijken of elke linker nevenklassen ook een rechter nevenklassen is (zie oplossingsmethode).

$$Re = R = eR$$
$$Rr_1 = \{e, r_1, r_2\} = r_1R$$
$$Rr_2 = \{e, r_1, r_2\} = r_2R$$
$$Rm_1 = \{m_1, m_2, m_3\} = m_1R$$
$$Rm_2 = \{m_1, m_2, m_3\} = m_2R$$
$$Rm_3 = \{m_1, m_2, m_3\} = m_3R$$

$R$ is dus een normaaldeler van $G$.
Ook de twee triviale deelgroepen zijn uiteraard nevenklassen.
$M_1, M_2, M_3$ zijn geen nevenklassen.
$M_1$ is bijvoorbeeld geen nevenklassen want:

$$M_1r_1 = \{r_1, m_2\} \neq \{r_1, m_3\} = r_1M_1$$

## 2.3 Oefening 3

Zoek de generatoren van de additieve cyclische groepen $\mathbb{Z}_{10}, \mathbb{Z}_{11}, \mathbb{Z}_{12}$

**Oplossingsmethode**

Voor een additieve groep, zoek je een element $g$ zodat

$\forall n \in \mathbb{N}_0 : \quad 0*g = e, \quad 1*g = g, \quad 2*g = g+g, \quad \ldots, \quad n*g = g+g+\cdots+g$

Waarbij $g$ dus alle elementen van die groep kan genereren (en ook geen andere) dus $\forall n \in \mathbb{N}_0$ is $n * g$ een element van die groep.

Voor een additieve groep $\mathbb{Z}_x$ zijn alle getallen $y$ die geen delers gemeenschappelijk hebben met $x$ generatoren voor $\mathbb{Z}_x$.

Zie definitie 2.5 deel I blz 97, definitie 1.3 en voorbeeld 1.5 blz 93.

**Oplossing**

$\mathbb{Z}_{10}$ bevat de elementen $\{0, \ldots, 9\}$ en de generatoren zijn dus $\{1, 3, 7, 9\}$

$\mathbb{Z}_{11}$ bevat de elementen $\{0, \ldots, 10\}$ en de generatoren zijn dus $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

$\mathbb{Z}_{12}$ bevat de elementen $\{0, \ldots, 11\}$ en de generatoren zijn dus $\{1, 5, 7, 11\}$

## 2.4 Oefening 4

Genereer de groep voortgebracht onder vermenigvuldiging door de matrices

$$A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \text{ en } B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Bewijs dat die een niet-abelse groep is van orde 8.

**Oplossingsmethode**

Definitie 2.1 (deel I blz. 93) : Een groep is een monoïde waarvoor elk element symmetriseerbaar is. Dus $\langle A, * \rangle$ is een groep asa :

- $*$ is overal bepaald
- $x * (y * z) = (x * y) * z$ (associatief)
- $\exists e \in A : \forall x \in A : x * e = e * x = x$ (neutraal element)
- $\forall x : \exists x^{-1} \in A : x * x^{-1} = x^{-1} * x = e$ (symmetriseerbaar)

Het aantal elementen van een groep is de orde van de groep. De groep is niet-abels als de bewerking niet commutatief is.
De definitie van een multiplicatieve generator vind je in deel I blz. 97.

**Oplossing**

Zowel $A$ als $B$ zijn diagonaalmatrices, het vermenigvuldigen van twee diagonaal matrices resulteert opnieuw in een diagonaal matrix.
Het vermenigvuldigen van $A$ en $B$ zal dus steeds resulteren in een matrix van de vorm

$$\begin{bmatrix} x_1 & 0 \\ 0 & x_2 \end{bmatrix} \text{ of } \begin{bmatrix} 0 & x_1 \\ x_2 & 0 \end{bmatrix}$$

Waarbij $x_1 = \pm 1$ en $x_2 = \pm 1$.
Hieruit kunnen we dus berekenen dat er in totaal 8 combinaties mogelijk zijn.

We generen eerst alle elementen met de matrix $A$.

$$A^0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad A^1 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \quad A^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \quad A^3 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

Aangezien dat $A^4$ terug gelijk is aan de eenheidsmatrix en we deze al zijn tegen gekomen tijdens de generatie met $A$ stoppen we bij $A^3$.

Nu genereren we alle elementen met de matrix $B$.

$$B^0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad B^1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Nu genereren we ook nog de combinaties van $A$ en $B$.

$$A^1{*}B^1 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad A^2{*}B^1 = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \quad A^2{*}B^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \quad A^3{*}B^1 = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$$

Nu hebben we dus 8 unieke elementen voor onze groep, namelijk:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \quad \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \quad \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \quad \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$$

Nu moeten we nog bewijzen dat deze elementen samen een groep vormen:

- Deze bewerking is duidelijk overal bepaald we hebben alle combinaties van diagonaal matrices met $\pm 1$ als elementen. Deze met elkaar vermenigvuldigen levert terug een diagonaal matrix op van hetzelfde type.

- Het vermenigvuldigen van matrices is associatief
- Deze verzameling bevat het neutraal element voor vermenigvuldiging van matrices, nl. de eenheidsmatrix.
- Elk element kan ook worden gesymmetriseerd.

We kunnen dus spreken over een groep, aangezien deze 8 elementen bevat is de orde van de groep ook 8.

De vermenigvuldiging van matrices is niet commutatief, dus deze groep is niet abels.

## 2.5 Oefening 5

Beschouw een groep $G = (\mathbb{Z}_7/\{0\}, .)$ van de gehele getallen modulo 7 zonder nul en met de vermenigvuldiging modulo 7. Bepaal de orde van al de elementen. Is de groep commutatief?

### Oplossingsmethode

De orde van een element $x$ is het kleinste natuurlijke getal $r$ waarvoor $x^r = e$ met $e$ het neutraal element. Zie def 2.5 deel I blz 97.

### Oplossing

De verzameling $G$ bevat de elementen $\{1, 2, 3, 4, 5, 6\}$, waarbij 1 het neutraal element is.
We gaan nu voor elk element apart zijn orde na.

1. De orde van 1 is 1 want $1^1 = 1$
2. De orde van 2 is 3 want $2^3 = 1$
3. De orde van 3 is 6 want $(3^2)^3 = 2^3 = 1$
4. De orde van 4 is 3 want $4^3 = 1$
5. De orde van 5 is 6 want $(5^2)^3 = 4^3 = 1$
6. De orde van 6 is 2 want $6^2 = 1$

De groep is commutatief want de vermenigvuldiging is commutatief.

## 2.6 Oefening 6

Bewijs dat elke deelgroep van een cyclische groep cyclisch is.

### Oplossingsmethode

Defintie van een cyclische groep zie def. 2.5 deel I blz 97.

### Oplossing

Opgelet, dit bewijs is niet correct/volledig.

*Bewijs.* Als $G$ een cyclische groep is dan bestaat er een generator $g$ zodat $G = \{g^0, g^1, g^2, \dots\}$

Als $H$ een deelgroep is van $G$ dan bevat $H$ dus minstens één element $g^k \in G$. Aangezien dat $H$ een groep is moet $H$ ook $\forall i \in \mathbb{N} : (g^k)^i$ bevatten, want een groep is overal bepaald.

$g^k$ is dus een generator voor $H$ en $H$ is dus een cyclische groep. $\square$

# 3 Oefenzitting 3

## 3.1 Oefening 1

Beschouw $\mathbb{Z}_{24} = \langle Z, +, . \rangle$.

(a) Ga na of $I = \{0, 3, 6, 9, 12, 15, 18, 21\}$ in deze ring een ideaal is.

(b) Is $I$ een prinicipaal ideaal ? Zo ja ga na welke elementen de generatoren zijn.

(c) Is $I$ een priemideaal ? Bepaal de quotiëntring $\mathbb{Z}_{24}|_I$

(d) Is $I$ een maximaal ideaal en zo ja, ga na dat de quotiëntring een veld is en bepaal de karakteristieken ervan.

(e) (extra) Bewijs dat elk ideaal in $\mathbb{Z}_n$ een principaal ideaal is (voor elke n).

**Oplossingsmethode**

In deel II blz. 6 vind je een voorbeeld dat bijna analoog is aan deze oefening.

(a) Gebruik defintie van een ring, zie deel I blz 114 en de def. van een ideaal zie deel I def. 4.1 blz 117.

(b) Principaal ideaal deel II blz 4.

(c) Een ideaal $\mathbb{D}$ in een ring $\mathbb{R}$ is een priemideaal als geldt (zie deel II blz. 6):

$$\forall a, b \in R \text{ en } ab \in D : a \in D \text{ of } b \in D.$$

Quotiëntring zie blz. 5 deel II en voorbeeld 2 blz. 6.

(d) Om na te gaan of een we een maximaal ideaal hebben gaan we na of de quotiëntring een veld is (stelling 7 deel II blz 9, def. van een veld zie blz 5).
Def. van de karakteristiek zie blz. 10 stelling 8. Gebruik stelling 9 blz 10 om de karakteristiek snel te vinden.

**Oplossing**

(a) We kijken eerst na of $I$ een ring is, het is duidelijk dat aan alle voorwaarden (zie deel I blz. 114) is voldaan om een ring te zijn.

$I$ bevat alle mogelijke veelvouden van 3 in $\mathbb{Z}_{24}$.
Het is duidelijk dat het aftrekken van twee veelvouden van 3 terug resulteert in een veelvoud van 3 (mod 24). Aangezien dat $I$ alle mogelijke veelvouden bevat is aan de eerste voorwaarden van een ideaal

al voldaan.
Ook het vermenigvuldigen van een veelvoud van 3 met een getal uit $\mathbb{Z}_{24}$ zal terug resulteren in een veelvoud van 3 (mod 24), ook aan de tweede voorwaarde is dus voldaan.
$I$ is dus een ideaal.

(b) $I$ is een principaal ideaal, waarbij de elementen $\{3, 9, 15, 21\}$ de generatoren zijn.

(c) Zoek dus voor elk element $x$ van I alle mogelijke a's en b's die een element zijn van $\mathbb{Z}_{24}$ zodat $a * b$ gelijk is aan $x$. Controleer vervolgens of a of b een element is van $I$.

Voor bijvoorbeeld $18 \in I$ vinden we

- $1, 18 \in \mathbb{Z}_{24}$ en $18 \in I$
- $1, 9 \in \mathbb{Z}_{24}$ en $9 \in I$
- $3, 6 \in \mathbb{Z}_{24}$ en $3 \in I$

Als je dit nakijkt voor elk element van $I$ zal je zien dat $I$ een priemideaal is.

De quotientring is dus $\{I, 1 + I, 2 + I\}$
$= \{\{0, 3, 6, 9, 12, 15, 18, 21\}, \{1, 4, 7, 10, 13, 16, 19, 22\}, \{2, 5, 8, 11, 14, 17, 20, 23\}\}$

(d) Om te kijken of de quotiëntring een veld is stellen we eerst de bewerkingstabel op, we gebruiken de volgende afkortingen:

$$I = \{0, 3, 6, 9, 12, 15, 18, 21\} \quad A = \{1, 4, 7, 10, 13, 16, 19, 22\}$$

$$B = \{2, 5, 8, 11, 14, 17, 20, 23\}$$

Dit geeft ons de volgende bewerkingstabel:

| . | $I$ | $A$ | $B$ |
|---|---|---|---|
| $I$ | $I$ | $I$ | $I$ |
| $A$ | $I$ | $A$ | $B$ |
| $B$ | $I$ | $B$ | $A$ |

Het is dus duidelijk dat $I$ het neutraal element is voor de optelling en dat $A$ het neutraal element is voor de vermigvuldiging.

