rijksuniversiteit groningen

faculteit wiskunde en natuurwetenschappen

Bijnalichamen

Rianne de Heide

Bachelorscriptie Wiskunde

25 mei 2012

Inleiding

Deze bachelorscriptie gaat over de algebraïsche structuur die 'bijnalichaam' wordt genoemd. Het eerste hoofdstuk geeft een overzicht van de belangrijkste definities en stellingen over groepen, ringen en lichamen die nodig zijn voor de volgende hoofdstukken. De stof behandeld in het college 'groepentheorie' wordt bekend verondersteld, en wanneer ook het college 'algebraïsche structuren' is gevolgd, kan het eerste hoofdstuk (deels) worden overgeslagen, om er eventueel later definities in terug te zoeken. In het tweede hoofdstuk worden enkele eigenschappen van een lichaam bij een bijnalichaam genoemd en bewezen. Het derde hoofdstuk richt zich op de constructie van eindige bijnalichamen, eerst via een nieuwe afbeelding voor de vermenigvuldiging in een lichaam, en daarna wordt een algemene manier om een bijnalichaam met behulp van een lichaam te construeren, bedacht door L.E. Dickson bestudeerd. In het vierde hoofdstuk worden de eindige bijnalichamen geclassificeerd volgens het zgn. Zassenhauscriterium, en worden hier voorbeelden bij gegeven. Het is bekend dat op zeven uitzonderingen na alle eindige bijnalichamen gevonden kunnen worden met behulp van de constructie van Dickson. Tenslotte ga ik iets dieper in op een van de zeven uitzonderingen.

Inhoudsopgave

Inhoudsopgave **iii**

1 Algebraïsche structuren **1**
1.1 Inleiding 1
1.2 Lichamen 6

2 Eigenschappen van bijnalichamen **9**
2.1 Commutativiteit van de optelling 9
2.2 Priemlichaam en karakteristiek 10

3 Constructie van bijnalichamen **11**
3.1 Constructie van een bijnalichaam 11
3.2 Een algemene manier om een bijnalichaam te construeren . . . 16
3.3 Toepassing van de methode 21

4 Classificatie van bijnalichamen **23**
4.1 Eenheidswortels en cirkeldelingspolynomen 23
4.2 Classificatie van eindige bijnalichamen 25
4.3 De eindige uitzonderingsbijnalichamen 28

Bibliografie **35**

Hoofdstuk 1

Algebraïsche structuren

Het volgende hoofdstuk is een soort opsomming van definities en stellingen die later in de scriptie gebruikt gaan worden. Lang niet alle stellingen worden hier bewezen, de bewijzen zijn terug te vinden in de aangegeven literatuur. Ook wordt hier het *bijnalichaam* gedefinieerd, en enkele heel belangrijke begrippen als *kern* en *centrum*.

1.1 Inleiding

Ringen

Zij $(R, +, \cdot, 0, 1)$ een algebraïsche structuur met R een verzameling, $+$ en $\cdot$ afbeeldingen:

$$\begin{aligned} + &: R \times R \to R, & (a, b) &\mapsto a + b \\ \cdot &: R \times R \to R, & (a, b) &\mapsto ab \end{aligned}$$

en 0 en 1 elementen van R; en een zestal axioma's:

(R1) $(R, +, 0)$ is een Abelse groep, dit houdt in:
- **(G1)** $a + (b + c) = (a + b) + c \; \forall \, a, b, c \in R$
- **(G2)** $0 + a = a + 0 = a \, \forall \, a \in R$
- **(G3)** $\forall a \in \mathbb{R} \, \exists - a \in R$ waarvoor geldt $a + (-a) = (-a) + a = 0$
- **(G4)** $a + b = b + a \, \forall \, a, b \in R$

(R2) associativiteit van $\cdot$: $a(bc) = (ab)c \; \forall \, a, b, c \in R$

(R3) distributieve wetten:

$$\begin{aligned} a(b + c) &= ab + ac \qquad \text{en} \\ (b + c)a &= ba + ca \qquad \forall \, a, b, c \in R \end{aligned}$$

(R4) $1a = a1 = a \; \forall \, a \in R$

(R5) $ab = ba \; \forall \, a, b \in R$

(R6) $1 \neq 0$, en $\forall a \in R$, $a \neq 0 \; \exists \, a^{-1} \in R$ waarvoor geldt $a \cdot a^{-1} = a^{-1} \cdot a = 1$

R heet een *ring* als axioma's (R1) tot en met (R3) gelden, en een *unitaire ring* als axioma's (R1) tot en met (R4) gelden. De ring R heet *commutatief* als bovendien (R5) geldt. Een *delingsring* of *scheeflichaam* voldoet aan (R1) tot en met (R4) en (R6). Een *lichaam* is een commutatieve delingsring, en voldoet derhalve aan (R1) tot en met (R6).[1]

Vaak wordt in de schrijfwijze het 0- en het 1-element weggelaten: $(R, +, \cdot)$ in plaats van $(R, +, \cdot, 0, 1)$, zowel voor ringen als voor groepen.

Een ring R heet *eindig* als het aantal elementen van R eindig is.

Het *centrum* van een ring R is als volgt gedefinieerd:

$$Z(R) := \{c \in R \mid cx = xc \ \forall x \in R\}$$

De *centralisator* van $X \subset R$ is:

$$Z_R(X) := \{c \in R \mid cx = xc \ \forall x \in X\}$$

Beide zijn deelringen van R. [2]

Eenheden

Zij R een ring met 1. Een element $a \in R$ heet een *eenheid* als er een $b \in R$ bestaat met

$$ab = ba = 1$$

De verzameling eenheden van R wordt genoteerd $U(R)$ en heet de *eenhedengroep* van R. De eenhedengroep $U(R)$ van een unitaire ring R is een groep ten opzichte van de vermenigvuldiging. Een element $a \in R$ heet een *linkseenheid* als $\exists b \in R : ab = 1$ en een *rechtseenheid* als $\exists c \in R : ca = 1$. $R \backslash \{0\}$ wordt genoteerd als R^*.

Nuldelers

Een element a van een ring R heet een *linkernuldeler* als $a \neq 0$ en $\exists b \in R : b \neq 0 \wedge ab = 0$; een *rechternuldeler* als $a \neq 0$ en $\exists c \in R : c \neq 0 \wedge ca = 0$; en een *nuldeler* als beide het geval is. Een *domein* of *integriteitsgebied* is een commutatieve ring met $1 \neq 0$ zonder nuldelers.

Idealen

Zij R een ring. Een *ideaal* I van R is een deelverzameling $I \subset R$ die de volgende eigenschappen heeft:

(I1) I is een ondergroep van de additieve groep van R:
- **(H1)** $0 \in I$
- **(H2)** $a - b \in I \, \forall \, a, b \in I$

(I2) $\forall r \in R$ geldt $ra \in I$ en $ar \in I$

Een *linksideaal* wordt verkregen door (I2) te vervangen door de zwakkere eis

$$\forall r \in R : \forall a \in I : ra \in I$$

En een *rechtsideaal* wordt verkregen door in het bovenstaande ra door ar te vervangen.

De *factorring* is gedefinieerd

$$R/A := \{x + A \mid x \in R\}$$

waarbij de optelling en de vermenigvuldiging zijn gedefinieerd door

$$(x + A) + (y + A) := (x + y) + A$$
$$(x + A) \cdot (y + A) := xy + A$$

Als een ideaal in een commutatieve ring R wordt voorgebracht door een element a_1, dan heet het door a_1 voortgebrachte ideaal een *hoofdideaal*

$$(a_1) = a_1R = Ra_1 = \{ra_1 : r \in R\}$$

Voorbeelden van hoofdidealen zijn het triviale ideaal $\{0\} = (0)$ en $R = (1)$.

Een ring R heet een *hoofdideaalring* als ieder ideaal van R een hoofdideaal is.

Zij R een commutatieve ring met 1. Een *priemideaal* is een ideaal $I \subset R$ dat voldoet aan:

(P1) $I \neq R$

(P2) $\forall\ a, b \in R$ met $ab \in I$ geldt: $a \in I$ of $b \in I$

Een ideaal M van R heet *maximaal* als geldt:

(M1) $M \neq R$

(M2) voor elk ideaal J van R met $M \subset J \subset R$ geldt $J = M$ of $J = R$

Voor idealen A van R geldt:
(i) R/A is een domein, dan en slechts dan als A een priemideaal is
(ii) R/A is een lichaam, dan en slechts dan als A een maximaal ideaal is

Deelbaarheid in domeinen

Zij R een domein. $a, b \in R$ heten *geassocieerd* als $a \cdot U(R) = b \cdot U(R)$. Wanneer a een deler van b is, schrijven we $a \mid b$, zo niet: $a \nmid b$. Een element $a \neq 0$ dat geen eenheid is heet *irreducibel* wanneer $a = bc$, $b \in U(R)$ of $c \in U(R)$ als gevolg heeft, en *priemelement* als uit $a \mid bc$ moet volgen $a \mid b$ of $a \mid c$. Ieder priemelement is irreducibel. [1]

Bijnaringen

Wanneer (R3) wordt vervangen door de zwakkere eis (linksdistributiviteit)

$$a \cdot (b + c) = ab + ac \ \forall a, b, c \in R$$

en (R2) door

$$0 \cdot a = 0 \ \forall a \in R$$

spreekt men van een *links-bijnaring*, en wanneer (R3) wordt vervangen door alleen de rechtsdistibutieve wet

$$(b + c) \cdot a = ba + ca$$

en (R2) door

$$a \cdot 0 = 0 \ \forall a \in R$$

spreekt men van een *rechts-bijnaring*.

Een *bijnalichaam* is een scheeflichaam waarbij (R3), de distributieve wetten, worden vervangen door een van bovenstaande zwakkere eisen, waarbij ook (R2) aangepast moet worden. Een bijnalichaam is dus eigenlijk een bijna-scheeflichaam, en is dus niet noodzakelijk commutatief in de vermenigvuldiging. [3]

Quasilichaam

Een *quasi-groep* is een groep $(Q, *)$ zodanig dat voor elke a en b in Q er unieke elementen x en y in Q bestaan zodanig dat

$$a * x = b$$
$$y * a = b$$

Een *lus* is een quasi-groep met een identiteitselement 1 zodanig dat

$$x * 1 = 1 * x = x$$

Een bijnaring F heet een *quasi-lichaam* wanneer $(F^*, \cdot, 1)$ een lus is, met

$$F^* = F \backslash \{0\}$$

Bijnalichaam

Een bijnaring $F \neq \{0\}$ is een bijnalichaam dan en slechts dan als $(F^*, \cdot, 1)$ een groep vormt. Ieder lichaam is een bijnalichaam. Een bijnalichaam dat geen lichaam is, wordt *eigenlijk* genoemd. Een deelverzameling $D \neq \emptyset$ van een bijnaring heet een *deelbijnaring* als voor $x, y \in D$ ook geldt $x - y \in D$ en $xy \in D$ (op dezelfde manier: *deellichaam*, *deelbijnalichaam*).

