Bijna-lichamen en hun relatie tot scherp tweevoudig transitieve groepswerkingen

Roos, L. de

A.L.S. de Roos

Bijna-lichamen en hun relatie tot scherp tweevoudig transitieve groepswerkingen

Bachelorscriptie

24 augustus 2020

Scriptiebegeleider: prof.dr. H.W. Lenstra

Universiteit Leiden
Mathematisch Instituut

Inhoudsopgave

1 Inleiding

De studie van de bijna-lichamen is een relatief onbekend gebied van de wiskunde. Toch heeft het toepassingen in de groepen theorie, namelijk bij scherp tweevoudig transitieve werkingen. Er blijkt zelfs dat er een manier is om bij elk eindig bijna-lichaam een eindige scherp tweevoudig transitieve werking te krijgen en omgekeerd, deze geven wij in stelling 3.10. Als we kijken naar algemene bijna-lichamen, dan blijkt er nog steeds een manier te zijn om een scherp tweevoudig transitieve werking te krijgen, maar het omgekeerde hoeft niet meer altijd te gelden. In stelling 3.15 laten wij zien dat als de scherp tweevoudig transitieve werkingen een zogeheten *reguliere normale ondergroep* hebben, ze dan wel altijd een bijna-lichaam geven en dat omgekeerd elk bijna-lichaam een scherp tweevoudig transitieve werking met een reguliere normale ondergroep geeft. In deze scriptie zullen wij eerst de theorie omtrent bijna-lichamen ontwikkelen, hierbij gaan wij ook kijken naar iets algemenere objecten, genaamd bijna-ringen. Deze kunnen wij gebruiken om manieren te vinden om bijna-lichamen te construeren en te representeren. Daarna gebruiken we deze theorie om de bovengenoemde methode concreet te maken. Ook zullen wij bewijzen dat deze methode in feite een equivalentie van categorieën geeft.

2 Bijna-ring en bijna-lichaam theorie

2.1 Introductie

In dit hoofdstuk zullen we eerst de algebraïsche structuren bijna-ring en bijna-lichaam introduceren. Deze verschillen van respectievelijk ringen dan wel delingsringen in dat bij bijna-ringen de optelling niet commutatief hoeft te zijn en voor beide hoeft alleen de linker distributieve wet te gelden (of de rechter distributieve wet). Hoewel we niet eisen dat de optelling van een bijna-lichaam commutatief is, zal blijken dat dit toch zal gelden. De belangrijkste stellingen die we bewijzen in dit hoofdstuk zijn de volgende:

- Stelling 2.32, waarin we een constructie geven door een afbeelding $\rho : D^* \to \mathrm{Aut}(D)$, met D een delingsring en ρ zo dat voor alle $a, b \in D$ geldt $\rho(a) \circ \rho(b) = \rho(a \cdot \rho(a)(b))$, dan is D een bijna-lichaam met vermenigvuldiging $* : D \times D \to D$, met $a * b = 0$, als $a = 0$ en $a * b = a \cdot \rho(a)(b)$ als $a \neq 0$.
- Stelling 2.25, waarin we laten zien dat een bijna-lichaam ook gegeven kan worden als een paar (G, Λ), waarbij G een groep is en $\Lambda \subseteq \mathrm{End}(G)$ zo dat $0 \in \Lambda$ en $\Lambda \backslash \{0\}$ een ondergroep van $\mathrm{Aut}(G)$ is zo dat er een bijectie $\mathrm{ev}_1 : \Lambda \to G, \lambda \mapsto \lambda(1)$ voor een zekere $1 \in G$, met $1 \neq e$.

2.2 Basis structuren

Voordat we het concept van een bijna-lichaam introduceren, zullen we eerst de algemenere *bijna-ring* introduceren. Dit is een ring waarvan de optelgroep niet abels hoeft te zijn, de vermenigvuldiging een monoïde vormt en alleen de linkerdistributieve wet wordt geëist.

Definitie 2.1 (Monoïde)**.** Een *monoïde* is een drietal $(M, *, e)$, waarbij M een verzameling is, er geldt $e \in M$ en $* : M \times M \to M$ een operatie is, zo dat de volgende eigenschappen gelden:

1. De operatie $*$ is associatief.
2. Het element e is een eenheid: $\forall a \in M : a * e = e * a = a$.

Definitie 2.2 (Bijna-ring)**.** Een *linker bijna-ring* is een vijftal $(R, +, \cdot, 0, 1)$ waarvoor de volgende voorwaarden gelden:

1. $(R, +, 0)$ vormt een groep.
2. $(R, \cdot, 1)$ vormt een monoïde.
3. Linksdistributiviteit van vermenigvuldiging, dus:
   $\forall a, b, c \in R : a \cdot (b + c) = a \cdot b + a \cdot c$.