In de tabel zien we ook dat elk van nul ($= I$) verschillend element een mulitplicatieve inverse heeft, voor $A$ is dit $A$ en voor $B$ is dit $B$.

Het is dus een veld en dus is $I$ een maximaal ideaal.

We weten al dat de karakteristiek van een eindig veld een priemgetal is (stelling 9 deel II blz. 10). We moeten dus opzoek gaan naar een priemgetal $\mu$ zodat $\mu A = I$ en $\mu B = I$.

Als we $\mu A$ doen dan vermenigvuldigen we elk element van $A$ met $\mu$ en moeten we uiteindelijk alle elementen van $I$ bekomen. Aangezien dat $A$ het element 1 bevat moet dus $\mu 1 = \mu \in I$. We moeten dus opzoek naar een priemgetal $\mu$ in $I$. Aangezien dat $I$ maar één priemgetal bevat, namelijk 3 moet $\mu$ dus gelijk zijn aan 3.
We zien nu dat $3 * A = I$ en $3 * B = I$.

De karakteristiek van $I$ is dus 3.

## 3.2 Oefening 2

Bepaal van de volgende uitbreidingsstructuren de kardinaliteit en de dimensie van de uitbreiding. Ga ook na of het velden zijn.

(a) $\mathbb{Q}(\sqrt[3]{2})$

(b) $\mathbb{Z}_5[x]|_{(x^2+1)}$

(c) $\mathbb{Z}_3[x]|_{(x^4+x^3+x-1)}$

(d) (extra) $\mathbb{Q}[x]|_{(x^3-5)}$

(e) (extra) $\mathbb{Z}_3[x]|_{(x^3-5)}$

**Oplossingsmethode**

Werkingsmethode voor uitbreiding van een veld zie cursus deel II blz 17.
De kardinaliteit is de het aantal elementen in een verzameling, zie deel II blz. 1.
Defintie van een veld is te vinden in deel II blz. 8. Om na te gaan of uitbreidingsstructuur een veld is gebruiken we meestal stelling 19 blz. 15 deel II.

**Oplossing**

(a) We zoeken eerst de veelterm $w(x) \in \mathbb{Q}$ zodat $w(\sqrt[3]{2}) = 0$.
Dit is dus de veelterm $x^3 - 2$.
$\mathbb{Q}(\sqrt[3]{2})$ is dus van de vorm $a + b\sqrt[3]{2} + c\sqrt[3]{2}^2$, waarbij $a, b, c \in \mathbb{Q}$.

Aangezien dat we voor zowel $a, b$ als $c$ eender welk element van $\mathbb{Q}$

mogen invullen zijn er dus $Q^3$ combinaties mogelijk en is dus de kardinaliteit van het uitbreidingsveld gelijk aan $|\mathbb{Q}|^3 = \infty$.
Aangezien dat $\mathbb{Q}(\sqrt[3]{2})$ van de vorm $a + b\sqrt[3]{2} + c\sqrt[3]{2}^2$ is, wat een tweede graadsveelterm is, is de dimensie van $\mathbb{Q}(\sqrt[3]{2})$ gelijk aan $2 + 1 = 3$.

Om een veld te kunnen zijn moet het een commutatieve ring zijn (def. zie blz. 3 deel II), het is eenvoudig na te gaan dat dit een commutatieve ring is.
We moeten nu enkel nog aantonen dat elk element een multiplicatieve inverse heeft. De uitwerking hiervan is nogal lang. Maar het komt erop neer dat je voor elk element van $x \in \mathbb{Q}(\sqrt[3]{2})$ een element $y \in \mathbb{Q}(\sqrt[3]{2})$ moet vinden zodat $xy = 1$.
Je moet dus $d, e$ en $f$ zoeken zodat voldaan is aan:

$$(a + b\sqrt[3]{2} + c\sqrt[3]{2}^2)(d + e\sqrt[3]{2} + f\sqrt[3]{2}^2) = 1$$

(b) $\mathbb{Z}_5[x]$ is de verzameling van veeltermen over $\mathbb{Z}_5$.
$\mathbb{Z}_5[x]|_{(x^2+1)}$ is de verzameling van nevenklassen die bij deling door $x^2 + 1$ dezelfde rest opleveren (zie deel II blz. 15), dit zijn dus alle veeltermen van de vorm $a + bx$ waarbij $a, b \in \mathbb{Z}_5$.

Gezien dat $a$ en $b$ allebei elementen zijn van $\mathbb{Z}_5$ en $\mathbb{Z}_5$ 5 elementen bevat, is het totaal aantal mogelijkheden dus gelijk aan $5^2 = 25$. De kardinaliteit van de uitbreiding is dus 25.

$a + bx$ is een veelterm van de eerste graad, de dimensie is dus gelijk aan $1 + 1 = 2$.

Nagaan of dit een veld is kunnen we nu eenvoudig met stelling 19 op blz. 15 van deel II.
We moeten dus enkel nagaan of $x^2 + 1$ irreduceerbaar is over $\mathbb{Z}_5$, met andere woorden moeten we dus nagaan of $x^2 + 1$ nulpunten heeft in $\mathbb{Z}_5$.
Dit is het geval, 2 en 3 zijn bijvoorbeeld nulpunten want $2^2 + 1 = 5 \bmod 5 = 0$ en $3^2 + 1 = 10 \bmod 5 = 0$.

(c) $\mathbb{Z}_3[x]|_{(x^4+x^3+x-1)}$ zijn dus alle veeltermen van de vorm $a+bx+cx^2+dx^3$ waarin dat $a, b, c, d \in \mathbb{Z}_3$.

$\mathbb{Z}_3$ bevat 3 elementen. Aangezien dat $a, b, c$ en $d$ elementen zijn van $\mathbb{Z}_3$ zijn er in totaal $4^3 = 81$ mogelijkheden. De kardinaliteit van $\mathbb{Z}_3[x]|_{(x^4+x^3+x-1)}$ is dus 81.

$a + bx + cx^2 + dx^3$ is een veelterm van graad 3, de dimensie is dus

$3 + 1 = 4$.

Nu kunnen we terug m.b.v. stelling 19 op blz. 15 bepalen of dat $\mathbb{Z}_3[x]|_{(x^4+x^3+x-1)}$ een veld is. We moeten dus nagaan of $x^4+x^3+x-1$ nulpunten heeft in $\mathbb{Z}_3$.

$$\begin{aligned} x = 0 \quad &\rightarrow \quad 0^4 + 0^3 + 0 - 1 = -1 \\ x = 1 \quad &\rightarrow \quad 1^4 + 1^3 + 1 - 1 = 2 \\ x = 2 \quad &\rightarrow \quad 2^4 + 2^3 + 2 - 1 = 25 \bmod 3 = 1 \end{aligned}$$

$x^4 + x^3 + x - 1$ heeft dus geen nulpunten in $\mathbb{Z}_3$, het kan dus niet gereduceerd worden naar het product van een eerstegraadsveelterm met een derdegraadsveelterm.
Nu moeten we nog nakijken of de veelterm niet kan worden gereduceerd naar een product van twee tweedegraadsveeltermen.
In $\mathbb{Z}_3$ zijn er drie irreduceerbare veeltermen van graad 2:

$$(x^2 + 1) \qquad (x^2 + x + 2) \qquad (x^2 + 2x + 2)$$

We zien nu dat $x^4 + x^3 + x - 1$ kan bekomen worden door het product van $(x^2 + 1)$ en $(x^2 + x + 2)$, de veelterm is dus niet irreduceerbaar, dus het is geen veld.

(d) $\mathbb{Q}[x]|_{(x^3-5)}$ zijn alle veeltermen van de vorm $a+bx+cx^2$ met $a, b, c \in \mathbb{Q}$

De kardinaliteit van $\mathbb{Q}[x]|_{(x^3-5)}$ is dus gelijk aan $|\mathbb{Q}|^3 = \infty$.

$a + bx + cx^2$ is een veelterm van de 2de graad, dus de dimensie is $2 + 1 = 3$.

We zoeken nu het nulpunt van $x^3 - 5$

$$\begin{aligned} & x^3 - 5 = 0 \\ \Leftrightarrow\, & x^3 = 5 \\ \Leftrightarrow\, & x = \sqrt[3]{5} \end{aligned}$$

Aangezien dat $\sqrt[3]{5} \notin \mathbb{Q}$ is $x^3 - 5$ dus irreduceerbaar over $\mathbb{Q}$ en dus is $\mathbb{Q}[x]|_{(x^3-5)}$ een veld.

(e) $\mathbb{Z}_3[x]|_{(x^3-2x+1)}$ zijn alle veeltermen van de vorm $a + bx + cx^2$ met $a, b, c \in \mathbb{Z}_3$

De kardinaliteit van $\mathbb{Z}_3[x]|_{(x^3-2x+1)}$ is dus gelijk aan $|\mathbb{Z}_3|^3 = 3^3 = 27$.

$a + bx + cx^2$ is een veelterm van de 2de graad, de dimensie is dus

$2 + 1 = 3$.

$x^3 - 2x + 1$ is niet irreduceerbaar over $\mathbb{Z}_3$ want 1 is een nulpunt, dus is $\mathbb{Z}_3[x]|_{(x^3-2x+1)}$ geen veld.

## 3.3 Oefening 3

Construeer een splitsingsveld van $w(x)$ over $\mathbb{F}$ en ontbind $w(x)$ hierover in lineaire factoren:

(a) $w(x) = (1 + x + x^2)$ over $\mathbb{F} = \mathbb{Z}_2$

(b) $w(x) = (1 + x^{16})(1 + x + x^2)$ over $\mathbb{F} = \mathbb{Z}_2$ (Gebruik stelling 22 p. 20)

(c) $w(x) = (x^5 + x^4 + x + 1)$ over $\mathbb{F} = \mathbb{Z}_3$

**Oplossingsmethode**

Algoritme en volledig annaloog voorbeeld te vinden in deel II blz. 19.

**Oplossing**

(a) We kijken eerst na of we geen nulpunten in $\mathbb{Z}_2$ vinden voor $1 + x + x^2$. Dit is niet het geval, aangezien dat het om een tweedegraadsveelterm gaat kunnen we dus besluiten dat $1 + x + x^2$ irreduceerbaar is in $\mathbb{Z}_2$.

We nemen nu $\gamma$ als nulpunt voor $1+x+x^2$, er geldt dus dat $1+\gamma+\gamma^2 = 0$.
Nu breiden we $\mathbb{Z}_2$ uit met $\gamma$, dit geeft onz $\mathbb{Z}_2(\gamma) = \{0, 1, \gamma, 1 + \gamma\}$.
Nu moeten we $w(x)$ nog ontbinden in factoren over $\mathbb{Z}_2(\gamma)$, aangezien dat $(x - \gamma)$ een nultpunt is van $w(x)$ is de levert de deling van $w(x)$ door $(x - \gamma)$ geen rest op.
Dit geeft ons de volgende staartdeling:

| | | | | |
|---|---|---|---|---|
| | $x^2$ | $x$ | $1$ | $(x-\gamma)$ |
| | $x^2$ | $x$ | | $x + (1 - \gamma)$ |
| - | $x^2$ | $-\gamma x$ | | |
| | | $(1-\gamma)x$ | $1$ | |
| | - | $(1-\gamma)x$ | $(\gamma - \gamma^2)$ | |
| | | | $0$ | |

$w(x) = 1 + x + x^2$ kunnen we dus ontbinden als $w(x) = 1 + x + x^2 = (x - \gamma)(x + 1 - \gamma) = (x - \gamma)(x - 1 + \gamma)$

(b) Om stelling 22 blz. 20 te mogen gebruiken moeten we eerst de karakteristiek van $\mathbb{Z}_2$ bepalen (zie blz. 10 deel II).