Kern en centrum

De *rechtsassociator* $A_F := \{a \in F \mid \forall x, y \in F : (xy)a = x(ya)\}$ is een deelbijnaring van F met associatieve vermenigvuldiging. De *distributor* $D_F := \{d \in F \mid \forall x, y \in F : (x + y)d = xd + yd\}$ is, wanneer $(F, +, 0)$ Abels is, een ondergroep van $(F, +, 0)$. De *kern* $K_F := A_F \cap D_F$ is een deelring van A_F, anders gezegd: de kern bestaat uit de elementen waarvoor zowel de associatieve als distributieve wetten opgaan. Het *centrum* $Z_F := \{z \in F \mid \forall x \in F : zx = xz\}$, ligt in D_F. Een quasilichaam Q is een bijnalichaam resp. lichaam dan en slechts dan als $Q = A_Q$ resp. $Q = K_Q$. [2]

Ook het centrum Z_F van een bijnaring F is een deelring. Neem een $x, y \in Z_F$, en neem een $f \in F$. Dan is $(x + y)f = xf + yf = fx + fy = f(x + y)$, dus $(x+y) \in Z_F$. Ook geldt $-x(f) = -(xf) = -(fx) = (-f)(x) = f(-x)$, dus ook $-x \in Z_F$. Als laatste geldt $(xy)f = x(yf) = x(fy) = (xf)y = (fx)y = f(xy)$, dus $xy \in Z_F$. Hiermee is bewezen dat Z_F een deelring is van F.

Homomorfismen

Een afbeelding f tussen twee ringen R_1 en R_2 $f : R_1 \to R_2$ heet een *homomorfisme* als geldt:

$$\begin{aligned} f(a + b) &= f(a) + f(b) \\ f(ab) &= f(a) \cdot f(b) \end{aligned}$$

$\forall\, a, b \in R_1$ en

$$f(1) = 1$$

als het unitaire ringen betreft. Een injectief homomorfisme heet een *monomorfisme*. Een homomorfisme dat bijectief is heet een *isomorfisme* en een homomorfisme van een ring R naar zichzelf heet een *automorfisme*. De verzameling van automorfismen van R vormt een groep: Aut$R$. R_1 en R_2 heten *isomorf* als er een isomorfisme bestaat van R_1 naar R_2 ($R_1 \cong R_2$).

Een afbeelding f tussen twee ringen R_1 en R_2 $f : R_1 \to R_2$ heet een *antihomomorfisme* als geldt:

$$\begin{aligned} f(a + b) &= f(a) + f(b) \\ f(ab) &= f(b) \cdot f(a) \end{aligned}$$

$\forall\, a, b \in R_1$

Het *isomorfie-type* van een bepaald wiskundig object is de klasse van dezelfde wiskundige objecten die hieraan isomorf zijn.

Groepen

De *orde* van een groep is de kardinaliteit: het aantal elementen van de groep. De *orde* van een element a van een groep is het kleinste gehele getal $n \in \mathbb{N}$ waarvoor geldt dat $a^n = e$, met e het identiteitselement van de groep. Als er

niet zo een n bestaat, dan is het element van oneindige orde. Alle elementen van eindige groepen zijn van eindige orde.

Een *periodieke groep* of *torsiegroep* is een groep waarin elk element eindige orde heeft. Alle eindige groepen zijn periodiek. Als p een priemgetal is, dan is een *p-groep* een torsiegroep, waarin elk element een macht van p als orde heeft. Zo een groep heet ook wel *p-primair* of *primair*. Een eindige groep is dan en slechts dan een p-groep als de orde (aantal elementen van de groep) een macht van p is.

Een *elementair-Abelse groep* is een eindige Abelse groep waar elk nontriviaal element orde p heeft, met p priem. Zij G een groep. Een element $g \in G$ heet een *torsie-element* als g van eindige orde is. Als het enige torsie-element in G het eenheidselement is, dan heet de groep G *torsievrij*.

(Stelling 1) Zij p een priemgetal en G een groep met orde p^n. Dan is het centrum van G, $Z(G) \neq \{1\}$.

Bewijs Schrijf G als disjuncte vereniging van conjugatieklassen $C_g := \{hgh^{-1} \mid h \in G\}$. Het aantal elementen van een C_g is een deler van het aantal elementen van G. Definieer voor $j \in \mathbb{N}$ het aantal conjugatieklassen n_j van G, met orde p^j. Dan is partitie van G in conjugatieklassen gegeven door:

$$\begin{aligned} \#G = p^n &= n_0 + pn_2 + p^t n_2 + \ldots + p^t n_t \\ n_0 &= p(n_1 + pn_2 + \ldots + p^{t-1} n_t + p^{n-1}) \end{aligned}$$

voor een bepaalde t en $n_0, \ldots, n_t \in \mathbb{N}$. p deelt dus n_0. De conjugatieklasse van het identiteitselement heeft één element, dus $n_0 \geq 1$, en omdat $p \mid n_0$, is $n_0 \geq p$. De conjugatieklasse van een element $g \in G$ heeft één element, dan en slechts dan als g in het centrum van G zit, dus n_0 is $\#Z(G)$. Er zitten tenminste p elementen van G in het centrum van G.

1.2 Lichamen

Lichaam van invarianten

Zij K een lichaam. Voor ieder automorfisme $\sigma \in \mathrm{Aut}(K)$ kan men een deellichaam van K definiëren:

$$K^\sigma := \{x \in K : \sigma(x) = x\} \tag{1.1}$$

Dit lichaam heet het *lichaam van invarianten* (Engels: fixed field; Duits: Fixkörper). Ook voor iedere ondergroep $G \subset \mathrm{Aut}(K)$ kan men een deellichaam van K definiëren, het *lichaam van invarianten* van G:

$$K^G := \{x \in K : \sigma(x) = x \forall \sigma \in G\} \tag{1.2}$$

Om verwarring te voorkomen zal ik in het vervolg de in Duitsland gebruikelijke notatie $K^\sigma := \mathrm{Fix}(\sigma)$ en $K^G := \mathrm{Fix}(G)$ gebruiken.

Priemlichaam en Karakteristiek

De doorsnede van *alle deellichamen* K' van een lichaam K wordt het *priemlichaam* K_0 van K genoemd:

$$K_0 := \bigcap_{K' \subset K} K'$$

Het priemlichaam K_0 is isomorf met:

- ofwel het lichaam $\mathbb{Q}$ der rationele getallen
- ofwel een van de lichamen $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, met p een priemgetal.

Laat K een lichaam zijn met priemlichaam K_0.
Als $K_0 \cong \mathbb{Q}$ zegt men dat K *karakteristiek* 0 heeft: $Kar(K) = 0$.
Als $K_0 \cong \mathbb{F}_p$ zegt men dat K *karakteristiek* p heeft: $Kar(K) = p$.

Minimumpolynoom

Als L een lichaam is en $K \subset L$ een deellichaam van L, dan heet L een *lichaamsuitbreiding* van K. Voor iedere $\alpha \in L$ is er een evaluatiehomomorfisme

$$\begin{aligned} \Psi_\alpha : K[x] &\to L, \\ f &\mapsto f(\alpha) \end{aligned}$$

De kern van Ψ_α is een ideaal in $K[x]$, en is dus een hoofdideaal. Dan is ofwel $ker(\Psi_\alpha) = (0)$, ofwel

$$\begin{aligned} ker(\Psi_\alpha) &= (f_K^\alpha), \\ f_K^\alpha &\in K[x], \end{aligned}$$

een uniek monisch polynoom, dat het *minimumpolynoom* van α over K wordt genoemd. [1]

Classificatie van eindige lichamen

De volgende stelling classificeert eindige lichamen.
a) Zij K een eindig lichaam. Dan is er een priemgetal p en een geheel getal $n \geq 1$ met $\#K = p^n$.
b) Omgekeerd is er voor elk priemgetal p en elk geheel getal $n \geq 1$ een eindig lichaam met p^n elementen, en dit lichaam is op isomorfie na eenduidig bepaald.
Het eenduidig bepaalde lichaam met $q = p^n$ elementen wordt aangegeven met $\mathbb{F}_q$, en het is het ontbindingslichaam van $X^q - X$ over $\mathbb{F}_p$ [1]:

$$\mathbb{F}_p \cong \Omega_{\mathbb{F}_q}^{X^q - X}$$

Hoofdstuk 2

Eigenschappen van bijnalichamen

2.1 Commutativiteit van de optelling

De commutativiteit van de optelling in een bijnalichaam kan worden afgeleid uit de andere axioma´s. Hieronder volgt het bewijs hiervoor: eerst voor het eindige geval, vervolgens wordt het bewijs van Neumann en Karzel in het algemene geval weergegeven.

Eindige bijnalichamen

Zij F een eindig bijnalichaam. In dat geval bestaat er een $n \in \mathbb{N}$ met $n \cdot 1 = 0$. De kleinste n is een priemgetal p. Stel dat n niet een priem is. Neem $n = pq$ met $p \leq q < n$. Dan is $p \cdot 1 \neq 0$ en $q \cdot 1 \neq 0$, maar $(p \cdot 1)(q \cdot 1) = (pq) \cdot 1 = 0$, hetgeen in tegenspraak is met het feit dat F nuldelervrij is.

$p \cdot x = x \cdot (p \cdot 1) = 0$ waardoor $(F, +)$ een p-groep is (zie het eerste hoofdstuk, Groepen) en deze heeft een element $a \neq 0$ in het centrum. Voor willekeurige $x, y \in F$ met $y \neq 0$ volgt hieruit:

$$x + y = ya^{-1} \cdot (ay^{-1}x + a) = ya^{-1} \cdot (a + ay^{-1}x) = y + x$$

Bewijs van Neumann en Karzel

Voor het algemene geval: niet alleen eindige bijnalichamen, zijn verschillende bewijzen geleverd, allereerst in 1940 door B.H. Neumann. H. Karzel heeft in 1964 een korter bewijs geformuleerd gebaseerd op dat van Neumann [4]. Hieronder wordt dat bewijs weergegeven. Hiervoor zijn eerst een aantal stellingen nodig.

1. Stelling: Voor alle elementen x, y van een bijnaring geldt $x \cdot 0 = 0$ en $x \cdot (-y) = -xy$

   Bewijs: volgt direct uit de linksdistributiviteit.