Het element 0 noemen we de additieve eenheid en 1 noemen we de multiplicatieve eenheid.

We zullen een linker bijna-ring vaak ook wel een bijna-ring noemen. Een *rechter bijna-ring* wordt analoog gedefinieerd met de rechter distributieve wet.

Voorbeeld 2.3. Laat $(G, +, 0)$ een (niet noodzakelijk Abelse) groep zijn en laat $\mathrm{Map}(G) := \{f : G \to G\}$ de verzameling functies van G naar G zijn. $\mathrm{Map}(G)$ is een rechter bijna-ring met als vermenigvuldiging de samenstelling en optelling als volgt:

$$\forall f, g \in \mathrm{Map}(G),\ \forall x \in G : (f + g)(x) := f(x) + g(x)$$

Schrijf 0 voor de nulafbeelding, dit is de additieve eenheid:

$$\forall f \in \mathrm{Map}(G),\ \forall x \in G : f(x) + 0(x) = f(x) = 0(x) + f(x)$$

De identiteit is de multiplicatieve eenheid: $\forall f \in \mathrm{Map}(G)\ \forall x \in G : \mathrm{id} \circ f(x) = f(x) = f \circ \mathrm{id}(x)$. De rechtsdistributiviteit volgt uit de definitie van de optelling: $\forall f, g, h \in \mathrm{Map}(G),\ \forall x \in G : (f + g) \circ h(x) = (f + g)(h(x)) = f(h(x)) + g(h(x)) = f \circ h(x) + g \circ h(x)$. Dus, omdat de samenstelling associatief is, is $\mathrm{Map}(G)$ een rechter bijna-ring. Merk op dat als G niet abels is, dat $\mathrm{Map}(G)$ dat ook niet is. We zullen nu $\mathrm{Map}(G)$ ook wel de afbeeldingsbijna-ring van G noemen.

Nu kunnen we een *bijna-lichaam* als volgt definiëren.

Definitie 2.4 (Bijna-lichaam)**.** Een *(linker) bijna-lichaam* is een vijftal $(B, +, \cdot, 0, 1)$ waarvoor de volgende voorwaarden gelden:

1. $(B, +, \cdot, 0, 1)$ is een (linker) bijna-ring.
2. $1 \neq 0$
3. Multiplicatieve inversen bestaan, oftewel:
   $\forall a \in B \backslash \{0\}\ \exists a^{-1} \in B : a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Ook hier wordt een *rechter bijna-lichaam* analoog gedefinieerd op basis van een rechter bijna-ring. In het algemeen zullen we ook wel zeggen dat R en B bijna-ringen dan wel bijna-lichamen zijn waarbij optelling, vermenigvuldiging en de elementen 0 en 1 geïmpliceerd zijn of bekend.

Voorbeeld 2.5. 1. Duidelijk is dat elk lichaam en elke delingsring een bijna-lichaam is.

2. Laat $\mathbb{F}_9 = \mathbb{F}_3(i)$ het lichaam van orde 9 zijn. Hier voldoet i aan de vergelijking $i^2 + 1 = 0$. Definieer de vermenigvuldiging $\circ : \mathbb{F}_9 \times \mathbb{F}_9 \to \mathbb{F}_9$ als volgt:

$$\forall a, b \in \mathbb{F}_9 : \ a \circ b = \begin{cases} a \cdot b, \text{ als } a \in H \\ a \cdot \bar{b}, \text{ als } a \neq 0 \text{ en } a \notin H \\ 0, \text{ als } a = 0 \end{cases}$$

waarbij $\bar{b}$ gegeven als volgt: $\forall x, y \in \mathbb{F}_3 : \overline{x + yi} = x - yi$ en H de ondergroep van $\mathbb{F}_9^*$ is die voortgebracht wordt door i. Het is een simpele opgave om te laten zien dat deze verminigvuldiging $(\mathbb{F}_9, +, \circ, 0, 1)$ tot een bijna-lichaam maakt. Merk wel op dat $(1+i) \circ b = (1 + i) \cdot \bar{b}$ en $1 \circ b + i \circ b = 1 \cdot b + i \cdot b = (1 + i) \cdot b$, maar als $b = i$ geldt bijvoorbeeld dan is $(1 + i) \cdot b \neq (1 + i) \cdot \bar{b}$, dus $(\mathbb{F}_9, +, \circ, 0, 1)$ is geen delingsring.