Aangezien dat:

$$2 * 1 = 2 = 0$$

Geldt dat de karakteristiek gelijk is aan 2. Aangezien dat $|\mathbb{Z}_2| = 2^1$ mogen we dus stelling 22 gebruiken.

Nu mogen we dus zeggen dat:

$$w(x) = (1 + x^{16})(1 + x + x^2) = (1 + x)^{16}(1 + x + x^2)$$

We moeten nu enkel nog $(1 + x + x^2)$ ontbinden. Aangezien we deze veelterm al hebben ontbonden in de vorige oefening gebruiken we dat resultaat hier opnieuw.
Zo krijgen we uiteindelijk:

$$w(x) = 1 + x + x^2 = (1 + x)^{16}(x - \gamma)(x - 1 + \gamma)$$

(c) We zoeken eerst naar nulpunten voor $x^5 + x^4 + x + 1$ in $\mathbb{Z}_3$, 2 is bijvoorbeeld zo'n nulpunt. Het resultaat van de deling van $x^5 + x^4 + x + 1$ door $(x - 2)$ kunnen we nu bepalen met het algoritme van Horner:

| | 1 | 1 | 0 | 0 | 1 | 1 |
|---|---|---|---|---|---|---|
| 2 | | 2 | 0 | 0 | 0 | 2 |
| | 1 | 0 | 0 | 0 | 1 | 0 |

We kunnen $w(x)$ dus ontbinden in:

$$w(x) = x^5 + x^4 + x + 1 = (x - 2)(x^4 - 1)$$

Nu moeten we $x^4 - 1$ verder ontbinden, aangezien dat deze veelterm geen nulpunten heeft in $\mathbb{Z}_3$, moeten we kijken of $x^4 - 1$ kan ontbonden worden in het product van twee tweedegraads veeltermen.

In $\mathbb{Z}_3$ zijn er drie irreduceerbare veeltermen van graad 2:

$$(x^2 + 1) \qquad (x^2 + x + 2) \qquad (x^2 + 2x + 2)$$

Zo vinden we dat :

$$x^4 - 1 = (x^2 + 2x + 2)(x^2 + x + 2)$$

Nu ontbinden we de veelterm $x^2 + x + 2$ verder, deze veelterm heeft geen nulpunten in $\mathbb{Z}_3$, daarom definiëren we $\alpha$ als nulpunt van deze veelterm, zodat:

$$\alpha^2 + \alpha + 2 = 0$$

Zo vinden we het volgende splitsingsveld:

$$\{[a\alpha + b] \mid a, b \in \mathbb{Z}_3\} = \{0, 1, 2, \alpha, \alpha + 1, \alpha + 2, 2\alpha, 2\alpha + 1, 2\alpha + 2\}$$

We kunnen nu $x^2 + x + 2$ verder ontbinden over dit veld:

$$x^2 + x + 2 = (x - \alpha)(x + \alpha + 1)$$

Nu moeten we enkel nog $x^2 + 2x + 2$ ontbinden, we kijken eerst of een element van ons splitsingsveld al een nulpunt is van deze veelterm:

$$\alpha^2 + 2 * \alpha + 2 = \alpha \neq 0$$

$$(\alpha + 1)^2 + 2 * (\alpha + 1) + 2 = \alpha = 0$$

$\alpha + 1$ is dus een nulpunt voor $x^2 + 2x + 2$ zo vinden we:

$$x^2 + 2x + 2 = (x - \alpha - 1)(x + \alpha) = (x + 2\alpha + 2)(x + \alpha)$$

De ontbinding van $w(x)$ is dus:

$$w(x) = x^5 + x^4 + x + 1 = (x + 1)(x + 2\alpha + 2)(x + \alpha)(x + 2\alpha)(x + \alpha + 1)$$

# 4 Oefenzitting 4

## 4.1 Oefening 1

Splits in irreduceerbare factoren over $\mathbb{Z}_3$:

(a) $x^5 + 2x^4 + x^3 + x^2 + 2$

(b) $x^7 + x^6 + x^5 - x^3 + x^2 - x - 1$

**Oplossingsmethode**

1. Kijk eerst of de veelterm nulpunten heeft in $\mathbb{Z}_3$.
2. Kijk of de veelterm (of de verkregen veeltermen) nog kunnen worden opgesplitst in irreduceerbare veeltermen van een lagere graad.

**Oplossing**

(a) We zoeken eerst de nulpunten in $\mathbb{Z}_3$ voor de gegeven veelterm, dit nulpunt zal gelijk zijn aan 2.
Met het algoritme van Horner doen we nu een eerste splitsing in factoren:

| | 1 | 2 | 1 | 1 | 0 | 2 |
|---|---|---|---|---|---|---|
| 2 | | 2 | 2 | 0 | 2 | 1 |
| | 1 | 1 | 0 | 1 | 2 | 0 |

Nu weten we dat:

$$x^5 + 2x^4 + x^3 + x^2 + 2 = (x - 2)(x^4 + x^3 + x + 2)$$

We proberen $(x^4 + x^3 + x + 2)$ nu nog verder te ontbinden.
Aangezien dat deze veelterm geen nulpunten heeft in $\mathbb{Z}_3$, moeten we kijken of we hem nog kunnen verder ontbinden in twee irreduceerbare veeltermen van de tweedegraad.
In $\mathbb{Z}_3$ zijn er drie irreduceerbare veeltermen van graad 2:

$$(x^2 + 1) \qquad (x^2 + x + 2) \qquad (x^2 + 2x + 2)$$

We zien nu dat $x^4 + x^3 + x - 1$ kan bekomen worden door het product van $(x^2 + 1)$ en $(x^2 + x + 2)$.
Nu is de reductie volledig, want alle bekomen veeltermen zijn irreduceerbaar:

$$x^5+2x^4+x^3+x^2+2 = (x-2)(x^4+x^3+x+2) = (x+1)(x^2+1)(x^2+x+2)$$

(b) Voor $x^7 + x^6 + x^5 - x^3 + x^2 - x - 1$ vinden we geen nulpunten in $\mathbb{Z}_3$.

We kijken nu of we de veelterm kunnen delen door één van de irreduceerbare veeltermen van de tweedegraad.

$$(x^2 + 1) \qquad (x^2 + x + 2) \qquad (x^2 + 2x + 2)$$

De veelterm kan inderdaad gedeeld worden door $(x^2 + 1)$ dit geeft:

$$x^7 + x^6 + x^5 - x^3 + x^2 - x - 1 = (x^2 + 1)(x^5 + x^4 + 2x^2 + 2x + 2)$$

$(x^5 + x^4 + 2x^2 + 2x + 2)$ heeft geen nulpunten in $\mathbb{Z}_3$, maar kan worden gedeeld door $(x^2 + 2x + 2)$.

Zo krijgen we uiteindelijk de irreduceerbare veelterm ontbinding:

$$x^7 + x^6 + x^5 - x^3 + x^2 - x - 1 = (x^2 + 1)(x^2 + 2x + 2)(x^3 + 2x^2 + 1)$$

## 4.2 Oefening 3

Zij $GF(4) = \{0, 1, \xi, \xi + 1\}$ met $\xi^2 + \xi + 1 = 0$.

(a) Bepaal alle monische veeltermen irreduceerbare veeltermen van graad twee over $GF(4)$.

(b) Contrueer $GF(4^2)$ uit $GF(4)$ m.b.v. de veelterm $x^2 + x\xi + \xi$.

(c) Bereken $\alpha^i$ voor $i = 0, 1, \ldots, 15$ met $\alpha^2 + \alpha\xi + \xi$.

(d) Bepaal de minimaalveeltermen van de elementen van $GF(4^2)$ over $GF(4)$.

(e) Bepaal de primitieve veeltermen van graad 2 over $GF(4)$.

**Oplossingsmethode**

Voorbeeld berekenen van de minimale veelterm zie voorbeeld 22 en 23 blz. 25-26 deel II.

De minimaalveelterm van een primitief element wordt een primitieve veelterm genoemd, zie def 13 blz. 24 deel II.

**Oplossing**

(a) We zoeken dus alle veeltermen van de vorm $x^2 + bx + c = 0$, die irreduceerbaar zijn dit zijn dus al de veeltermen van deze vorm die geen nulpunt hebben in $GF(4)$.
Om dit te doen stellen we de volgende tabel op:

| $c \backslash b$ | 0 | 1 | $\xi$ | $\xi + 1$ |
|---|---|---|---|---|
| 0 | × | × | × | × |
| 1 | × | × | | |
| $\xi$ | × | | | × |
| $\xi + 1$ | × | | × | |

Deze tabel stellen we op de volgende manier op:

Als $x = 0$ dan kan de veelterm $x^2 + bx + c = 0$ enkel nog gelijk zijn aan nul als $c = 0$. We zetten in de hele rij, voor $c = 0$ een kruisje in de tabel.

Als $x = 1$ dan is de veelterm van de vorm $1 + b + c = 0$ hieraan is voldaan als:

- $b = 1$ en $c = 0$
- $b = 0$ en $c = 1$
- $b = \xi$ en $c = \xi + 1$
- $b = \xi + 1$ en $c = \xi$

Al deze gevallen duiden we nu ook aan in de tabel met een kruisje.

Als $x = \xi$ dan is de veelterm van de vorm $\xi^2 + b\xi + c = 0$ wat gelijk is aan $\xi + 1 + b\xi + c = 0$ hieraan is voldaan als:

- $b = 0$ en $c = \xi + 1$
- $b = 1$ en $c = 1$
- $b = \xi$ en $c = 0$
- $b = \xi + 1$ en $c = \xi$

Ook deze gevallen duiden we nu ook aan in de tabel met een kruisje.

Als $x = \xi + 1$ dan is de veelterm van de vorm $(\xi + 1)^2 + b(\xi + 1) + c = 0$ wat gelijk is aan $\xi + b\xi + b + c = 0$ hieraan is voldaan als:

- $b = 0$ en $c = \xi$
- $b = 1$ en $c = 1$
- $b = \xi$ en $c = \xi + 1$
- $b = \xi + 1$ en $c = 0$

Ook deze gevallen duiden we nu ook aan in de tabel met een kruisje.

Alle combinaties voor waardes voor $b$ en $c$ die nog geen kruisje hebben in de tabel zijn nu de monische irreduceerbare veeltermen van graad twee over $GF(4)$.
Dit zijn dus:

$$(x^2+\xi x+1) \quad (x^2+(\xi+1)x+1) \quad (x^2+x+\xi) \quad (x^2+\xi x+\xi)$$

$$(x^2+x+\xi+1) \quad (x^2+(\xi+1)x+\xi+1)$$

(b) Volledig analoog voorbeeld is te vinden op blz. 24 deel II.

We nemen $\alpha$ als nulpunt voor de gegeven veelterm, zodat $\alpha^2+\alpha\xi+\xi = 0$.

Zo vinden we dan:

$$GF(4^2) = \{a\alpha + b | a, b \in GF(4)\}$$

(c) Als $\alpha^2+\alpha\xi+\xi$ dan geldt dat $\alpha^2 = \alpha\xi+\xi$.
We weten ook dat $\xi^2 = \xi+1$.