2. Stelling: In elk bijnalichaam F geldt voor alle $x, y \in F$:

   a) $x^2 = 1 \Leftrightarrow x = 1$ of $x = -1$

b) $(-1) \cdot x = x \cdot (-1)$

c) $(-x) \cdot y = -xy = x \cdot (-y)$

Bewijs:

a) $\Leftarrow$ volgt uit de eerste stelling. Voor $\Rightarrow$ zie het volgende:

$$(-1)(1+1) = (-1) + (-1) = -(1+1) = (1+1)(-1) \qquad (2.1)$$

Nu geldt $x^2 = 1$. In het geval dat $1 = -1$, definieer $y := x - 1$, en in het geval dat $2 := 1+1 \neq 0$, definieer $y := 1 + (-1+x) \cdot 2^{-1}$. Uit de eerste stelling en (2.1) volgt nu:

$$\begin{aligned} 1 = -1 : xy &= 1 - x = (1-x)(-1) = -(1-x) = y \\ 1 \neq -1 : xy &= x + (-x+1) \cdot 2^{-1} = 1 + (-x+1)(-1+2^{-1}) \\ &= 1 + (-x+1)2^{-1}(-1) = 1 + (-x+1)(-1)2^{-1} = y \end{aligned}$$

In beide vergelijkingen volgt $x = 1$ of $y = 0$, en $y = 0$ levert $x = 1$ in de eerste vergelijking en $x = -1$ in de tweede.

b) Voor alle $x \neq 0$ geldt $(x(-1)x^{-1})^2 = 1$, waaruit het in combinatie met a) is aangetoond.

c) Volgt direct uit b) en de eerste stelling.

Uit 2c volgt het volgende. Gegeven $x, y \in F$ met inversen $-x, -y$.

$$\begin{aligned} (x+y) + ((-y) + (-x)) &= x + (y + (-y)) + (-x) \\ &= x + (0) + (-x) \\ &= x + (-x) = 0 \\ -y - x &= -(x+y) \\ &= (-1)(x+y) \\ &= (-1)x + (-1)y = -x - y \end{aligned}$$

Waarmee is bewezen dat de additieve groep van een bijnalichaam Abels is.

2.2 Priemlichaam en karakteristiek

Voor een bijnalichaam F is de kern K_F een deelscheeflichaam, en bevat het centrum Z_F van F. De karakteristiek van het bijnalichaam F wordt gedefinieerd als de karakteristiek van de kern: $Kar(F) := Kar(K_F)$. Ook het priemlichaam van F wordt gedefinieerd als het priemlichaam van de kern: $F_p := (K_F)_p$.

Hoofdstuk 3

Constructie van bijnalichamen

In het volgende hoofdstuk gaan we proberen een bijnalichaam te construeren met behulp van een lichaam, voorbeelden te vinden en een algemene manier te vinden bijnalichamen te construeren.

3.1 Constructie van een bijnalichaam

Voordat een bijnalichaam geconstrueerd kan worden, moet er een lichaam geconstrueerd worden. Hierna proberen we een nieuwe vermenigvuldiging op de elementen van het lichaam te vinden, zodanig dat er een bijnalichaam wordt geconstrueerd. In het daaropvolgende gedeelte wordt in detail ingegaan op de constructie van het kleinste eigenlijke bijnalichaam, dat 9 elementen heeft.

Constructie van een eindig lichaam

De eenvoudigste eindige lichamen zijn de restklassen $\mathbb{K}_p = \mathbb{Z}/p\mathbb{Z}$ voor priemgetallen p. De elementen van het lichaam kunnen dan weergegeven worden door $\{0, 1, 2, ..., p-1\}$ en de afbeeldingen zijn de optelling en vermenigvuldiging modulo p. Dit lichaam heeft p elementen, dus in bovenstaande classificatie $n = 1$. Als $n \neq 1$, moet het lichaam op een andere manier geconstrueerd worden.

Een lichaam construeren met $q = p^n$ elementen dat werkt voor willekeurige n gaat als volgt. Kies een monisch irreducibel polynoom $f(X)$ in de polynoomring $\mathbb{K}_p[X]$ (dus met coëfficiënten in $\mathbb{K}_p$) van graad n. Het door $f(X)$ voortgebrachte ideaal is $(f(X))$. Dan is $\mathbb{K}_p[X]/(f(X))$ een lichaam met $q = p^n$ elementen.

Voorbeeld: een lichaam met 4 elementen
Neem $f(X) = X^2 + X + 1$, deze is irreducibel in $\mathbb{Z}/2\mathbb{Z}$. Het lichaam is dan $(\mathbb{Z}/2\mathbb{Z})[x]/(x^2 + x + 1)$. De elementen zijn $\{0, 1, x, y\}$, met $0 = 0 + (x^2 + x + 1$ en $x = x + (x^2 + x + 1)$. De vermenigvuldiging wordt als volgt geconstrueerd: we hebben $X^2 + X + 1$, en omdat we in $\mathbb{Z}/2\mathbb{Z}$ zitten, is $-1 = 1$ dus is het te schrijven als $X^2 = X + 1$. Bijvoorbeeld: $x^3 = x(x^2) = x(x + 1) = x^2 + x = x + 1 + x = 2x + 1 = 1$. Om de inverse van x ten opzichte van de vermenigvuldiging te construeren, moet er een polynoom $p(x)$ gevonden worden

zodanig dat $xp(x) = 1 \bmod (x^2 + x + 1)$. Dit werkt voor $p(x) = x + 1$ dus $1/x = x + 1$.

Voorbeeld: een lichaam met 9 elementen
Een lichaam heeft p^n elementen, dus $p = 3$ en $n = 2$ in dit voorbeeld. Neem het lichaam $\mathbb{K}_3$ en het polynoom $f = x^2 + x - 1 \in \mathbb{K}_3[x]$, dan is $\mathbb{K}_3[x]/(f)$ een eindig lichaam met 9 elementen.

Het lichaam $\mathbb{K}_3[x]/(f)$ bestaat uit de elementen $\{0, 1, 2, \theta, \theta+1, \theta+2, 2\theta, 2\theta+1, 2\theta+2\}$, $\theta = x + (x^2 + x - 1)$. De optelling en vermenigvuldiging gaan als volgt:

$+$	0	1	2	θ	$\theta+1$	$\theta+2$	2θ	$2\theta+1$	$2\theta+2$
0	0	1	2	θ	$\theta+1$	$\theta+2$	2θ	$2\theta+1$	$2\theta+2$
1		2	0	$\theta+1$	$\theta+2$	θ	$2\theta+1$	$2\theta+2$	2θ
2			1	$\theta+2$	θ	$\theta+1$	$2\theta+2$	2θ	$2\theta+1$
θ				2θ	$2\theta+1$	$2\theta+2$	0	1	2
$\theta+1$					$2\theta+2$	2θ	1	2	0
$\theta+2$						$2\theta+1$	2	0	1
2θ							θ	$\theta+1$	$\theta+2$
$2\theta+1$								$\theta+2$	θ
$2\theta+2$									$\theta+1$

$*$	0	1	2	θ	$\theta+1$	$\theta+2$	2θ	$2\theta+1$	$2\theta+2$
0	0	0	0	0	0	0	0	0	0
1		1	2	θ	$\theta+1$	$\theta+2$	2θ	$2\theta+1$	$2\theta+2$
2			1	2θ	$2\theta+2$	$2\theta+1$	θ	$\theta+2$	$\theta+1$
θ				$2\theta+1$	1	$\theta+1$	$\theta+2$	$2\theta+2$	2
$\theta+1$					$\theta+2$	2θ	2	θ	$2\theta+1$
$\theta+2$						2	$2\theta+2$	1	θ
2θ							$2\theta+1$	$\theta+1$	1
$2\theta+1$								2	2θ
$2\theta+2$									$\theta+2$

De vermenigvuldiging gaat op de volgende manier:

$$\begin{aligned}(\theta)(\theta) &= (x + (f))(x + (f)) \\ &= x^2 + (f) \\ &= f - x + 1 + (f) \\ &= 2x + 1 + (f) \\ &= 2\theta + 1\end{aligned}$$

Bijvoorbeeld:

$$\begin{aligned}(2\theta)(\theta + 1) &= 2\theta^2 + 2\theta \\ &= 2(\theta + 1) + 2\theta \\ &= \theta + 2 + 2\theta \\ &= 2\end{aligned}$$

Een bijnalichaam met 9 elementen

Uit het in het voorbeeld hierboven verkregen lichaam met 9 elementen, kan een bijnalichaam gevormd worden. We hadden het lichaam van de verzameling

$$K = \{0, 1, 2, \theta, \theta+1, \theta+2, 2\theta, 2\theta+1, 2\theta+2\} \tag{3.1}$$

met de optelling $+$ en vermenigvuldiging $*$. Definieer een nieuwe vermenigvuldiging $\cdot$

$$a \cdot b = \begin{cases} a * b & \text{als } b \in K \text{ een kwadraat is, met } a \in K \text{ willekeurig} \\ a^3 * b & \text{als } b \in K \text{ niet kwadraat is, met } a \in K \text{ willekeurig} \end{cases}$$

$(K, +, \cdot)$ is een bijnalichaam met 9 elementen. Dit is het kleinste eigenlijke bijnalichaam. De volgende elementen in K_9^* zijn een kwadraat:

$$\begin{aligned} 1 &= 1^2 = 2^2 \\ 2 &= (\theta+2)^2 = (2\theta+1)^2 \\ \theta+2 &= (\theta+1)^2 = (2\theta+2)^2 \\ 2\theta+1 &= \theta^2 = (2\theta)^2 \end{aligned}$$

En de overige elementen $\{\theta, \theta+1, 2\theta, 2\theta+2\}$ zijn geen kwadraat.

De optelling is bij een bijnalichaam commutatief, dus wordt de volgende tabel verkregen:

$+$	0	1	2	θ	$\theta+1$	$\theta+2$	2θ	$2\theta+1$	$2\theta+2$
0	0	1	2	θ	$\theta+1$	$\theta+2$	2θ	$2\theta+1$	$2\theta+2$
1		2	0	$\theta+1$	$\theta+2$	θ	$2\theta+1$	$2\theta+2$	2θ
2			1	$\theta+2$	θ	$\theta+1$	$2\theta+2$	2θ	$2\theta+1$
θ				2θ	$2\theta+1$	$2\theta+2$	0	1	1
$\theta+1$					$2\theta+2$	2θ	1	2	0
$\theta+2$						$2\theta+1$	2	0	1
2θ							θ	$\theta+1$	$\theta+2$
$2\theta+1$								$\theta+2$	θ
$2\theta+2$									$\theta+1$

De vermenigvuldigingstabel ziet er als volgt uit:

$*$	0	1	2	θ	$\theta+1$	$\theta+2$	2θ	$2\theta+1$	$2\theta+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	θ	$\theta+1$	$\theta+2$	2θ	$2\theta+1$	$2\theta+2$
2	0	2	1	θ	$\theta+1$	$2\theta+1$	2θ	$\theta+2$	$2\theta+2$
θ	0	θ	2θ	$\theta+2$	2	$\theta+1$	$2\theta+1$	$2\theta+2$	1
$\theta+1$	0	$\theta+1$	$2\theta+2$	2	$\theta+1$	2θ	1	θ	$\theta+2$
$\theta+2$	0	$\theta+2$	$2\theta+1$	$2\theta+2$	θ	2	$\theta+1$	1	2θ
2θ	0	2θ	θ	$2\theta+1$	1	$2\theta+2$	$\theta+2$	$\theta+1$	2
$2\theta+1$	0	$2\theta+1$	$\theta+2$	$\theta+1$	2θ	1	$2\theta+2$	2	θ
$2\theta+2$	0	$2\theta+2$	$\theta+1$	1	$\theta+2$	θ	2	2θ	$2\theta+1$

Dat dit een bijnalichaam is kan worden nagegaan door de axioma's te controleren voor elke combinatie van elementen in K. Verderop zal een algemene manier worden gevonden om een bijnalichaam te construeren, waarin bovenstaand bijnalichaam verkregen wordt en daarmee wordt aangetoond dat het bovenstaande een bijnalichaam is.