Nu bereken we alle $\alpha^i$:

$$\begin{array}{lcl}
\alpha & \rightarrow & \alpha \\
\alpha^2 & \rightarrow & \alpha\xi+\xi \\
\alpha^3 & \rightarrow & \alpha+\xi+1 \\
\alpha^4 & \rightarrow & \alpha+\xi \\
\alpha^5 & \rightarrow & \xi \\
\alpha^6 & \rightarrow & \alpha\xi \\
\alpha^7 & \rightarrow & \alpha\xi+\alpha+\xi+1 \\
\alpha^8 & \rightarrow & \alpha\xi+1 \\
\alpha^9 & \rightarrow & \alpha\xi+\xi+1 \\
\alpha^{10} & \rightarrow & \xi+1 \\
\alpha^{11} & \rightarrow & \alpha\xi+\alpha \\
\alpha^{12} & \rightarrow & \alpha+1 \\
\alpha^{13} & \rightarrow & \alpha\xi+\xi+\alpha \\
\alpha^{14} & \rightarrow & \alpha\xi+\alpha+1 \\
\alpha^{15} & \rightarrow & 1
\end{array}$$

(d) Om de minimale veelterm te bepalen moeten we eerst de cyclotomische

nevenklassen bepalen, dit geeft ons:

$$\begin{array}{lcl} C_0 & = & \{0\} \\ C_1 & = & \{1,4\} \\ C_2 & = & \{2,8\} \\ C_3 & = & \{3,12\} \\ C_4 & = & \{4,1\} \\ C_5 & = & \{5\} \\ C_6 & = & \{6,9\} \\ C_7 & = & \{7,13\} \\ C_8 & = & \{8,2\} \\ C_9 & = & \{9,6\} \\ C_{10} & = & \{10\} \\ C_{11} & = & \{11,14\} \end{array}$$

Hieruit kunnen we nu de volgende minimale veeltermen berekenen:

$$\begin{array}{lcll} C_0 & = & \{0\} & \rightarrow \quad m^{(0)} = (x-\alpha^0) = x+1 \\ C_1 & = & \{1,4\} & \rightarrow \quad m^{(1)} = (x-\alpha^1)(x-\alpha^4) = x^2+\xi x+\xi \\ C_2 & = & \{2,8\} & \rightarrow \quad m^{(2)} = (x-\alpha^2)(x-\alpha^8) = x^2+(1+\xi)x+\xi+1 \\ C_3 & = & \{3,12\} & \rightarrow \quad m^{(3)} = (x-\alpha^3)(x-\alpha^{12}) = x^2+\xi x+1 \\ C_4 & = & \{4,1\} & \rightarrow \quad m^{(4)} = m^{(1)} \\ C_5 & = & \{5\} & \rightarrow \quad m^{(5)} = (x-\alpha^5) = x+\xi \\ C_6 & = & \{6,9\} & \rightarrow \quad m^{(6)} = (x-\alpha^6)(x-\alpha^9) = x^2+(\xi+1)x+1 \\ C_7 & = & \{7,13\} & \rightarrow \quad m^{(7)} = (x-\alpha^7)(x-\alpha^{13}) = x^2+x+\xi \\ C_8 & = & \{8,2\} & \rightarrow \quad m^{(8)} = m^{(2)} \\ C_9 & = & \{9,6\} & \rightarrow \quad m^{(9)} = m^{(6)} \\ C_{10} & = & \{10\} & \rightarrow \quad m^{(10)} = (x-\alpha^{10}) = x+\xi+1 \\ C_{11} & = & \{11,14\} & \rightarrow \quad m^{(11)} = (x-\alpha^{11})(x-\alpha^{14}) = x^2+x+\xi+1 \end{array}$$

(e) In dit geval is $\alpha$ ons primitief element.

We geven twee voorbeelden:

- $m^{(6)}$ is geen primitieve veelterm want:

  $$m^{(6)} = (x-\alpha^6)(x-\alpha^9) = x^2-\alpha^6 x-\alpha^9-\alpha^{15}$$

  Aangezien dat $\alpha^{15}=1$ is deze veelterm dus niet opgebouwd uit enkel het primitief element en is deze veelterm dus geen primitieve veelterm.
- $m^{(2)}$ is wel een primitieve veelterm want:

  $$m^{(2)} = (x-\alpha^2)(x-\alpha^8) = x^2-\alpha^2 x-\alpha^8 x-\alpha^{10}$$

  Deze veelterm is dus duidelijk enkel opgebouwd uit het primitieve element.

We bekomen zo de volgende vier primitieve veeltermen:

- $x^2 + \xi x + \xi$
- $x^2 + (1 + \xi)x + \xi + 1$
- $x^2 + x + \xi$
- $x^2 + x + \xi + 1$

## 4.3 Oefening 4

Zij $GF(4) = \{0, 1, 2, \alpha, \alpha + 1, \alpha + 2, 2\alpha, 2\alpha + 1, 2\alpha + 2\}$ met $\alpha^2 = 1 - \alpha$.

(a) Ga na dat $x^2 + \alpha x + 1$ irreduceerbaar is over $GF(9)$.

(b) Construeer $GF(81)$ uit $GF(9)$ door uit te breiden met een nulpunt $\xi$ van deze veelterm.

**Oplossingsmethode**

Uitbreiding van een veld, zie voorbeeld 19 blz. 24.
Bekijk ook voorbeeld 15 blz. 17.

De multiplicatieve orde van een element $x$ is de kleinste positieve waarde $r$ zodat $x^r = 1$

**Oplossing**

(a) Aangezien dat $x^2 + \alpha x + 1$ een tweedegraadsveelterm is, is deze irreduceerbaar als de veelterm geen nulpunten heeft in $GF(9)$.
Welke waarde we uit $\{0, 1, 2, \alpha, \alpha + 1, \alpha + 2, 2\alpha, 2\alpha + 1, 2\alpha + 2\}$ ook invullen voor $x$ we verkijgen nooit 0.

(b) Aangezien dat $\xi$ een nulpunt is van $x^2 + \alpha x + 1$ geldt:

$$GF(81) = GF(9)|_{x^2+\alpha x+1} = \{a\xi + b | a, b \in GF(3)\}$$

(c) We verheffen $\xi$ tot we de macht $r$ vinden waarbij $\xi^r = 1$.

$$\begin{aligned}
\xi^1 &= \xi \\
\xi^2 &= \alpha\xi - 1 \\
\xi^3 &= -\alpha\xi - \alpha \\
\xi^4 &= \xi - \alpha \\
\xi^5 &= 2 \\
\xi^6 &= 2\xi \\
\xi^7 &= \alpha\xi + 1 \\
\xi^8 &= \alpha\xi - \alpha \\
\xi^9 &= \xi - \alpha \\
\xi^{10} &= 1
\end{aligned}$$

De multiplicatieve orde van $\xi$ is dus 10.

# 5 Oefenzitting 5

## 5.1 Oefening 1

Ontbind $x^n - 1$ in irreduceerbare factoren over $GF(q)$ voor:

(a) $(n, q) = (15, 4)$

(b) $(n, q) = (5, 4)$

(c) $(n, q) = (15, 3)$

**Oplossingsmethode**

1. Zoek de kleinste $k$ zodat $q^k \bmod n = 1$
2. Neem $\alpha$ het primitief element van $GF(q^k)$.
3. Neem $\beta = \alpha^{(q^k-1)/n}$
4. Bereken de cyclotomische nevenklassen modulo $n$ over $GF(q)$ (zie blz. 25).
5. Bepaal voor elke nevenklassen de minimaal veelterm
6. Het product van al deze minimale veeltermen is nu gelijk aan $x^n - 1$

**Oplossing**

(a) **Stap 1**

We zoeken $k$:

$$4^2 \bmod 15 = 1 \quad \Rightarrow \quad k = 2$$

**Stap 2**

Om de oefening eenvoudig te houden gebruiken we het resultaat van oefening 3.b van de vorige oefenzitting.

$\alpha$ is dus het nulpunt van de irreduceerbare veelterm $x^2 + x\xi + \xi$ uit $GF(4)$.

We gaan er voor deze oefening dus vannuit dat we $GF(2)$ al hebben uitgebreid tot $GF(4)$, waarbij dat $\xi$ het primitief element is van $GF(4)$.

**Stap 3**

Nu hebben we:

$$\beta = \alpha^1 = \alpha$$

**Stap 4**

We bepalen nu de cyclotomische nevenklassen modulo 15 over $GF(4)$:

$$\begin{array}{lcl} C_0 & = & \{0\} \\ C_1 & = & \{1,4\} \\ C_2 & = & \{2,8\} \\ C_3 & = & \{3,12\} \\ C_4 & = & \{4,1\} \\ C_5 & = & \{5\} \\ C_6 & = & \{6,9\} \\ C_7 & = & \{7,13\} \\ C_8 & = & \{8,2\} \\ C_9 & = & \{9,6\} \\ C_{10} & = & \{10\} \\ C_{11} & = & \{11,14\} \end{array}$$

**Stap 5**

Omdat $\beta = \alpha$ moeten we hier de $\beta$'s niet omzetten naar $\alpha$'s.

We bereken eerst alle $\alpha^i$'s:

$$\begin{array}{lcl} \alpha & \rightarrow & \alpha \\ \alpha^2 & \rightarrow & \alpha\xi + \xi \\ \alpha^3 & \rightarrow & \alpha + \xi + 1 \\ \alpha^4 & \rightarrow & \alpha + \xi \\ \alpha^5 & \rightarrow & \xi \\ \alpha^6 & \rightarrow & \alpha\xi \\ \alpha^7 & \rightarrow & \alpha\xi + \alpha + \xi + 1 \\ \alpha^8 & \rightarrow & \alpha\xi + 1 \\ \alpha^9 & \rightarrow & \alpha\xi + \xi + 1 \\ \alpha^{10} & \rightarrow & \xi + 1 \\ \alpha^{11} & \rightarrow & \alpha\xi + \alpha \\ \alpha^{12} & \rightarrow & \alpha + 1 \\ \alpha^{13} & \rightarrow & \alpha\xi + \xi + \alpha \\ \alpha^{14} & \rightarrow & \alpha\xi + \alpha + 1 \\ \alpha^{15} & \rightarrow & 1 \end{array}$$

We krijgen zo de volgende minimale veeltermen:

$$\begin{array}{lcll}
C_0 & = & \{0\} & \rightarrow \quad m^{(0)} = (x-\alpha^0) = x+1 \\
C_1 & = & \{1,4\} & \rightarrow \quad m^{(1)} = (x-\alpha^1)(x-\alpha^4) = x^2+\xi x+\xi \\
C_2 & = & \{2,8\} & \rightarrow \quad m^{(2)} = (x-\alpha^2)(x-\alpha^8) = x^2+(1+\xi)x+\xi+1 \\
C_3 & = & \{3,12\} & \rightarrow \quad m^{(3)} = (x-\alpha^3)(x-\alpha^{12}) = x^2+\xi x+1 \\
C_4 & = & \{4,1\} & \rightarrow \quad m^{(4)} = m^{(1)} \\
C_5 & = & \{5\} & \rightarrow \quad m^{(5)} = (x-\alpha^5) = x+\xi \\
C_6 & = & \{6,9\} & \rightarrow \quad m^{(6)} = (x-\alpha^6)(x-\alpha^9) = x^2+(\xi+1)x+1 \\
C_7 & = & \{7,13\} & \rightarrow \quad m^{(7)} = (x-\alpha^7)(x-\alpha^{13}) = x^2+x+\xi \\
C_8 & = & \{8,2\} & \rightarrow \quad m^{(8)} = m^{(2)} \\
C_9 & = & \{9,6\} & \rightarrow \quad m^{(9)} = m^{(6)} \\
C_{10} & = & \{10\} & \rightarrow \quad m^{(10)} = (x-\alpha^{10}) = x+\xi+1 \\
C_{11} & = & \{11,14\} & \rightarrow \quad m^{(11)} = (x-\alpha^{11})(x-\alpha^{14}) = x^2+x+\xi+1
\end{array}$$

**Stap 6**

Onze veelterm is nu ontbonden.

$x^{15}-1 = (x+1)(x^2+\xi x+\xi)(x^2+(1+\xi)x+\xi+1)(x^2+\xi x+1)(x+\xi)(x^2+(\xi+1)x+1)(x^2+x+\xi)(x^2+x+\xi)(x+\xi+1)(x^2+x+\xi+1)$

(b) **Stap 1**

We zoeken $k$:

$$4^2 \bmod 5 = 1 \quad \Rightarrow \quad k = 2$$

**Stap 2**

Aangezien dat $GF(4)$ al een uitbreiding is van $GF(2)$ moeten we dit schrijven als $GF(4^2) = GF(16) = GF(2^4)$.
We vinden nu de volgende irreduceerbare veelterm van de 4de graad over $GF(2)$ (zie tabel blz. 27):

$$x^4+x+1$$

Nu nemen we $\alpha$ als nulpunt van deze veelterm zodat:

$$\alpha^4+\alpha+1 = 0 \quad \Rightarrow \quad \alpha^4 = \alpha+1$$

$\alpha$ is nu het primitief element van $GF(4^2) = GF(2^4)$.

**Stap 3**

We berekenen hieruit nu $\beta$:

$$\beta = \alpha^{(4^2-1)/5} = \alpha^3$$

**Stap 4**

We bepalen nu de cyclotomische nevenklassen modulo 5 over $GF(4)$:

$$\begin{array}{lcl} C_0 & = & \{0\} \\ C_1 & = & \{1,4\} \\ C_2 & = & \{2,3\} \end{array}$$

**Stap 5**

Gebruikmakende van $\beta = \alpha^3$ en $\alpha^4 = \alpha + 1$ , bepalen we nu alle $B^i$'s:

$$\begin{array}{lcl} \beta^1 & = & \alpha^3 \\ \beta^2 & = & \alpha^3 + \alpha^2 \\ \beta^3 & = & \alpha^3 + \alpha \\ \beta^4 & = & \alpha^3 + \alpha^2 + \alpha + 1 \\ \beta^5 & = & 1 \end{array}$$

Hiermee berekenen we nu de minimaalveeltermen:

$$\begin{array}{lcll} m^{(0)} & = & (x-\beta^0) & = & x+1 \\ m^{(1)} & = & (x-\beta^1)(x-\beta^4) & = & x^2 + (\alpha^2+\alpha+1)x + 1 \\ m^{(2)} & = & (x-\beta^2)(x-\beta^3) & = & x^2 + (\alpha^2+\alpha)x + 1 \end{array}$$

**Stap 6**

We verkijgen nu de volgende ontbonden veelterm:

$$x^5 - 1 = (x+1)(x^2 + (\alpha^2+\alpha+1)x + 1)(x^2 + (\alpha^2+\alpha)x + 1)$$

(c) **Stap 1**

We zoeken eerst een $k$ zodat $3^k \bmod 15 = 1$. Maar aangezien dat 15 een veelvoud is van 3 zullen we geen $k$ vinden die voldoet aan deze voorwaarden.

Om dit op te lossen passen we stelling 22 op blz. 20 toe, deze stelling mogen we toepassen omdat een Galoisveld voldoet aan de benodigde voorwaarden.
Zo verkrijgen we:

$$x^{15} - 1 = x^{15} + (-1)^{15} = (x^5 - 1^5)^3 = (x^5 - 1)^3$$

We kunnen nu $(x^5 - 1)$ factoriseren en het resultaat verheffen tot de derde macht.

We bepalen nu $k$ voor $(x^5 - 1)$:

$$3^4 \bmod 5 = 1 \quad \Rightarrow \quad k = 4$$

**Stap 2**

We bepalen nu $\alpha$ als nulpunt van de veelterm $x^4 + x + 2$, dit is een irreduceerbare veelterm van de vierde graad van $GF(3)$.

**Stap 3**

We berekenen hieruit nu $\beta$:

$$\beta = \alpha^{(3^4-1)/5} = \alpha^{16}$$

**Stap 4**

We bepalen nu de cyclotomische nevenklassen modulo 5 over $GF(3)$:

$$\begin{array}{lcl} C_0 & = & \{0\} \\ C_1 & = & \{1, 3, 4, 2\} \end{array}$$

**Stap 5**

Omdat er maar twee cyclotomische nevenklassen zijn, kunnen we dit eenvoudiger oplossen zonder de minimaalveeltermen te berekenen.

We bereken enkel de eerste minimaalveelterm (deze is toch super eenvoudig):

$$m^{(0)} = x - \beta^0 = x - 1$$

**Stap 6**

We weten dat de factorisatie gelijk is aan het product van de minimaalveeltermen:

$$x^5 - 1 = m^{(0)} * m^{(1)} = (x - 1) * m^{(1)}$$

We kunnen nu de tweede minimaalveelterm berekenen m.b.v. Horner, zo krijgen we uiteindelijk:

$$x^5 - 1 = (x + 2)(x^4 + 2x^3 + x^2 + 2x + 1)$$

Wanneer we nu alles verheffen tot de derde macht verkrijgen we:

$$x^{15} - 1 = (x + 2)^3(x^4 + 2x^3 + x^2 + 2x + 1)^3$$

## 5.2 Oefening 2

Bepaal de graad van alle irreduceerbare factoren van $x^{17} - 1$ over $GF(2)$.

### Oplossingsmethode

Om de graad van alle irreduceerbare factoren te bepalen moeten we enkel de cyclotomische nevenklassen bepalen (zie voorbeeld 22 blz. 25), daaruit kunnen de graden van de factoren onmiddellijk aflezen.

### Oplossing

We bepalen de cyclotomische nevenklassen modulo 17 over GF(2):

$$\begin{aligned} C_0 &= \{0\} \\ C_1 &= \{1, 2, 4, 8, 16, 15, 13, 9\} \\ C_3 &= \{3, 6, 12, 7, 14, 11, 5, 10\} \end{aligned}$$

$C_0$ heeft één element $\Rightarrow$ minimaalveelterm van graad 1.
$C_1$ heeft acht elementen $\Rightarrow$ minimaalveelterm van graad 8.
$C_3$ heeft acht elementen $\Rightarrow$ minimaalveelterm van graad 8.

## 5.3 Oefening 3

Gegeven een $(n, k)$ lineaire blokcode $\mathbb{C}$ over $GF(2)$:

$$\mathbb{C} = \{000000, 000111, 011001, 011110, 101011, 101100, 110010, 110101\}$$

(a) Is deze code wel een blokcode?

(b) Is deze code wel lineair?

(c) Wat is $n$? Wat is $k$?

(d) Construeer een generatormatrix $G$ voor deze code. Codeer enkele informatiewoorden.

(e) Ga over op een equivalente code met een generatormatrix $\tilde{G}$ in standaardvorm.

(f) Bepaal de pariteitstestmatrix $\tilde{H}$ van die equivalente code.

(g) Bepaal de pariteitstestmatrix $H$ van de oorspronkelijke code.

(h) Hoeveel fouten kan men detecteren? Hoeveel fouten kan men verbeteren?

(i) Vervolledig de decoderingstabel voor deze code?

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 000000 | 000111 | 011001 | 011110 | 101011 | 101100 | 110010 | 110101 |
| 100000 | 100111 | 111001 | 111110 | 001011 | 001100 | 010010 | 010101 |
| 010000 | 010111 | 001001 | 001110 | 111011 | 111100 | 100010 | 100101 |
| 001000 | 001111 | 010001 | 010110 | 100011 | 100100 | 111010 | 111101 |
| 000100 | 000011 | 011101 | 011010 | 101111 | 101000 | 110110 | 110001 |
| 000010 | 000101 | 011011 | 011100 | 101001 | 101110 | 110000 | 110111 |

(j) De syndroomtabel maak je door het syndroom van de vertegenwoordigers van de nevenklassen in een tabel te steken.
Zie voorbeeld 47 blz. 46.

(k) Je ontvangt 110011. Wat is de gedecodeerde boodschap?

(l) Is deze code perfect?

**Oplossingsmethode**

(a) Defintie van blokcode blz. 33

(b) Defintie en gevolg van een lineaire blokcode zie blz. 39.

(c) $n$ is de lengte van het code woord.
$k$ is de grootte van de basis of de lengte van het informatiewoord.

(d) Theorie blz. 39-40 en voorbeeld 41 blz. 40.

(e) We zetten m.b.v. rij-operaties en kolompermutaties de matrix $G$ om naar een matrix van de vorm $[I|P]$, zie blz. 43 bovenaan.

(f) De pariteitstestmatrix $\tilde{H} = [-P^T|I]$, zie blz. 43 bovenaan.

(g) We kunnen de matrix $H$ bekomen uit de matrix $\tilde{H}$ door de permutaties die we hebben doorgevoerd op $G$ omgekeerd uit te voeren op $\tilde{H}$.
Zie voorbeeld 45 blz. 43.

(h) Een lineaire code kan $d-1$ fouten detecteren, zie gevolg 5 blz. 37.
Het aantal fouten dat je kan verbeteren is $(d-1)/2$, zie blz. 39.

(i) Zie voorbeeld 46 blz. 44.

(j) Zie voorbeeld 46 blz. 44

(k) Je ontvangt 110011. Wat is de gedecodeerde boodschap?

(l) Theorie zie blz. 49.
Voorbeeld zie voorbeeld 51 blz. 49.

**Oplossing**

(a) Dit is een blokcode want elk woord heeft dezelfde lengte.

(b) Deze code is lineair want de som en het verschil van twee codewoorden is terug een codewoord.
De code bevat ook het nulcodewoord.

(c) $n$ is de lengte van het codewoord, dus $n = 3$.
Om $k$ te bepalen, moeten we eerst uit de gegevens codewoorden een basis vormen.
Een voorbeeld van zo'n basis is :

$$b_1 = 000111 \quad b_2 = 011001 \quad b_3 = 101011$$

$k$ is nu gelijk aan de dimensie van de basis $k = 3$.

(d) De generatormatrix kunnen we construeren door een matrix te maken waarin dat de rijen achtereenvolgens $b_1, b_2, b_3$ zijn.

$$G = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

We coderen bijvoorbeeld 011110:

$$011110 = 1 * b_1 + 1 * b_2 = 110$$

We gaan na dat dit juist is:

$$\begin{bmatrix} 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} = 011110$$

(e) Om dit te doen voeren we de volgende kolompermutaties uit op de matrix $G$:

- Verwissel kolom 1 en 3
- Verwissel daarna kolom 1 en 4

We hebben nu de matrix $\tilde{G}$:

$$\tilde{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

(f) Aan de hand van de matrix $\tilde{G}$ bepalen we nu de matrix $\tilde{H}$:

$$\tilde{H} = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

(g) We voeren de volgende permutaties uit op $\tilde{H}$:

- Verwissel kolom 1 en 4
- Verwissel daarna kolom 1 en 3

Dit geeft ons de volgende matrix:

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

(h) De afstand van deze code is gelijk aan $d = 3$.

Het aantal fouten dat je kan detecteren is dus $s = 3 - 1 = 2$.
Het aantal fouten dat je kan verbeteren is dus $t = (3 - 1)/2 = 1$.

(i) In $GF(2)$ kunnen we $2^6$ verschillende codes maken van lengte 6. De decodeertabel moet al deze codes bevatten. We moeten dus nog 16 codes, oftewel 2 rijen met codes toevoegen.