Nieuwe vermenigvuldiging

De bovenstaande constructie voor een bijnalichaam met 9 elementen is echter heel specifiek, en we willen liever een nieuwe vermenigvuldiging zoeken waarmee alle (eventueel alleen eindige) bijnalichamen te construeren zijn.

Neem een lichaam $\mathbb{F}_{q^2} = \mathbb{F}_q(j)$ met q oneven. Kies een $d \in \mathbb{F}_q \neq \square$. Schrijf $\mathbb{F}_{q^2} = \mathbb{F}_q(j)$ met $j^2 = d$. We zoeken nu een nieuwe vermenigvuldiging

$$* : \mathbb{F}_{q^2} \times \mathbb{F}_{q^2} \longrightarrow \mathbb{F}_{q^2}$$

met de kern $K(\mathbb{F}_{q^2}, *) = (\mathbb{F}_q, \cdot)$, zodanig dat $(\mathbb{F}_{q^2}, *, +)$ een eigenlijk bijnalichaam is.

Stel dat $\chi : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ gegeven is. Probeer dan

$$(a + bj) * (c + dj) = ac + \chi(ab)bdj^2 + (bc + \chi(ab)ad)j \tag{3.2}$$

waarbij $a + bj$ en $c + dj$ elementen zijn van $\mathbb{F}_{q^2}$, met $a, b, c, d \in \mathbb{F}_q$.

Voorbeeld: Kies $q = 3$ en

$$\begin{aligned} \chi(0) &= 1 \\ \chi(1) &= -1 \\ \chi(2) &= 1 \end{aligned}$$

Met deze keuze is $(\mathbb{F}_9, *, +)$ inderdaad een eigenlijk linksbijnalichaam.

Ter illustratie geven we voor dit voorbeeld $q = 3$ en de genoemde χ enkele vermenigvuldigingen

$$j * j = -1 \tag{3.3}$$
$$j * (1 + j) = -1 + j \tag{3.4}$$
$$(1 + j) * j = 1 - j \tag{3.5}$$
$$(1 + j) * (1 + j) = 2 \tag{3.6}$$

Uit (3.3) volgt dat $j^2 = j * j = -1$. Uit (3.4) en (3.5) volgt dat er niet aan de commutativiteit van de vermenigvuldiging wordt voldaan, en uit (3.6) volgt dat de rechtsdistributieve wet niet opgaat. Dat aan de associativiteit wordt voldaan kan worden nagerekend [5]. De multiplicatieve inverse bestaat (voor bovenstaand voorbeeld met $q = 3$):

$$(a + bj) * (\frac{a - \chi(ab)bj}{a^2 + b^2}) = (\frac{a - \chi(ab)bj}{a^2 + b^2}) * (a + bj) = 1 = e$$

(multiplicatieve identiteit), en $a^2 + b^2 = 0$ dan en slechts dan als $a \equiv b \equiv 0$.

De afbeelding χ

Nu willen we onderzoeken, welke eigenschappen χ heeft, als inderdaad de constructie (3.2) een bijnalichaam oplevert. $(\mathbb{F}_9, *, 0, 1)$ is met behulp van zo een χ te beschrijven. In de volgende sectie ga ik proberen of dit ook meer algemeen lukt voor $\mathbb{F}_{q^2} = \mathbb{F}_q(j)$. In de keuze van de constructie (3.2) zou de linksdistributieve wet wel moeten gelden, en de rechtsdistributieve wet niet, met een keuze van de $j^2 \neq \square \in \mathbb{F}_q$.

Allereerst proberen we een vermenigvuldiging uit te werken met de rechtsdistributieve wet. Volgens formule (3.2) geldt:

$$(a + bj) * (c + dj) = ac + \chi(ab)bdj^2 + (bc + \chi(ab)ad)j$$

Volgens de rechtsdistributieve wet, respectievelijk stellend $b = 0$ en $a = 0$ geldt:

$$\begin{aligned}(a + bj) * (c + dj) &= a * (c + dj) + bj * (c + dj)\\ &= a * (c + dj) + \chi(0)bdj^2 + bcj\\ &= ac + \chi(0)adj + \chi(0)bdj^2 + bcj\end{aligned}$$

Op de basis $\{1, j\}$ van $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$ levert dit

$$\begin{aligned}ac + \chi(ab)bdj^2 &= ac + \chi(0)bdj^2\\ bdj^2(\chi(ab) - \chi(0)) &= 0\\ &\forall\, a, b, d, \in \mathbb{F}_q\end{aligned}$$

en

$$\begin{aligned}bc + \chi(ab)ad &= bc + \chi(0)ad\\ ad(\chi(ab) - \chi(0)) &= 0\\ &\forall\, a, b, d \in \mathbb{F}_q\end{aligned}$$

Dit zou impliceren dat χ constant is. Gezien dit een linksbijnalichaam moet opleveren, kan hieruit de conclusie getrokken worden dat de afbeelding χ niet constant mag zijn, omdat de rechtsdistributieve wet dan wel zou gelden.

Nu proberen we het uit te werken met de linksdistributieve wet. Volgens formule (3.2) geldt

$$(a + bj) * (c + dj) = ac + \chi(ab)bdj^2 + (bc + \chi(ab)ad)j$$

En volgens de linksdistributieve wet geldt

$$\begin{aligned}(a + bj) * (c + dj) &= (a + bj) * c + (a + bj) * dj\\ &= ac + bcj + \chi(ab)bdj^j + ad\chi(ab)j\end{aligned}$$

Op de basis $\{1, j\}$ van $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$ levert dit

$$\begin{aligned}ac + \chi(ab)bdj^2 &= ac + \chi(ab)bdj^2\\ bc + ad\chi(ab) &= bc + ad\chi(ab)\end{aligned}$$

Conclusie: de constructie (3.2) voldoet aan de linksdistributieve wet zonder dat er eisen aan χ worden opgelegd. Ten tweede kan de afbeelding χ niet constant zijn, omdat dan aan beide distributieve wetten wordt voldaan, en dan is $\mathbb{F}_{q^2}$ geen eigenlijk bijnalichaam.

Vervolgens proberen we een eis te stellen aan $\chi(0)$. Hiervoor moet zijn $a = 0$ of $b = 0$ of beide. In het laatste geval is het product altijd nul. Kies $a = 0$

$$\begin{aligned} bj * (c + dj) &= \chi(0)bdj^2 + bcj \\ (c + dj) * bj &= \chi(cd)bdj^2 + \chi(cd)bcj \end{aligned}$$

Kies nu $b = 1$, $c = 1$ en $d = 0$, dan staat in bovenstaande formule $j * 1$ en $1 * j$, en dit moet gelijk zijn

$$\begin{aligned} j * 1 &= 1 * j \\ j &= \chi(0)j \end{aligned}$$

En dit impliceert $\chi(0) = 1$.

We proberen de volgende afbeelding voor χ:

$$\begin{aligned} \chi(0) &= 1 \\ \chi(a) &= -a^{\frac{q-1}{2}} \end{aligned}$$

Omdat $\mathbb{F}_q^*$ een cyclische groep is met $q - 1$ elementen, zijn er a met $\chi(a) \neq 1$. Bijvoorbeeld: een voortbrenger van $\mathbb{F}_q^*$ heeft orde $q - 1$, dus $a^{(q-1)/2} \neq 1$. χ is dus niet constant, en voor $a \neq 0$ geldt $(\chi(a))^2 = (-a^{(q-1)/2})^2 = a^{q-1} = 1$, dus $\chi(a) \in \{-1, 1\}$. Merk op dat voor $q = 3$ dit precies het voorbeeld oplevert dat we al eerder gaven. Het zou goed kunnen dat het ook werkt voor $q = 5$, of voor iedere q. Dit heb ik niet verder onderzocht.

Het blijkt lastig om aanvullende eisen aan χ te stellen, omdat de uitwerking van andere axioma's ofwel heel er ingewikkeld zijn, of geen eisen aan χ opleggen. Wellicht is het op deze manier niet mogelijk een algemene manier te vinden om een bijnalichaam te construeren.

3.2 Een algemene manier om een bijnalichaam te construeren

In 3.1 werd een bijnalichaam verkregen uit een lichaam door de vermenigvuldiging te vervangen. Er is ook een algemene formule voor deze constructie, die werkt voor bijnalichamen $\mathbb{F} = (F, \cdot, +)$. $Z(\mathbb{F})$ is het centrum is en $K(\mathbb{F})$ de kern. Het bijnalichaam heeft q^n elementen, $Z(\mathbb{F}) = K(\mathbb{F})$ heeft q elementen, en n is de dimensie van de vectorruimte over de kern. Hiervoor is de volgende stelling nodig, waarbij twee voorwaarden worden gesteld waar q en n aan moeten voldoen.

Zij $q = p^l$ met p priem en $l \in \mathbb{N}$, en n zodanig dat

$$\begin{cases} \forall\, \pi \text{ priem} & \text{als } \pi \mid n \text{ dan } \pi \mid q - 1 \\ \text{en} & \text{als } 4 \mid n \text{ dan } 4 \mid q - 1 \end{cases}$$

Dan zijn

$$\{\frac{(q^i-1)}{(q-1)}; 0 < i \leq n\}$$

alle restklassen modulo n. Het bewijs van deze stelling staat even verderop.