De huidige tabel bevat bijvoorbeeld de codes 000001 en 100001 nog niet, we voegen de nevenklassen waartoe deze behoren nog toe:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 000000 | 000111 | 011001 | 011110 | 101011 | 101100 | 110010 | 110101 |
| 100000 | 100111 | 111001 | 111110 | 001011 | 001100 | 010010 | 010101 |
| 010000 | 010111 | 001001 | 001110 | 111011 | 111100 | 100010 | 100101 |
| 001000 | 001111 | 010001 | 010110 | 100011 | 100100 | 111010 | 111101 |
| 000100 | 000011 | 011101 | 011010 | 101111 | 101000 | 110110 | 110001 |
| 000010 | 000101 | 011011 | 011100 | 101001 | 101110 | 110000 | 110111 |
| 000001 | 000110 | 011000 | 011111 | 101010 | 101101 | 110011 | 110100 |
| 100001 | 100110 | 111000 | 111111 | 001010 | 001101 | 010011 | 010100 |

(j) We verkrijgen de volgende syndroomtabel:

| vertegenwoordiger | syndroom |
|---|---|
| 000000 | 000 |
| 100000 | 111 |
| 010000 | 101 |
| 001000 | 100 |
| 000100 | 011 |
| 000010 | 010 |
| 000001 | 001 |
| 100001 | 110 |

(k) Hiervoor bereken we eerst het syndroom voor $v$:

$$s = vH^T$$

$$\begin{bmatrix}1 & 1 & 0 & 0 & 1 & 1\end{bmatrix} \begin{bmatrix}1 & 1 & 1 & 0 & 0 & 0\\ 1 & 0 & 0 & 1 & 1 & 0\\ 1 & 1 & 0 & 1 & 0 & 1\end{bmatrix} = \begin{bmatrix}0 & 0 & 1\end{bmatrix}$$

Aangezien dat $s = 001$ vinden we in de syndroomtabel dat $e = 000001$. Zo vinden we:

$$c = v - e = 110011 - 000001 = 110010$$

(l) We bereken eerst $r_p$:

| c | $S_c(0)$ |
|---|---|
| 000000 | {000000} |
| 000111 | {000111} |
| 011001 | {011001} |
| 011110 | {011110} |
| 101011 | {101011} |
| 101100 | {101100} |
| 110010 | {110010} |
| 110101 | {110101} |

| c | $S_c(1)$ |
|---|---|
| 000000 | {000000, 000001, 000010, 000100, 001000, 010000, 100000} |
| 000111 | {000111, 000110, 000101, 000011, 001111, 010111, 100111} |
| 011001 | {011001, 011000, 011011, 011101, 010001, 001001, 111001} |
| 011110 | {011110, 011111, 011100, 011010, 010110, 001110, 111110} |
| 101011 | {101011, 101010, 101001, 101111, 100011, 111011, 001011} |
| 101100 | {101100, 101101, 101110, 101000, 100100, 111100, 001100} |
| 110010 | {110010, 110011, 110000, 110110, 111010, 100010, 010010} |
| 110101 | {110101, 110100, 110111, 110001, 111101, 100101, 010101} |

$r_p$ is duidelijk gelijk aan 1 want als we 100010 en 100100 allebei nog één bit laten afwijken dan zijn ze gelijk aan elkaar.

In $GF(2)$ kunnen we $2^6 = 64$ verschillende codes maken van lengte 6, in de tabel voor $S_c(1)$ staan er $7 * 8 = 56$. We zullen dus pas bij $S_c(2)$ alle mogelijke combinaties bekomen (en veel dubbels).
We weten nu dus dat $r_d = 2$.

Het is dus een quasi-perfecte code want $r_d = r_p + 1$.

# 6 Oefenzitting 6

## 6.1 Oefening 1

$(9, 7)$ Hamming code over GF(8).
$\alpha$ primitief element van $GF(8)$, nulpunt van $x^3 + x + 1$.

$\alpha^0 = 1 = [100]$
$\alpha^1 = \alpha = [010]$
$\alpha^2 = \alpha^2 = [001]$
$\alpha^3 = 1 + \alpha = [110]$
$\alpha^4 = \alpha + \alpha^2 = [011]$
$\alpha^5 = 1 + \alpha + \alpha^2 = [111]$
$\alpha^6 = 1 + \alpha^2 = [101]$
$(\alpha^7 = 1 = [100])$

Een generatormatrix en bijhorende pariteitsmatrix van de $(9, 7)$ Hamming code over $GF(8)$ zijn:

$$G = \begin{bmatrix} \alpha^5 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ \alpha^6 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ \alpha & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ \alpha^2 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ \alpha^3 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ \alpha^4 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

$$H = \begin{bmatrix} 1 & 0 & 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

(a) Hoeveel codewoorden zijn er in de code?

(b) Welke dimensies heeft de decoderingstabel?

(c) Welke dimensies heeft de syndroomtabel?

(d) Codeer een zelfgekozen informatiewoord.

(e) Bereken voor het onder (d) bekomen codewoord $c$ : $cH^T$.

(f) Zet op het codewoord $c$ één fout en bereken voor dit ontvangen woord $v$ het syndroom $s$.

(g) Hoe kan men, zonder gebruik te maken van de syndroomtabel uit $s$ en $v$ het correcte codewoord terugvinden.

**Oplossingsmethode**

(a) Het aantal codewoorden is $q^k$.

(b) De decodeertabel heeft evenveel kolommen als het aantal codewoorden $q^k$.
Daarnaast bevat de decodeertabel alle mogelijke codes $q^n$, het aantal rijen is dus $q^n/q^k$.

(c) De syndroomtabel heeft steeds 2 kolommen en het aantal rijen is steeds gelijk aan het aantal rijen van de decodeertabel $q^n/q^k$.

(d) Een informatie woord $i$ kan gecodeerd worden door $c = iG$ te doen.
Zie voorbeeld 48 blz. 47.

(e) Bij het berekenen van $c : cH^T$, bereken we eigenlijk het syndroom van $c$, hieruit kunnen we dan de fout afleiden en die fout terug aftrekken van $c$, maar als we $c$ correct hebben gecodeerd, dan zit er geen fout op $c$ en zal dus $cH^T = \begin{bmatrix}0 & 0\end{bmatrix}$.

(f) Zie voorbeeld 48 blz. 47.

(g) Zie voorbeeld 48 blz. 47.

**Oplossing**

(a) Er zijn hier dus $8^7$ codewoorden.

(b) De decodeertabel heeft $8^7$ kolommen en $8^9/8^7 = 8^2$ rijen.

(c) De syndroomtabel heeft dus $8^2$ rijen en 2 kolommen.

(d) We coderen:

$$i = \begin{bmatrix}001 & 111 & 101 & 100 & 011 & 100 & 110\end{bmatrix}$$

Doormiddel van de gegeven tabel voor $\alpha^i$'s te gebruiken weten we dat dit gelijk is aan:

$$i = \begin{bmatrix}\alpha^2 & \alpha^5 & \alpha^6 & 1 & \alpha^4 & 1 & \alpha^3\end{bmatrix}$$

Nu bereken we $c$, we gebruiken ook hier de tabel om alles terug om te zetten naar iets van de vorm $\alpha^i$ :

$$c = iG = \begin{bmatrix}\alpha^5 & \alpha^3 & \alpha^6 & 1 & \alpha^4 & 1 & \alpha^3 & \alpha^2 & \alpha^5\end{bmatrix}$$

(e) We berekenen het syndroom voor $c$:

$$cH^T = \begin{bmatrix}0 & 0\end{bmatrix}$$

Zoals verwacht zit er dus geen fout op $c$, de codering is dus juist verlopen.

(f) We zetten op $c$ de volgende fout:

$$e = \begin{bmatrix} 0 & 0 & \alpha^1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Het ontvangen woord $v$ is nu gelijk aan $c$ plus de fout $e$:

$$v = c + e = \begin{bmatrix} \alpha^5 & \alpha^3 & \alpha^5 & 1 & \alpha^4 & 1 & \alpha^3 & \alpha^2 & \alpha^5 \end{bmatrix}$$

want

$$\alpha^6 + \alpha = \alpha^2 + 1 + \alpha = \alpha^5$$

Nu bereken we het syndroom van $v$:

$$s = vH^T = \begin{bmatrix} \alpha & \alpha \end{bmatrix} = \alpha \text{ keer de derde kolom van } H$$

(g) We kunnen $\begin{bmatrix} \alpha & \alpha \end{bmatrix}$ dus bekomen uit $H$ door:

$$\begin{bmatrix} \alpha & \alpha \end{bmatrix} = \begin{bmatrix} 0 & 0 & \alpha & 0 & 0 & 0 & 0 \end{bmatrix} * H^T$$

Nu weten we dat:

$$e = \begin{bmatrix} 0 & 0 & \alpha & 0 & 0 & 0 & 0 \end{bmatrix}$$

Wat dus gelijk is aan de fout die we op $c$ hadden gezet.

Door deze fout terug af te trekken van $v$ bekomen we $c$ terug.

$$c = v - e = \begin{bmatrix} \alpha^5 & \alpha^3 & \alpha^6 & 1 & \alpha^4 & 1 & \alpha^3 & \alpha^2 & \alpha^5 \end{bmatrix}$$

## 6.2 Oefening 2

(a) Bepaal de generatorveelterm van een BCH-code van lengte $n = 12$ over $GF(7)$ die $t = 2$ fouten kan verbeteren. Kies hierbij $l$ de kleinste waarde in $\mathbb{N}_0$ die de dimensie van de code maximaal maakt.

(b) Decodeer met behulp van het PGZ(=Peterson-Gorenstein-Zierler)-algoritme het ontvangen woord $v(x) = 2x + 5x^2 + 6x^4 + x^4 + 4x^5$.

### Oplossingsmethode

(a) Om dit op te lossen moeten we eerst $x^n - 1$ factoriseren over $GF(q)$. Dit doen we volgens dezefde stappen als in de vorige oefenzitting. De dimensie van een code is de lengte van het informatiewoord $i$ (zie blz. 40), we weten ook dat $c = iG$, de dimensie van het informatie woord is dus maximaal als de graad van $G$ minimaal is.
Zie ook voorbeeld 57 blz. 58.

(b) Zie algoritme op blz. 64. Volledig analoog voorbeeld op blz. 65.

**Oplossing**

(a) We factoriseren eerst $x^12 - 1$ over $GF(7)$.

**1)** $7^k \bmod 12 = 1 \Rightarrow k = 7$.
**2)** $\alpha$ is primitief element van $GF(7^2)$ met $\alpha^2 = 6\alpha + 4$.
**3)** $\beta = \alpha^4$.

Hiermee berekenen we:

$$\begin{array}{lcllcl} \beta^1 &=& 5\alpha + 6 & \beta^7 &=& 2\alpha + 1 \\ \beta^2 &=& 3 & \beta^8 &=& 4 \\ \beta^3 &=& \alpha + 4 & \beta^9 &=& 6\alpha + 3 \\ \beta^4 &=& 2 & \beta^{10} &=& 5 \\ \beta^5 &=& 3\alpha + 5 & \beta^{11} &=& 4\alpha + 2 \\ \beta^6 &=& 6 & \beta^{12} &=& 1 \end{array}$$

**4)** We bepalen de nevenklassen module 12 in $GF(7)$:

$$\begin{array}{lcllcl} C_0 &=& \{0\} & C_5 &=& \{5,11\} \\ C_1 &=& \{1,7\} & C_6 &=& \{6\} \\ C_2 &=& \{2\} & C_8 &=& \{8\} \\ C_3 &=& \{3,9\} & C_{10} &=& \{10\} \\ C_4 &=& \{4\} & & & \end{array}$$

**5)** We bepalen minimaalveeltermen:

$$\begin{array}{lcllcl} m^{(0)} &=& (x - \beta^0) = x + 6 & m^{(5)} &=& (x - \beta^5)(x - \beta^1 1) = x^2 + 2 \\ m^{(1)} &=& (x - \beta^1)(x - \beta^7) = x^2 + 4 & m^{(6)} &=& (x - \beta^6) = x + 1 \\ m^{(2)} &=& (x - \beta^2) = x + 4 & m^{(8)} &=& (x - \beta^8) = x + 3 \\ m^{(3)} &=& (x - \beta^3)(x - \beta^9) = x^2 + 1 & m^{(10)} &=& (x - \beta^{10}) = x + 2 \\ m^{(4)} &=& (x - \beta^4) = x + 5 & & & \end{array}$$

Nu moeten we enkel nog een vier opeenvolgende $\beta^i$'s kiezen, zodat de graad van het product van de bijhorende minimaal veeltermen minimaal is.