De eenhedengroep $\mathbb{F}_{q^n}^* =< \omega >$ is een cyclische groep met $q^n - 1$ elementen. Nu ga ik gebruiken dat $n \mid q^n - 1$, wat zal volgen uit het bewijs van bovenstaande stelling. Neem $< \omega^n > \subset \mathbb{F}_{q^n}^* =< \omega >$, hetgeen een ondergroep van $\mathbb{F}_{q^n}^*$ is met $(q^n - 1)/n$ elementen. Neem $\mathbb{F}_{q^n}^* / < \omega^n >$, en de elementen hiervan zijn $\lambda \cdot < \omega^n > = \omega^a \cdot < \omega^n >$, waarbij $\lambda \in \mathbb{F}_q^*$.Twee elementen hiervan zijn gelijk: $\omega^a \cdot < \omega^n > = \omega^b \cdot < \omega^n >$ dan en slechts dan als $\omega^{b-a} \in < \omega^n >$, dus $a \equiv b \bmod n$. Dus ieder element van $\mathbb{F}_{q^n}^* / < \omega^n >$ is te schrijven als

$$\omega^{\frac{q^i-1}{q-1}} \cdot < \omega^n >$$

voor precies een i uit $0 < i \leq n$. Gegeven $a \in \mathbb{F}_{q^n}^*$. Schrijf $a \cdot < \omega^n > = \omega^{\frac{q^i-1}{q-1}} \cdot < \omega^n >$ voor een (unieke) i met $0 < i \leq n$. Definieer nu een automorfisme van $\mathbb{F}_{q^n}^*$:

$$\psi_a(b) = b^{q^i}$$

Definieer op de verzameling $\mathbb{F}_{q^n}$ de nieuwe vermenigvuldiging

$$a * b = \begin{cases} 0 & \text{als } a = 0 \\ a \cdot \psi_a(b) & \text{als } a \neq 0 \end{cases}$$

De verzameling $F = \mathbb{F}_{q^n}$ met de optelling van het eindige lichaam $\mathbb{F}_{q^n}$ en de nieuwe vermenigvuldiging $*$ is een bijnalichaam $\mathbb{F} = (F, *, +)$. Bovenstaande bijnalichamen worden Dicksonse genoemd. Volgens [3] zijn op zeven uitzonderingen na alle eindige bijnalichamen ofwel Dicksons, ofwel lichamen.

Bewijs van de gebruikte stelling

Wat we nog willen bewijzen, is dat

$$\{\frac{(q^i-1)}{(q-1)}; 0 < i \leq n\}$$
$$= \{1, \frac{q^2-1}{q-1}, \frac{q^3-1}{q-1}, \ldots, \frac{q^n-1}{q-1}\}$$

een volledig representantensysteem modulo n vormt, met de volgende restricties op de keuze van q en n Zij $q = p^l$ met p priem en $l \in \mathbb{N}$, en n zodanig dat

$$\begin{cases} \forall\, \pi \text{ priem} & \text{als } \pi \mid n \text{ dan } \pi \mid q-1 \\ \text{en} & \text{als } 4 \mid n \text{ dan } 4 \mid q-1 \end{cases}$$

en $\frac{q^n-1}{q-1} \equiv 0 \bmod n$.

Voor het bewijs ga ik een aantal stellingen gebruiken.

Neem $a \in \mathbb{N}$, met u een priemdeler van $a-1$. Allereerst kijken we naar de hoogste macht van u die a^n-1 deelt, met $n \in \mathbb{N}$. Een ondergrens voor u volgt uit de volgende stelling.

(Stelling 2) Als $u^A \mid a-1$ en $u^B \mid n$ dan $u^{A+B} \mid a^n-1$, met $A, B \in \mathbb{N}$.

Bewijs: Schrijf $n = u^B\delta$ met $\delta \in \mathbb{N}$, waarbij de grootste gemene deler $ggd(u,\delta) = 1$. Nu gaan we inductie naar B toepassen. Omdat $(a-1)$ een factor is van a^n-1, is het gewenste resultaat waar voor $B=0$. Neem aan dat $u^{A+B} \parallel a^n-1$ wanneer $B=b$. Neem $B=b+1$ met:

$$a^{u^{b+1}\delta} - 1 = (a^{u^b\delta} - 1)\sum_{i=0}^{u-1} a^{u^b\delta i}$$

En volgens de aanname bij de inductie is de term $(a^{u^b\delta}-1)$ deelbaar door u^{A+B} en de som is $\sum_{i=0}^{u-1} a^{u^b\delta i} \equiv u(\bmod u)$ omdat elk van de u termen die er in zitten gelijk is aan $1(\bmod u)$. Dus de linkerkant van de vergelijking hierboven is deelbaar door u^{A+B} wanneer $B = b+1$, waarmee het bewijs rond is.

In het bijzondere geval dat $\gcd(n,u) = 1$, is bovenstaande ondergrens de precieze waarde voor de hoogste macht van u die a^n-1 deelt. De volgende stelling ga ik verderop ook gebruiken.

(Stelling 3) Stel $2 \parallel a-1$, en schrijf $n = 2^\beta\delta$ met $\beta, \delta \in \mathbb{N}$, zodat δ oneven is. Dan geldt voor $\beta \geq 1$:

$$a^n - 1 \equiv 0(\bmod 2^{\beta+2})$$

*Bewijs:*Als $\beta = 1$ dan is

$$a^n - 1 = (a^{\frac{\delta}{2}} - 1)(a^{\frac{n}{2}} + 1) \equiv 0(\bmod 8)$$

zoals vereist. Het algemene geval volgt uit inductie naar β: neem aan dat het waar is wanneer $2^\beta \parallel n$, en beschouw het geval dat $n = 2^{2^{\beta+1}\delta}$ met δ oneven.

$$a^{2^{\beta+1}\delta} - 1 = (a^{2^\beta\delta} - 1)(a^{2^\beta\delta} + 1) \equiv 0(\bmod\ 2^{\beta+2}2)$$

Waarmee het is bewezen.

Dus, in het geval dat $u = 2$ en $\alpha = 1$, is $u^{\alpha+\beta+1}$ een deler van $a^n - 1$, waar $u^\beta \parallel n$. Hierna is ook $\alpha \in \mathbb{N}$.

(Stelling 4) Stel dat er een geheel getal $\beta \geq 0$ is zodanig dat

$$a^{u^\beta} - 1 \not\equiv 0(\bmod u^{\alpha+\beta+1}) \tag{3.7}$$

$$a^{u^{\beta+1}} - 1 \equiv 0(\bmod u^{\alpha+\beta+2}) \tag{3.8}$$

Dan is $\beta = 0$ en $u^\alpha = 2$.

Bewijs: Schijf

$$a^{u^{\beta+1}} - 1 = (a^{u^\beta} - 1)(\sum_{i=0}^{u-1} a^{u^\beta i})$$

dan hebben we volgens (3.8):

$$(a^{u^\beta} - 1)(\sum_{i=0}^{u-1} a^{u^\beta i} \equiv 0(\text{mod } u^{a+\beta+2})$$

En omdat volgens stelling 2 en (3.7) geldt:

$$a^{\alpha+\beta} \mid a^{u^\beta} - 1$$

hebben we nu

$$\sum_{i=0}^{u-1} a^{u^\beta i} \equiv 0(\text{mod}\, u^2) \tag{3.9}$$

en volgens stelling 2 geld voor elke i:

$$a^{u^\beta i} \equiv 1(\text{mod } u^{\alpha+\beta} \tag{3.10}$$

en in het bijzonder: Als $\alpha + \beta \geq 2$ dan $a^{u^\beta i} \equiv 1(\text{mod}\, u^2)$. In combinatie met (3.9) volgt:

$$Als\, \alpha + \beta \geq 2, dan\, u \equiv 0(\text{mod}\, u^2) \tag{3.11}$$

En dat is een tegenspraak, tenzij $\alpha + \beta \leq 1$. Maar de aanname was $u \mid a - 1$, dus we moeten hebben $a = 1$ en $\beta = 0$, en (3.7) blijft gelden. Met de aanname dat $u^\alpha > 2$ hebben we nu ook dat $u^\alpha = u$ is een oneven priemdeler van $a - 1$, en (3.8) verandert in

$$a^u - 1 \equiv 0(\text{mod}\, u^3) \tag{3.12}$$

En als je daar op toepast dat $u^\alpha = u$ een oneven priemdeler van $a - 1$ is, krijg je

$$\sum_{i=0}^{u-1} a^i \equiv 0(\text{mod}\, u^2) \tag{3.13}$$

Bovendien geldt

$$\begin{aligned}\sum_{i=0}^{u-1} a^i &= u + \sum_{i=1}^{u-1}(a^i - 1) \\ &= u + (a-1)\sum_{i=1}^{u-1}\sum_{j=1}^{i-1} a^j\end{aligned}$$

En omdat $a-1 \equiv 0(\mathrm{mod}\, u)$ en $a^j \equiv 1(\mathrm{mod}\, u)$ hebben we ook $(a-1)a^j \equiv (a-1)\ 1\ (\mathrm{mod}\ u^2)$. Dus

$$\begin{aligned}\sum_{i=0}^{u-1} a^i &\equiv u + \sum_{i=0}^{u-1} i (\mathrm{mod}\, u^2) \\ &\equiv u + (a-1)\frac{u(u-1)}{2} (\mathrm{mod}\, u^2)\end{aligned}$$

En gezien de linkerkant van bovenstaande vergelijking $0(\mathrm{mod}\, u^2)$ is, hebben we volgens vergelijking (3.13)

$$1 + \frac{(a-1)(u-1)}{2} (\mathrm{mod}\, u)$$

maar omdat het priemgetal u een oneven deler is van $a-1$, is er een tegenspraak. De combinatie van dit verhaal en stelling 3 geeft:

(Stelling 5) Voor $u^a > 2$,is $u^{a+\beta}$ de hoogste macht van u die $a^n - 1$ deelt.

(Stelling 6) Uit stelling 3 en stelling 4 volgt de volgende stelling. Neem $a > 1$ en $n \geq 1$ gehele getallen en u is een priemdeler van $a-1$ zodanig dat $u^\alpha \parallel a-1$ en $u^\beta \parallel n$. Als $u^a > 2$ of $\beta = 0$, dan geldt $u^{\alpha+\beta} \parallel a^n - 1$. Als $u^\alpha = 2$ en $\beta \geq 1$ dan geldt $u^{\alpha+\beta+1} \mid a^n - 1$.

Het volgende doel is om bovenstaande stelling toe te passen om te laten zien dat $a^k - 1/a - 1$ alle restklassen modulo n bij langs gaat, wanneer k wordt gevarieerd.

(Stelling 7) Neem $a > 1$ en $N > 1$ zodanig dat

$$\begin{cases} \forall\, \pi \,\text{priem} & \text{als } \pi \mid N \text{ dan } \pi \mid a-1 \\ \text{en} & \text{als } 4 \mid n \text{ dan } 4 \mid a-1 \end{cases}$$

Dan is $a^N - 1 \not\equiv 0(\mathrm{mod}\, N(a-1))$ voor $1 \leq n < N$.