We kiezen $\beta^1, \beta^2, \beta^3, \beta^4$, waarbij $l = 1$ ook minimaal is in $\mathbb{N}_0$, het product van de bijhorende minimaal veeltermen is nu $g(x)$:

$$g(x) = (x^2 + 4)(x + 4)(x^2 + 1)(x + 5)$$

(b) We vullen eerst alle nulpunten van $g(x)$ in in $v(x)$, dit geeft ons:

$$\begin{array}{lcl} S_1 = v(\beta^1) = 3 \\ S_2 = v(\beta^2) = 6 \\ S_3 = v(\beta^3) = 3 \\ S_4 = v(\beta^4) = 6 \end{array}$$

We stellen $\nu = 2$, dit geeft ons:

$$H^{(2)} = \begin{bmatrix} 3 & 6 \\ 6 & 3 \end{bmatrix}$$

det(H) $\neq 0$, dus $\nu$ is inderdaad gelijk aan 2.

Nu krijgen we het volgende stelsel:

$$\begin{bmatrix} 3 & 6 \\ 6 & 3 \end{bmatrix} \begin{bmatrix} \Lambda_0 \\ \Lambda_1 \end{bmatrix} = - \begin{bmatrix} 3 \\ 6 \end{bmatrix} = \begin{bmatrix} 4 \\ 1 \end{bmatrix}$$

Als we dit oplossen vinden we dat $\Lambda_0 = 6$ en $\Lambda_1 = 0$.

Dit geeft ons dan weer:

$$\Lambda(x) = \Lambda_0 + \Lambda_1 x + x^2 = 6 + x^2.$$

De nulpunten van deze veelterm (in $GF(7)$) zijn, $X_1 = 1 = \beta^0$ en $X_2 = 6 = \beta^6$.

Hiermee kunnen we dan weer het volgende stelsel opstellen:

$$\begin{bmatrix} 1 & 6 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} Y_1 \\ Y_2 \end{bmatrix} = \begin{bmatrix} 3 \\ 6 \end{bmatrix}$$

Als we dit oplossen vinden we dat $Y_1 = 1$ en $Y_2 = 5$.

Dit geeft ons dan:

$$e(x) = 100000500000$$

Uitendelijk bekomen we dan:

$$c(x) = v(x) - e(x) = 025614000000 - 100005000000 = 625614200000$$

## 6.3 Oefening 3

Beschouw een BCH-code van lengte $n = 5$ over $GF(4)$ die $t = 1$ fouten kan verbeteren. Kies hierbij $l$ de kleinste waarde in $\mathbb{N}_0$ die e dimensie van de code maximaal maakt. Decodeer het ontvangen woord $v =$ 10 11 11 11 01 met het PGZ algoritme.

$GF(4)$ als uitbreiding van $GF(2)$
Primitief element: $\eta$: nulpunt van $x^2 + x + 1$ over $GF(2)$.
$\eta^2 + \eta + 1 = 0 \rightarrow \eta^2 = 1 + \eta$
$\eta^0 = 1 \quad \eta^1 = \eta \quad \eta^2 = 1 + \eta \quad (\eta^3 = 1)$
$GF(16)$ als uitbreiding van $GF(4)$
Primitief element: $\alpha$: nulpunt van $x^2 + \eta x + \eta$ over $GF(4)$.
$\alpha^2 + \eta\alpha + \eta = 0 \rightarrow \alpha^2 = \eta + \eta\alpha$

| | | |
|---|---|---|
| $\alpha^0 = 1$ | $\alpha^5 = \eta$ | $\alpha^{10} = \eta^2$ |
| $\alpha^1 = \alpha$ | $\alpha^6 = \eta\alpha$ | $\alpha^{11} = \eta^2\alpha$ |
| $\alpha^2 = \eta + \eta\alpha$ | $\alpha^7 = \eta^2 + \eta^2\alpha$ | $\alpha^{12} = 1 + \alpha$ |
| $\alpha^3 = \eta^2 + \alpha$ | $\alpha^8 = 1 + \eta\alpha$ | $\alpha^{13} = \eta + \eta^2\alpha$ |
| $\alpha^4 = \eta + \alpha$ | $\alpha^9 = \eta^2 + \eta\alpha$ | $\alpha^{14} = 1 + \eta^2\alpha$ |

**Oplossingsmethode**

Volledig analoog aan de vorige oefening.

**Oplossing**

We factoriseren eerst $x^5 - 1$ over $GF(4)$.

**1)** $4^k \bmod 5 = 1 \Rightarrow k = 2$.
**2)** Gegeven is dat $\alpha$ het primitief element is van $GF(4^2)$ met $\alpha^2 = \eta + \eta\alpha$.
**3)** $\beta = \alpha^3$.

Hiermee berekenen we:

$$\begin{aligned} \beta^1 &= \alpha + \eta + 1 \\ \beta^2 &= \alpha\eta \\ \beta^3 &= \alpha\eta + \eta + 1 \\ \beta^4 &= \alpha + 1 \\ \beta^5 &= 1 \end{aligned}$$

**4)** We bepalen de nevenklassen module 5 in $GF(4)$:

$$\begin{aligned} C_0 &= \{0\} \\ C_1 &= \{1,4\} \\ C_2 &= \{2,3\} \end{aligned}$$

Als we $\beta^2$ en $\beta^3$ als nulpunten van $g(x)$ nemen dan is de graad van $g(x)$ minimaal:

$$g(x) = m^{(2)} = x^2 + \alpha^{10}x + 1$$

Nu decoderen we het gegeven woord.

Aangezien dat $v = 10\ 11\ 11\ 11\ 01$:

$$v(x) = 1 + \eta^2 x + \eta^2 x^2 + \eta^2 x^3 + \eta x^4$$

We vullen eerst alle nulpunten van $g(x)$ in in $v(x)$, dit geeft ons:

$$\begin{array}{lcll} S_1 & = & v(\beta^2) & = & \alpha\eta + 1 \\ S_2 & = & v(\beta^3) & = & \alpha\eta + \eta \end{array}$$

We stellen $\nu = 1$, dit geeft ons:

$$H^{(1)} = \begin{bmatrix} \alpha\eta + 1 \end{bmatrix}$$

det(H) $\neq 0$, dus $\nu$ is inderdaad gelijk aan 2.

Nu krijgen we het volgende stelsel:

$$\begin{bmatrix} \alpha\eta + 1 \end{bmatrix} \begin{bmatrix} \Lambda_0 \end{bmatrix} = \begin{bmatrix} \alpha\eta + \eta \end{bmatrix}$$

In de gegeven tabel zien we dat $\alpha\eta + 1 = \alpha^8$ en ook dat $\alpha^{15} = 1$ dus dan geldt dat:

$$\alpha^8 * \alpha^7 = \alpha^{15} = 1$$

Nu vinden we zo:

$$\Lambda_0 = \alpha\eta + \eta * \alpha^7 = \alpha^2 * \alpha^7 = \alpha^9$$

Dit geeft ons dan weer:

$$\Lambda(x) = \Lambda_0 + x = \alpha^9 + x.$$

De nulpunt van deze veelterm is $X_1 = \alpha^9 = \beta^3$.

Hiermee kunnen we dan weer het volgende stelsel opstellen:

$$\begin{bmatrix} (\alpha^9)^2 \end{bmatrix} \begin{bmatrix} Y_1 \end{bmatrix} = \begin{bmatrix} \alpha^8 \end{bmatrix}$$

Als we dit uitwerken vinden we $Y_1 = \alpha^8 * \alpha^{12} = \alpha^5$.

Dit geeft ons dan:

$$e(x) = \eta x^3$$

Uitendelijk bekomen we dan:

$$c(x) = v(x) - e(x) = 1 + \eta^2 x + \eta^2 x^2 + \eta^2 x^3 + \eta x^4 - \eta x^3 = 1 + \eta^2 x + \eta^2 x^2 + x^3 + \eta x^4$$

Het ontvangen informatiewoord $i(x)$ is dan:

$$i(x) = c(x)/g(x) = 1 + 0x + \eta x^2 = \begin{bmatrix} 1 & 0 & \eta \end{bmatrix} = \begin{bmatrix} 10 & 00 & 01 \end{bmatrix}$$

### 6.3.1 Oefening 4

Beschouw een BCH-code van lengte $n = 15$ over $GF(4)$ die $t = 4$ fouten kan verbeteren. Neem $l = 1$. Decodeer het ontvangen woord $v(x) = x^2 + \eta x^5 + \eta^2 x^{13}$ (met $\eta^2 + \eta + 1 = 0$ (zie hoger)) met het PGZ algoritme.

**Oplossingsmethode**

Zelfde methode als voorgaande oefeningen

**Oplossing**

We factoriseren eerst $x^5 - 1$ over $GF(4)$.

**1)** $4^k \bmod 15 = 1 \Rightarrow k = 2$.
**2)** Gegeven is dat $\alpha$ het primitief element is van $GF(4^2)$ met $\alpha^2 = \eta + \eta\alpha$.
**3)** $\beta = \alpha$.