Bewijs: We willen een tegenspraak krijgen, dus stel dat voor een $n \in \{1, \ldots, N-1\}$ geldt:

$$a^n - 1 \equiv 0(\mathrm{mod}(N(a-1)) \tag{3.14}$$

Omdat $n < N$, is er ten minste één priemdeler u van N zodanig dat voor een $b \geq 0$, $u^b \parallel n$ en $u^{b+1} \parallel N$. Volgens stelling 6 is $a^n - 1$ deelbaar door $u^{\alpha+\beta}$, en dit is hoogste macht van u die $a^n - 1$ deelt, tenzij $u^\alpha = 2$. Dus voor $u^\alpha > 2$, $u^{a+b} \parallel a^n - 1$ in tegenspraak met (3.14). Dus in het vervolg mogen we aannemen dat $u^\alpha = 2$, dus 2^{b+1} deelt N, en dit is in tegenspraak met de aanname dat $N \not\equiv 0(\mathrm{mod}\, 4)$, wanneer $2 \parallel a-1$, tenzij $b = 0$. Maar in dat geval impliceert stelling 6 nog steeds dat $u^{a+b} \parallel a^n - 1$, wat weer (3.14) tegenspreekt.

Nu is bewezen dat $a^k - 1/a - 1$ de restklassen modulo n afgaat, als k de getallen $1 \ldots n$ afgaat. Het enige wat nog te bewijzen valt, is dat de termen uniek zijn.

(Stelling 8)

$$\{\frac{(a^i-1)}{(a-1)}; 0 < i \leq n\}$$
$$= 1, \frac{a^2-1}{a-1}, \frac{a^3-1}{a-1}, \ldots, \frac{a^n-1}{a-1}$$

een volledig representantensysteem modulo n vormt, met onze restricties op de keuze van a en n: Zij $a = p^l$ met p priem en $l \in \mathbb{N}$, en n zodanig dat

$$\begin{cases} \forall\, \pi \,\text{priem} & \text{als } \pi \mid n \text{ dan } \pi \mid a-1 \\ \text{en} & \text{als } 4 \mid n \text{ dan } 4 \mid a-1 \end{cases}$$

en $\frac{a^n-1}{a-1} \equiv 0 \bmod n$.

De tweede voorwaarde anders opgeschreven is: Als $a \equiv 3 (\mathrm{mod}\, 4)$ dan $N \not\equiv 0 \pmod 4$. Dan is $a^N - 1 \not\equiv 0 (\mathrm{mod}\, N(a-1))$ voor $1 \leq n < N$. Om een tegenspraak te creëren nemen we aan dat twee verschillende termen gelijk zijn.

Bewijs: Stel twee verschillende termen zijn gelijk modulo n: $j > i$ met

$$\frac{a^j-1}{a-1} \equiv \frac{a^i-1}{a-1} (\mathrm{mod}\, n)$$
$$\Rightarrow a^i \frac{a^{j-i}-1}{a-1} \equiv 0 (\mathrm{mod}\, n)$$
$$\Rightarrow \frac{a^{j-i}-1}{a-1} \equiv 0 (\mathrm{mod}\, n)$$

Dit is in tegenspraak met stelling 7. Dus elke van de n termen is een verschillend residu modulo n. Bovendien geldt $a^n - 1/a - 1 \equiv 0 (\mathrm{mod}\, n)$, en dat volgt direct uit stelling 6.

3.3 Toepassing van de methode

Als voorbeeld zal ik de methode toepassen voor $q = 3 = 3^1$ en $n = 2$ om het voorbeeld uit 3.1 te krijgen. Alle priemgetallen die $n = 2$ delen: $\{2\}$, delen ook $q - 1 = 2$, en 4 is geen deler van n.

$$\{\frac{(q^i-1)}{(q-1)}; 0 \leq i < n\}$$
$$= \{0, 1\}$$

Is het representantensysteem modulo 2. $\mathbb{F}^*_{q^n} = \{1, 2, \theta, \theta+1, \theta+2, 2\theta, 2\theta+1, 2\theta+2\} =< \omega >$. En de ondergroep $< \omega^n > \subset < \omega >$ is $< \omega^2 > = \{1, 2, \theta+2, 2\theta+1\}$. Deze heeft inderdaad $\frac{q^n-1}{n} = \frac{3^2-1}{2} = 4$ elementen. $\mathbb{F}^*_{q^n} / < \omega^n > = \lambda \cdot < \omega^n > = \{1, 2, \theta+2, 2\theta+1\}$. Dit zijn ook de elementen die in het voorbeeld van het lichaam met 9 elementen in (3.1) een kwadraat zijn. Nu definieren we het automorfisme van $\mathbb{F}^*_{3^2}$

$$\psi_b(a) = \begin{cases} a & \text{als } b \in < \omega^2 > = \{1, 2, \theta+2, 2\theta+1\} \\ a^3 & \text{als } b \in \omega \cdot < \omega^2 > = \{\theta, \theta+1, 2\theta, 2\theta+2\} \end{cases}$$

Hiermee is precies het voorbeeld van een bijnalichaam met 9 elementen uit (3.1) verkregen.

Hoofdstuk 4

Classificatie van bijnalichamen

Op zeven eindige uitzonderingen na, zijn alle tot nu toe bekende constructies van bijnalichamen Dicksons (er bestaan dus ook oneindige Dicksonse bijnalichamen, waar ik in deze scriptie echter niet op in ga). Het blijkt moeilijk om de Dicksonse bijnalichamen te kenmerken, en dat is ook maar voor een paar klassen gebeurd. Hans Julius Zassenhaus (1912-1991) heeft voor eindige bijnalichamen een classificatie gemaakt, het zgn. *Zassenhauscriterium*, maar voor het oneindige geval is zo'n criterium niet bekend. Susan Dancs heeft in 1976 het Zassenhauscriterium veralgemeniseerd voor lokaal eindige bijnalichamen. Alle eindige bijnalichamen zijn ofwel Dicksons, ofwel isomorf aan een van de zeven uitzonderingsbijnalichamen.

4.1 Eenheidswortels en cirkeldelingspolynomen

In de classificatie van eindige bijnalichamen zijn cirkeldelingspolynomen benodigd. Hier volgen enkele definities en de belangrijkste stellingen over eenheidswortels en cirkeldelingspolynomen, uit [6] en [7].

Een *n-eenheidswortel* of een *De Moivre getal* is een complex getal z dat een oplossing is van de vergelijking $z^n - 1 = 0$, $n \in \mathbb{N}$.

De vergelijking $z^n - 1 = 0$ heeft precies n oplossingen (volgens de hoofdstelling van de algebra), die allemaal op de eenheidscirkel in het complexe vlak liggen. De verzameling van alle n-eenheidswortels wordt aangeduid met μ_n en vormt een multiplicatieve cyclische groep. De *orde* of *exponent* van een n-eenheidswortel $z \in \mathbb{C}$ is het kleinste positieve gehele getal m zodanig dat $z^m = 1$

Een n-eenheidswortel heet *primitief* als zijn orde n is, d.w.z. z is een primitieve eenheidswortel als $z^k \neq 1$ voor $k = 1, 2, \ldots n-1$.

Voor $b \neq 0$ in een lichaam K, is de *exponent* van b het kleinste positieve gehele getal n zodanig dat $b^n = 1$, indien er zo een n bestaat (de orde van b in de groep $U(K)$). Dus, b is een nulpunt van $x^n - 1$ maar niet van $x^d - 1$ voor

$d < n$. Nu worden er polynomen $\Phi_n(x) \in \mathbb{Z}[x]$ geconstrueerd, zodanig dat

$$\Phi_n(b) = 0 \tag{4.1}$$

dan en slechts dan als b exponent n heeft, $b \in \mathbb{C}$. De polynomen Φ_n zijn de *cirkeldelings-* of *cyclotomische polynomen.*

$$\Phi_n(x) = \prod_{k=1}^{\phi(n)} (x - x_k) \tag{4.2}$$

met $\phi(n)$ de Euler fucntie

$$\phi(n) = n \prod_{p|n} (1 - \frac{1}{p})$$

en x_k de primitieve eenheidswortels in $\mathbb{C}$.

Met bovenstaande defenitie kan een alternatieve, inductieve definitie worden gegeven

$$\begin{aligned} \Phi_1(x) &= x - 1 \\ \Phi_n(x) &= \frac{x^n - 1}{\prod_{d|n, d \neq n} \Phi_d(x)} \\ n &= 1, 2, \ldots \end{aligned}$$

Eigenschappen van cirkeldelingspolynomen

Stelling: Als $n \in \mathbb{N}$, dan is

$$x^n - 1 = \prod_{d|n} \Phi_d(x) \tag{4.3}$$

en de graad van $\Phi_d(x)$ is $\phi(d)$.

Bewijs: de nulpunten van $x^n - 1$ zijn precies de n-eenheidswortels. Andersom, als z een nulpunt is van orde d, dan is z een primitieve d-eenheidswortel, dus een nulpunt van $\Phi_d(x)$. Omdat $d \mid n$, is het ook een nulpunt van het product aan de rechterkant. De linker en rechterkant van (4.3) hebben gelijke nulpunten, en ze zijn beide monisch, dus ze zijn gelijk.

Stelling: $\Phi_n(x)$ is een monisch polynoom met gehele coëfficienten.

Bewijs: Een bewijs door middel van inductie. $\Phi_1(x) = x - 1$. Neem aan dat het resultaat waar is voor alle $d < n$ en bewijs voor n. Volgens de aanname hebben we:

$$F(X) = \prod_{d<n, d|n} \Phi_d(x) \in \mathbb{Z}[X]$$

en de kopcoëfficiënt is 1. Omdat $F(x)$ monisch is, bestaat er (via deling met rest) een $h(x), r(x) \in \mathbb{Z}[X]$ zodanig dat $h(x)$ monisch is en $x^n - 1 = F(x)h(x) +$

$r(x)$, waarbij $r(x) = 0$ of $graad(r(x)) < graad(F(x))$. Maar we hadden $x^n - 1 = F(x)\Phi_n(x)$, dus vanwege de uniciteit van het quotiënt en de rest in $\mathbb{C}[X]$, moet het zijn $h(x) = \Phi_n(x)$, dus $\Phi_n(x)$ heeft kopcoëfficiënt 1.

Volgens het *Lemma van Gauss* is een monisch polynoom $f(x)$ met gehele coëfficienten dat irreducibel is in $\mathbb{Z}$ - er zijn geen polynomen g, h met gehele coëfficienten zodanig dat $f(x) = g(x)h(x)$ - ook irreducibel in $\mathbb{Q}$. Als f en g monische polynomen met gehele coëfficienten zijn zodanig dat $g \mid f$ over $\mathbb{Q}$, dan bestaat er een polynoom h met rationele coëfficienten zodanig dat $f(x) = g(x)h(x)$, waarbij ofwel $g \mid f$ over $\mathbb{Z}$, ofwel h heeft alleen gehele coëfficienten. Dus de vergelijking

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n, d\neq n} \Phi_d(x)}$$

levert alleen polynomen op met gehele coëfficienten, dus $\Phi_n(x)$ heeft gehele coëfficienten.

4.2 Classificatie van eindige bijnalichamen

In tegenstelling tot lichamen, zijn bijnalichamen van gelijke orde en rang niet noodzakelijk isomorf. Een eindig Dicksons bijnalichaam $\mathbb{F}_{q^n}$ heeft een centrum met een priemmacht q elementen, en dimensie n over het centrum. Voor de keuze van q en n moet voor iedere priem p en $p = 4$ gelden dat $p \mid n$ impliceert $p \mid q - 1$. Voor iedere $\mathbb{F}_{q^n}$ met priemlichaam $\mathbb{F}_p$ kan een monische, irreducibele factor μ van het n-de cirkeldelingspolynoom $\Phi_n \in \mathbb{F}_p[x]$ gevonden worden. Het isomorfietype van het eindige Dicksonse bijnalichaam wordt door (q, n, μ) vastgelegd. Het bewijs hiervoor is te vinden in [3].

In ons voorbeeld van het bijnalichaam met 9 elementen is $q = 3$ en $n = 2$. We zoeken het tweede cirkeldelingspolynoom over $\mathbb{F}_p$, waarbij p de priemfactor van q is en in dit geval gelijk is aan q. $q = p = 3$, dus we zoeken Φ_2 over $\mathbb{F}_3$: $\Phi_2 = X + 1$, $\mu = X + 1$. Er bestaat dus op isomorfie na maar één bijnalichaam met 9 elementen. Iedere twee bijnalichamen met dimensie 2 over het centrum zijn isomorf.

Een ander voorbeeld is $\mathbb{F}_{7^3}$ waarbij $q = 7$ en $n = 3$. Dit is het kleinste bijnalichaam met dimensie 3 over de kern. Het cirkeldelingspolynoom is $\Phi_3 = x^2 + x + 1$, en over $\mathbb{F}_7$ heeft het de factoren $\mu = x - 2$ en $\mu = x - 4$, dus er zijn twee isomorfietypen van bijnalichamen met 343 elementen, vastgelegd door $(7, 3, x - 2)$ en $(7, 3, x - 4)$.

Voor bovenstaand voorbeeld is het representantensysteem modulo 3 is

$$\{\frac{(q^i - 1)}{(q - 1)}; 0 < i \leq n\}$$
$$= \{0, 1, 2\}$$

We nemen het lichaam $\mathbb{F}_{q^n}$ en gaan hiervoor de nieuwe vermenigvuldiging construeren zodat het een bijnalichaam wordt. $\mathbb{F}^*_{q^n} =< \omega >$. De ondergroep $<$

$\omega^n > \subset < \omega >$ is $< \omega^3 >$. $\mathbb{F}_{7^3}^{*3}$ heeft $\frac{q^n-1}{n} = \frac{7^3-1}{3} = 114 = 3 \cdot 2 \cdot 19$ elementen, een het aantal voortbrengers is $2 \cdot 18 = 36$. $\mathbb{F}_{q^n}^* / < \omega^n > = \{\lambda \cdot < \omega^n > | \ \lambda \in \mathbb{F}_{q^n}^*\}$. We kunnen kiezen voor ω een nulpunt van $x^3 + 6x^2 + 4 \in \mathbb{F}_7[x]$, $\mathbb{F}_7(\omega) = \mathbb{F}_{7^3}$ en de orde van ω is 342. Net als in hoofdstuk 3 definieren we het automorfisme ψ met ω:

$$\psi_b(a) = \begin{cases} a & \text{als } b \in < \omega^3 > \\ a^7 & \text{als } b \in \omega \cdot < \omega^3 > \\ a^{49} & \text{als } b \in \omega^2 \cdot < \omega^3 > \end{cases}$$

Een andere voortbrenger van $\mathbb{F}_{7^3}^*$ is $v = \omega^{-1}$, waarmee we $\overline{\psi}$ definiëren:

$$\overline{\psi}_b(a) = \begin{cases} a & \text{als } b \in < v^3 > \\ a^7 & \text{als } b \in v^2 \cdot < v^3 > \\ a^{49} & \text{als } b \in v \cdot < v^3 > \end{cases}$$

De vraag is nu: hoe vind je bij een gegeven bijnalichaam de eenheidswortel? Volgens de manier waarop Dicksonse bijnalichamen geconstrueerd worden, hangt het isomorfietype af van de keuze van de voortbrenger ω. Neem $m = \frac{q^n-1}{n}$, en neem ω^m. Het polynoom μ is dan gedefinieerd als het minimumpolynoom van ω^m over $\mathbb{F}_q$.

In het voorbeeld van $\mathbb{F}_{7^3}$ gaat het als volgt: $\mathbb{F}_{7^3}^*$ heeft 342 elementen, dus $m = 114$. Kies een voortbrenger ω, en $\omega^{114} = 2$. Het minimumpolynoom van deze is $x^3 + 6x + 4$. Het minimumpolynoom van $\omega^m = 2$ is $x - 2$. Definieer $v = \omega^{-1}$, en heeft als minimumpolynoom $x^3 + 5x + 2$. Het minimumpolynoom van $v^m = 4$ is $x - 4$. Nu is duidelijk welke μ bij welk bijnalichaam hoort: het bijnalichaam met als voortbrenger het nulpunt van x^3+6x+4 wordt vastgelegd door $(7, 3, x - 2)$.

We nemen een nog veel groter voorbeeld: $(q, n) = (13, 36)$. Met behulp van het computerprogramma *Magma* (de code staat hieronder), zoeken we een voortbrenger ω van $\mathbb{F}_{13^{36}}^*$ met orde $13^{36} - 1$. Het minimumpolynoom van de eerstgevonden ω waarvoor dat geldt, is: $x^{36} + 8x^{35} + x^{33} + 9x^{32} + 3x^{31} + 9x^{29} + 5x^{28} + 11x^{27} + x^{25} + 4x^{24} + 10x^{23} + 8x^{22} + 2x^{21} + 7x^{20} + 2x^{19} + x^{18} + 3x^{17} + 2x^{15} + 11x^{14} + 6x^{13} + x^{12} + 5x^{11} + 9x^{10} + 9x^9 + 8x^8 + 2x^7 + 6x^6 + 2x^5 + 2x^4 + 2x^3 + 2x^2 + 6x + 6$. Nu nemen we $m = \frac{13^{36}-1}{36} = 351283848686954088451930252248929344740$ en het minimumpolynoom van ω^m is $x^3 + 7$. Een andere voortbrenger is ω^{11}, en deze tot de macht m heeft als minimumpolynoom $x^3 + 2$. Op dezelfde manier levert ω^{29} het polynoom $x^3 + 11$, en de inverse van deze levert $x^3 + 6$. Dit zijn precies de factoren van $\Phi_{36} \in \mathbb{F}_{13}[x]$.

Magma code

```
> F<w>:=GF(7^3);
> Order(w);
```

```
342
> m:=(7^3-1)/3;
> w^114;
2
> MinimalPolynomial(w);
$.1^3 + 6*$.1^2 + 4
> v:=w^(-1);
> v^114;
4
> MinimalPolynomial(v);
$.1^3 + 5*$.1 + 2
> F<w>:=GF(13^36);
> MinimalPolynomial(w);
$.1^36 + 2
> Order(w);
432
> Order(w+F!1);
3161554638182586796067372270240364102660
> Factorize(3161554638182586796067372270240364102660);

>> Factorize(3161554638182586796067372270240364102660);
   ^
User error: Identifier 'Factorize' has not been declared or assigned
> Factorization(3161554638182586796067372270240364102660);
[ <2, 2>, <3, 3>, <5, 1>, <7, 1>, <17, 1>, <19, 1>, <37, 1>, <61, 1>,
<157, 1>, <271, 1>, <937, 1>, <28393, 1>, <428041,
1>, <1471069, 1>, <1609669, 1> ]
> Factorization(13^36-1);
[ <2, 4>, <3, 3>, <5, 1>, <7, 1>, <17, 1>, <19, 1>, <37, 1>, <61, 1>,
<157, 1>, <271, 1>, <937, 1>, <28393, 1>, <428041,
1>, <1471069, 1>, <1609669, 1> ]
> w:=Random(F);13^36-1-Order(w);
11943650855356439007365628576463597721160
> w:=Random(F);13^36-1-Order(w);
0
> MinimalPolynomial(w);
$.1^36 + 8*$.1^35 + $.1^33 + 9*$.1^32 + 3*$.1^31 + 9*$.1^29 + 5*$.1^28
+ 11*$.1^27 + $.1^25 + 4*$.1^24 + 10*$.1^23 +
    8*$.1^22 + 2*$.1^21 + 7*$.1^20 + 2*$.1^19 + $.1^18 + 3*$.1^17
    + 2*$.1^15 + 11*$.1^14 + 6*$.1^13 + $.1^12 + 5*$.1^11
    + 9*$.1^10 + 9*$.1^9 + 8*$.1^8 + 2*$.1^7 + 6*$.1^6
    + 2*$.1^5 + 2*$.1^4 + 2*$.1^3 + 2*$.1^2 + 6*$.1 + 6
> (13^36-1)/36;
351283848686954088451930252248929344740
> MinimalPolynomial(w^351283848686954088451930252248929344740);
$.1^3 + 7
> v:=w^11;
> MinimalPolynomial(v^351283848686954088451930252248929344740);
$.1^3 + 2
> v:=w^13;
```

```
> MinimalPolynomial(v^351283848686954088451930252248929344740);
$.1^3 + 7
> v:=w^23;
> MinimalPolynomial(v^351283848686954088451930252248929344740);
$.1^3 + 2
> v:=w^121;
> MinimalPolynomial(v^351283848686954088451930252248929344740);
$.1^3 + 7
> v:=w^29;
> MinimalPolynomial(v^351283848686954088451930252248929344740);
$.1^3 + 11
> v:=v^(-1);
> MinimalPolynomial(v^351283848686954088451930252248929344740);
$.1^3 + 6
```

4.3 De eindige uitzonderingsbijnalichamen

Er bestaan precies zeven eindige bijnalichamen die niet Dicksons zijn [3]. Allen hebben dimensie 2 over hun priemlichaam $\mathbb{F}_p$ Hier volgt een opsomming van de zeven uitzonderingensbijnalichamen, waarna er op één voorbeeld dieper in wordt gegaan.

Allereerste worden de multiplicatieve groepen G van de uitzonderingsbijnalichamen geconstrueerd.