**4)** We bepalen de nevenklassen module 15 in $GF(4)$:

$$\begin{array}{lcl} C_0 & = & \{0\} \\ C_1 & = & \{1, 4\} \\ C_2 & = & \{2, 8\} \\ C_3 & = & \{3, 12\} \\ C_4 & = & \{4, 1\} \\ C_5 & = & \{5\} \\ C_6 & = & \{6, 9\} \\ C_7 & = & \{7, 13\} \\ C_8 & = & \{8, 2\} \\ C_9 & = & \{9, 6\} \\ C_{10} & = & \{10\} \\ C_{11} & = & \{11, 14\} \end{array}$$

We krijgen zo de volgende minimale veeltermen:

$$\begin{array}{lcll} C_0 & = & \{0\} & \rightarrow \quad m^{(0)} = (x - \alpha^0) = x + 1 \\ C_1 & = & \{1, 4\} & \rightarrow \quad m^{(1)} = (x - \alpha^1)(x - \alpha^4) = x^2 + \eta x + \eta \\ C_2 & = & \{2, 8\} & \rightarrow \quad m^{(2)} = (x - \alpha^2)(x - \alpha^8) = x^2 + (1 + \eta)x + \eta + 1 \\ C_3 & = & \{3, 12\} & \rightarrow \quad m^{(3)} = (x - \alpha^3)(x - \alpha^{12}) = x^2 + \eta x + 1 \\ C_5 & = & \{5\} & \rightarrow \quad m^{(5)} = (x - \alpha^5) = x + \eta \\ C_6 & = & \{6, 9\} & \rightarrow \quad m^{(6)} = (x - \alpha^6)(x - \alpha^9) = x^2 + (\eta + 1)x + 1 \\ C_7 & = & \{7, 13\} & \rightarrow \quad m^{(7)} = (x - \alpha^7)(x - \alpha^{13}) = x^2 + x + \eta \\ C_{10} & = & \{10\} & \rightarrow \quad m^{(10)} = (x - \alpha^{10}) = x + \eta + 1 \\ C_{11} & = & \{11, 14\} & \rightarrow \quad m^{(11)} = (x - \alpha^{11})(x - \alpha^{14}) = x^2 + x + \eta + 1 \end{array}$$

Als we $\beta^2$ en $\beta^3$ als nulpunten van $g(x)$ nemen dan is de graad van $g(x)$ minimaal:

$$g(x) = m^{(2)} = x^2 + \alpha^{10}x + 1$$

# 7 Oefenzitting 7

## 7.1 Oefening 1

Beschouw een BCH-code van lengte $n$ over $GF(q)$ met ontwerpparamters $t$ en $l$. Decodeer het ontvangen woord $v$ m.b.v. het BMF-algoritme (BMF=Berlekamp-Massey en Forney) voor:

(a) $(n, q, t, l) = (5, 4, 1, 2)$ en $v =$ 10 11 11 11 01

(b) $(n, q, t, l) = (15, 4, 4, 1)$ en $v(x) = x^2 + \eta x^5 + \eta^2 x^{13}$ met $\eta^2 + \eta + 1 = 0$

(c) $(n, q, t, l) = (15, 11, 3, 2)$ en $v =$ 3 5 4 3 6 9 10 9 8 10 8 4 6 4 7, waarbij $x^2+x+7$ als primitieve veelterm over $GF(11)$ gebruikt wordt en enkele syndromen zijn $S_2 = 10$, $S_3 = 3$, $S_4 = 0$, $S_5 = 8$ en $S_6 = 1$.

### Oplossingsmethode

We factoriseren eerst $x^n - 1$ over $GF(q)$, de stappen die we uitvoeren vind je in oefenzitting 5.

Daarna voeren we het BM-algoritme uit (zie blz. 75). Kijk zeker naar voorbeeld 65 op blz. 75-76.

Tot slot voeren we dan het algoritme van Forney uit, zie voorbeeld 67 blz. 78-79.

### Oplossing

(a) We factoriseren eerst $x^5 - 1$ over $GF(4)$.

**1)** $4^k \bmod 5 = 1 \Rightarrow k = 2$.
**2)** Gegeven is dat $\alpha$ het primitief element is van $GF(4^2)$ met $\alpha^2 = \eta + \eta\alpha$.
**3)** $\beta = \alpha^3$.

Hiermee berekenen we:

$$\begin{array}{lcll} \beta^1 & = & \alpha + \eta + 1 & = & \alpha^3 \\ \beta^2 & = & \alpha\eta & = & \alpha^6 \\ \beta^3 & = & \alpha\eta + \eta + 1 & = & \alpha^9 \\ \beta^4 & = & \alpha + 1 & = & \alpha^{12} \\ \beta^5 & = & 1 & = & \alpha^0 \end{array}$$

**4)** We bepalen de nevenklassen module 5 in $GF(4)$:

$$\begin{array}{lcl} C_0 & = & \{0\} \\ C_1 & = & \{1,4\} \\ C_2 & = & \{2,3\} \end{array}$$

Aangezien $t = 1$ moeten we $t * 2 = 2$ opeenvolgende $\beta$'s nemen als nulpunt voor $g(x)$, te beginnen bij $\beta^l = \beta^2$, we nemen dus $\beta^2$ en $\beta^3$.

Nu geldt dat:

$$g(x) = m^{(2)} = (x - \beta^2)(x - \beta^3) = x^2 + \alpha^{10}x + 1$$

Aangezien dat $v = 10\ 11\ 11\ 11\ 01$:

$$v(x) = 1 + \eta^2 x + \eta^2 x^2 + \eta^2 x^3 + \eta x^4$$

We vullen alle nulpunten van $g(x)$ in in $v(x)$, dit geeft ons:

$$\begin{array}{lcllcl} S_1 & = & v(\beta^2) & = & \alpha\eta + 1 & = & \alpha^8 \\ S_2 & = & v(\beta^3) & = & \alpha\eta + \eta & = & \alpha^2 \end{array}$$

Nu voeren we het BM-algoritme uit, dit geeft ons de volgende resultaten in tabel-vorm:

| $s$ | $\Delta$ | $n$ | $d$ | $\Lambda(x)$ | $\Lambda^*(x)$ |
|---|---|---|---|---|---|
| 0 | / | 0 | 0 | 1 | 0 |
| 1 | $\alpha^8$ | 0 | 1 | $x$ | $\alpha^7$ |
| 2 | $\alpha^2$ | 1 | 1 | $x + \alpha^9$ | $\alpha^7$ |

We weten dus dat $\Lambda(x) = x + \alpha^9$.

Het nulpunt van deze veelterm is $X_1 = \alpha^9$.

Nu passen we het algoritme van Forney toe.

We berekenen eerst $S(x)$:

$$S(x) = \sum_{k=0}^{1} S_{2-k}x^k = S_2 + S_1 x = \alpha^2 + \alpha^8 x$$

Hiermee berekenen we $\Omega(x)$:

$$\Omega(x) = R_{x^2}((\alpha^2 + \alpha^8 x)(x + \alpha^9)) = R_{x^2}(\alpha^{11} + \alpha^8 x^2)$$

$R_{x^2}(\alpha^{11} + \alpha^8 x^2)$ is gelijk aan de rest wanneer dat $\alpha^{11} + \alpha^8 x^2$ wordt gedeeld door $x^2$:

$$\Omega(x) = R_{x^2}(\alpha^{11} + \alpha^8 x^2) = \alpha^{11}$$

De afgeleide van $\Lambda(x)$:

$$\Lambda'(x) = 1$$

Nu bereken we nog $Y_1$:

$$Y_1 = \frac{\alpha^{11}}{X_1^4 * 1} = \frac{\alpha^{11}}{\alpha^6} = \alpha^5$$

Hiermee vinden we nu $e(x)$:

$$e(x) = Y_1 x^3 = \alpha^5 x^3 = \eta x^3$$

Nu kunnen we $c(x)$ berekenen:

$$c(x) = v(x) - e(x) = 1 + \eta^2 x + \eta^2 x^2 + x^3 + \eta x^4$$

Het ontvangen informatiewoord $i(x)$ is dan:

$$i(x) = c(x)/g(x) = 1 + 0x + \eta x^2 = \begin{bmatrix} 1 & 0 & \eta \end{bmatrix} = \begin{bmatrix} 10 & 00 & 01 \end{bmatrix}$$

(b) We factoriseren eerst $x^{15} - 1$ over $GF(4)$.

**1)** $4^k \bmod 15 = 1 \Rightarrow k = 2$.
**2)** Gegeven is dat $\alpha$ het primitief element is van $GF(4^2)$ met $\alpha^2 = \eta + \eta\alpha$.
**3)** $\beta = \alpha$.
**4)** We bepalen de nevenklassen module 15 in $GF(4)$:

| | | | | | |
|---|---|---|---|---|---|
| $C_0$ | = | {0} | $C_6$ | = | {6,9} |
| $C_1$ | = | {1,4} | $C_7$ | = | {7,13} |
| $C_2$ | = | {2,8} | $C_{10}$ | = | {10} |
| $C_3$ | = | {3,12} | $C_{11}$ | = | {11} |
| $C_5$ | = | {5} | | | |

**5)** We bepalen minimaalveeltermen:

$$\begin{aligned}
m^{(1)} &= (x-\beta^1)(x-\beta^4) = x^2 + \alpha^5 x + \alpha^5 \\
m^{(2)} &= (x-\beta^2)(x-\beta^8) = x^2 + \alpha^{10} x + \alpha^1 0 \\
m^{(3)} &= (x-\beta^3)(x-\beta^{12}) = x^2 \alpha^5 x + 1 \\
m^{(5)} &= (x-\beta^5) = x + \alpha^5 \\
m^{(6)} &= (x-\beta^6)(x-\beta^9) = x^2 + \alpha^{10} + 1 \\
m^{(7)} &= (x-\beta^7)(x-\beta^{13}) = x^2 + x + \alpha^5 \\
m^{(10)} &= (x-\beta^{10}) = x + \alpha^{10} \\
m^{(11)} &= (x-\beta^{11}) = x + \alpha^{11}
\end{aligned}$$

Aangezien $t = 4$ moeten we $4 * 2 = 8$ opeenvolgende $\beta$'s nemen als nulpunt voor $g(x)$, te beginnen bij $\beta^l = \beta^1$, we nemen dus $\beta^1, \beta^2, \ldots, \beta^8$.

Nu geldt dat:

$$g(x) = m^{(1)}m^{(2)}m^{(3)}m^{(5)}m^{(6)}m^{(7)} =$$

We vullen alle nulpunten van $g(x)$ in in $v(x)$, dit geeft ons:

$$\begin{array}{lllll} S_1 & = & v(\alpha) & = & 0 & = & 0 \\ S_2 & = & v(\alpha^2) & = & \eta^2\alpha + \eta^2 & = & \alpha^7 \\ S_3 & = & v(\alpha^3) & = & \eta^2\alpha & = & \alpha^{11} \\ S_4 & = & v(\alpha^4) & = & 0 & = & 0 \\ S_5 & = & v(\alpha^5) & = & \eta^2 & = & \alpha^{10} \\ S_6 & = & v(\alpha^6) & = & \eta\alpha + 1 & = & \alpha^8 \\ S_7 & = & v(\alpha^7) & = & \eta & = & \alpha^5 \\ S_8 & = & v(\alpha^8) & = & \eta^2\alpha + \eta & = & \alpha^{13} \end{array}$$

De verdere uitwerking, moet nog worden aangevuld.

(c) We factoriseren eerst $x^{15} - 1$ over $GF(11)$.

**1)** $11^k \bmod 15 = 1 \Rightarrow k = 2$.
**2)** Gegeven is dat $\alpha$ het primitief element is van $GF(11^2)$ met $\alpha^2 = 10\alpha + 4$.
**3)** Gegeven is dat $\beta = \alpha^8$.

**4)** We bepalen de nevenklassen module 5 in $GF(4)$:

$$\begin{array}{lllll} C_0 & = & \{0\} & C_5 & = & \{5,10\} \\ C_1 & = & \{1,11\} & C_6 & = & \{6\} \\ C_2 & = & \{2,7\} & C_8 & = & \{8,13\} \\ C_3 & = & \{3\} & C_9 & = & \{91\} \\ C_4 & = & \{4,14\} & C_{12} & = & \{1\} \end{array}$$

**5)** We bepalen minimaalveeltermen:

$$\begin{array}{lll} m^{(2)} & = & x^2 + 9x + 4 \\ m^{(3)} & = & x + 6 \\ m^{(4)} & = & x^2 + 4x + 5 \\ m^{(5)} & = & x^2 - \beta^{14}x \\ m^{(6)} & = & x + 8 \\ m^{(8)} & = & x^2 + 5x + 3 \\ m^{(9)} & = & x + 7 \\ m^{(12)} & = & x + 2 \end{array}$$

Aangezien $t = 3$ moeten we $3 * 2 = 6$ opeenvolgende $\beta$'s nemen als nulpunt voor $g(x)$, te beginnen bij $\beta^l = \beta^2$, we nemen dus $\beta^2, \beta^3, \ldots, \beta^8$.

Nu geldt dat:

$$g(x) = m^{(2)}m^{(3)}m^{(4)}m^{(5)}m^{(6)}m^{(8)}$$