$\mathrm{GL}(2,p)$ is de groep van alle inverteerbare 2×2 matrices over $\mathbb{F}_p$,

$\mathrm{SL}(2,p) := \{M \in \mathrm{GL}(2,p) \mid \det M = 1\}$,

$$E := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

en

$$0 := \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

p is een priemgetal,

$$A := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

$B \in \mathrm{SL}(2,p)$,

$C = c \cdot E$ voor een $c \in \mathbb{F}_p$,

en G is de ondergroep van $\mathrm{GL}(2,p)$ die door A, B en C wordt voortgebracht.

(I) $p = 5$

$$B = \begin{pmatrix} 1 & -2 \\ -1 & -2 \end{pmatrix}$$

$C = E \Longrightarrow G \cong SL(2,3)$

(II) $p = 11$

$$B = \begin{pmatrix} 1 & 5 \\ -5 & -2 \end{pmatrix}$$

$C = 4 \cdot E \Longrightarrow G \cong SL(2,3) \times \mathbb{Z}/5\mathbb{Z}$

(III) $p = 7$

$$B = \begin{pmatrix} 1 & 3 \\ -1 & -2 \end{pmatrix}$$

$C = E \Longrightarrow G \cong O^*$ Waarbij O^* de zgn. binaire oktaëdergroep is, zie [2].

(IV) $p = 23$

$$B = \begin{pmatrix} 1 & -6 \\ 12 & -2 \end{pmatrix}$$

$C = 2 \cdot E \Longrightarrow G \cong O^* \times \mathbb{Z}/11\mathbb{Z}$

(V) $p = 11$

$$B = \begin{pmatrix} 2 & 4 \\ 1 & -3 \end{pmatrix}$$

$C = E \Longrightarrow G \cong SL(2,5)$

(VI) $p = 29$

$$B = \begin{pmatrix} 1 & -7 \\ -12 & -2 \end{pmatrix}$$

$C = -4 \cdot E \Longrightarrow G \cong SL(2,5) \times \mathbb{Z}/7\mathbb{Z}$

(VII) $p = 59$

$$B = \begin{pmatrix} 9 & 15 \\ -10 & -10 \end{pmatrix}$$

$C = 4 \cdot E \Longrightarrow G \cong SL(2,5) \times \mathbb{Z}/29\mathbb{Z}$

Neem nu een van bovenstaande gevallen en definieer $F := G \cup \{0\}$. Dan bestaat er voor iedere vector $\alpha = \begin{pmatrix} a \\ b \end{pmatrix} \in F_p^2$ precies één element $M_\alpha \in F$ waarvan de eerste rij α is. Vervolgens wordt op F ernaast de gewone matrixvermenigvuldiging $\cdot$ een optelling $+$ gedefinieerd:

$$M_\alpha + M_\beta := M_{\alpha+\beta}$$

$(F, +, \cdot)$ vormt een bijnalichaam met multiplicatieve groep G.

De hierboven geconstrueerde bijnalichamen zijn de zeven eindige uitzonderingen. Paarsgewijs zijn ze niet isomorf.

We kijken nu naar (I): is dit een bijnalichaam? Het aantal elementen van F is $p^2 = 5^2 = 25$. Ten tweede moeten twee elementen $X, Y \in G$ met dezelfde eerste rij hetzelfde zijn. Het bewijs hiervan staat in [2]. Ten derde moet de ene distributieve wet gecontroleerd worden, dit kan in het algemene geval. Volgens

de definitie van $+$, zijn $(F,+)$ en $(F_p^2,+)$ isomorf. Voor willekeurige $\alpha,\beta \in F_p^2$ en $D \in G$ geldt:

$$\begin{aligned} D\cdot(M_\alpha + M_\beta) &= D\cdot M_{\alpha+\beta} \\ &= M_{D\cdot(\alpha+\beta)} \\ &= M_{D\cdot\alpha + D\cdot\beta} \\ &= M_{D\cdot\alpha} + M_{D\cdot\beta} \\ &= D\cdot M_\alpha + D\cdot M_\beta \end{aligned}$$

Dus is $(F,+,\cdot)$ een bijnalichaam.

Met het computerprogramma *Magma* zal ik kijken naar het centrum van [1] en dit vergelijken met het centrum van het bijnalichaam $\mathbb{F}_{5^2}$. De code staat hieronder.

We constueren de matrixgroep over $\mathbb{F}_5$ met de voortbrengers van [1]. Dit is de multiplicatieve groep van het eerste uitzonderingsbijnalichaam, en heeft inderdaad 24 elementen.Het centrum van deze groep heeft 2 elementen met als voortbrenger $\left(\begin{smallmatrix}4&0\\0&4\end{smallmatrix}\right)$. Vervolgens construeren we de multiplicatieve groep van het Dicksonse bijnalichaam $\mathbb{F}_{5^2}$. Deze heeft ook 25 elementen, maar heeft een centrum met 4 elementen met als voortbrengers $\left(\begin{smallmatrix}2&0\\0&2\end{smallmatrix}\right)$ en $\left(\begin{smallmatrix}4&0\\0&4\end{smallmatrix}\right)$ Alle Dicksonse bijnalichamen met dimensie 2 over de kern en hetzelfde aantal elementen zijn isomorf. Het eerste uitzonderingsbijnalichaam heeft net als $\mathbb{F}_{5^2}$ 25 elementen, maar heeft een ander aantal elementen in de kern. Voor de andere zes uitzonderingsbijnalichamen geldt dit ook, en daarom zijn de uitzonderingsbijnalichamen niet Dicksons.

Ieder eindig bijnalichaam is ofwel Dicksons, ofwel isomorf aan één van de zeven uitzonderingsbijnalichamen. Het bewijs hiervan is te vinden in [3] en [2].

Magma code

```
> G:=MatrixGroup< 2 , GF(5) | [0,-1,1,0], [1,-2,-1,-2]>;
> #G;
24
> Center(G);
MatrixGroup(2, GF(5)) of order 2
Generators:
    [4 0]
    [0 4]
> P<x>:=PolynomialRing(GF(5));

> F<j>:= P/ideal<P|x^2-2>;
> F;
Univariate Quotient Polynomial Algebra in j over Finite field of size 5
with modulus j^2 + 3

> (j+1)^12;
```

```
1
> L:=[ [GF(5)!a1,GF(5)!a2,GF(5)!((a1+j*a2)^12*2*a2),GF(5)!
((a1+a2*j)^12*a1] : a1 in [1..4], a2 in [1..4]];

>> L:=[ [GF(5)!a1,GF(5)!a2,GF(5)!((a1+j*a2)^12*2*a2),GF(5)!
((a1+a2*j)^12*a1] : a1 in [1..4], a2 in [1..4]];
                                                                ^
User error: bad syntax
> L:=[ [GF(5)!a1,GF(5)!a2,GF(5)!((a1+j*a2)^12*2*a2),GF(5)!
((a1+a2*j)^12*a1)] : a1 in [1..4], a2 in [1..4]];
> L;
[
    [ 1, 1, 2, 1 ],
    [ 2, 1, 3, 3 ],
    [ 3, 1, 3, 2 ],
    [ 4, 1, 2, 4 ],
    [ 1, 2, 1, 4 ],
    [ 2, 2, 4, 2 ],
    [ 3, 2, 4, 3 ],
    [ 4, 2, 1, 1 ],
    [ 1, 3, 4, 4 ],
    [ 2, 3, 1, 2 ],
    [ 3, 3, 1, 3 ],
    [ 4, 3, 4, 1 ],
    [ 1, 4, 3, 1 ],
    [ 2, 4, 2, 3 ],
    [ 3, 4, 2, 2 ],
    [ 4, 4, 3, 4 ]
]
> GD:=MatrixGroup<2, GF(5) | L>;
> #GD;
24
> Center(GD);
MatrixGroup(2, GF(5)) of order 2^2
Generators:
    [2 0]
    [0 2]

    [4 0]
    [0 4]
>
```

Samenvatting

Een bijnalichaam is een algebraïsche structuur die wordt gedefinieerd door de axioma's van een scheeflichaam, waarbij een van de distributieve wetten wordt weggelaten. De kern K_F van een bijnalichaam F bestaat uit de elementen waarvoor zowel de associatieve als distributieve wetten opgaan. Het centrum is $Z_F := \{z \in F \mid \forall x \in F : zx = xz\}$.

De commutativiteit van de optelling in een bijnalichaam kan worden afgeleid uti de andere axioma's. Het priemlichaam van een bijnalichaam F wordt gedefinieerd als het priemlichaam van de kernk K_F, en de karakteristiek van een bijnalichaam F als de karakteristiek van de kern K_F.

L.E. Dickson heeft een manier bedacht waarop bijnalichamen geconstrueerd kunnen worden door de vermenigvuldiging in een lichaam te vervangen. Alle bijnalichamen die op deze manier geconstrueerd worden, worden 'Dicksons' genoemd.

Op 7 uitzonderingen na, zijn alle eindige bijnalichamen Dicksons, en alle tot nu toe bekende oneindige bijnalichamen zijn ook Dicksons. Een eindig bijnalichaam wordt geclassificeerd door het zgn. 'Zassenhauscriterium': (q, n, μ), de priemmacht q is het aantal elementen van het centrum, n de dimensie over het centrum, en μ een monische irreducibele factor van het n-de cirkeldelingspolynoom $\Psi_n \in \mathbb{F}_p[x]$.

Een deel van de scriptie, zoals de manier van Dickson voor de constructie van een eindig bijnalichaam, en het Zassenhauscriterium, is een samenvatting uit literatuur. Hier heb ik aan toegevoegd: de constructie via de afbeelding χ, de voorbeelden, toepassingen, en het stuk waarin gekeken wordt waarom een van de uitzonderingsbijnalichamen niet Dicksons is.

Bibliografie

[1] Prof. dr. B. van Geemen, Prof. dr. H.W. Lenstra jr., Prof. dr. F. Oort, and Prof. dr. J. Top. *Ringen en Lichamen*. http://www.math.rug.nl/∼top/dic.pdf.

[2] Heinz Wähling. *Theorie der Fastkörper*. Thales Verlag, Essen, 1987.

[3] Hans Zassenhaus. Über endliche Fastkörper. *Abh. Math. Sem. Univ. Hamburg*, 11:187–220, 1936.

[4] Helmut Karzel. Bericht über projektive inzidenzgruppen. *Jber. Deutsch. Math.-Verein*, 67:58–92, 1964.

[5] Yuen e.a. Fong. *Near-Rings and Near-Fields*. Kluwer Academic Publishers, Dordrecht, 1995.

[6] Ravindranathan Thangadurai. On the coëfficients of cyclotomic polynomials. *Cyclotomic Fields and Related Topics (Pune)*, page 311C322, 1999.

[7] Samuel Bamunoba. *Cyclotomic Polynomials*. African Institute for Mathematical Sciences, Stellenbosch University, South-Africa, 2010.