Het blijkt dat de optelling in een bijna-lichaam altijd commutatief is. We zullen dit in stelling 2.31 bewijzen met behulp van groepen theorie. H. Wähling geeft hier ook een bewijs voor zonder groepen theorie, dit is te vinden in [3] op pagina 12.

We zullen in de volgende propositie met $x^\dagger$ de additieve inverse van x bedoelen.

Propositie 2.6. *Laat R een linker bijna-ring zijn, dan geldt voor alle $x, y \in R$ dat $x \cdot 0 = 0$ en $x \cdot y^\dagger = (xy)^\dagger$*

Bewijs. Laat de linksvermenigvuldiging met x gegeven zijn als $\lambda_x : R \to R, y \to x \cdot y$, dan volgt uit de linksdistributiviteit van R dat λ_x een groepshomomorfisme is. De bewering uit de propositie volgt nu direct. □

Voor een rechter bijna-ring R geldt analoog natuurlijk dat $0 \cdot x = 0$.

We zullen voor elke bijna-ring R, de verzameling van multiplicatieve eenheden noteren met $R^* = \{x \in R \mid \exists y \in R : x \cdot y = y \cdot x = 1\}$. Er geldt zelfs dat deze verzameling een groep vormt onder vermenigvuldiging.

Lemma 2.7. *Laat $(R, +, \cdot, 0, 1)$ een linker bijna-ring zijn, dan is $(R^*, \cdot, 1)$ een groep.*

Bewijs. Laat $x, y \in R^*$ willekeurig gegeven zijn en laat $x^{-1}, y^{-1} \in R^*$ hun multiplicatieve inversen zijn. We vinden dan dat $(x \cdot y) \cdot (y^{-1} \cdot x^{-1}) = e = (y^{-1} \cdot x^{-1}) \cdot (x \cdot y)$, dus $x \cdot y$ heeft een multiplicatieve inverse. Aangezien we dus weten dat R gesloten is onder vermenigvuldiging, vinden we dat $(R^*, \cdot, 1)$ een deelmonoïde is van $(R, \cdot, 1)$. Bovendien geldt dat inversen in monoïden uniek zijn als ze bestaan. Het is duidelijk dat R^* gesloten onder inversie is, dus $(R^*, \cdot, 1)$ is een groep. □

Er blijkt nu zelfs dat voor bijna-lichamen vermenigvuldiging met 0 van beide kanten weer in 0 resulteert.

Propositie 2.8. *Laat B een linker bijna-lichaam zijn, dan geldt voor alle $x \in B$ dat $0 \cdot x = 0$.*

Bewijs. Merk op dat $B\backslash\{0\} \subseteq B^*$. Omdat volgens propositie 2.6 voor elke $x \in B$ geldt dat $x \cdot 0 = 0$, weten we dat $0 \notin B^*$, dus $B^* = B\backslash\{0\}$. Laat nu $x \in B$ willekeurig gegeven zijn. Stel dat $x = 0$, dan geldt $0 \cdot x = 0$, weer vanwege propositie 2.6. Stel dat $x \neq 0$, dan is er een $x^{-1} \in B^*$, zo dat $x \cdot x^{-1} = x^{-1} \cdot x = 1$. Nu vinden we het volgende:

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

Omdat B^* een groep is, geldt dat ofwel $x^{-1} = 0$, ofwel $0 \cdot x = 0$, maar omdat $B^* = B\backslash\{0\}$, weten we dat $x^{-1} \neq 0$, dus nu volgt $0 \cdot x = 0$. □

Net zoals bij veel algebraïsche structuren, kunnen onze monoïden, bijna-ringen en bijna-lichamen ook deelstructuren bevatten.

Definitie 2.9 (Deelmonoïde)**.** Laat $(M, *, e)$ een monoïde zijn, dan is een deelmonoïde van M een deelverzameling $M' \subseteq M$, zo dat $(M', *, e)$ een monoïde is. Equivalent is een deelmonoïde een deelverzameling $M' \subseteq M$, zo dat $e \in M'$ en dat M gesloten is onder $*$.

Definitie 2.10 (Deelbijna-ring)**.** Laat $(R, +, \cdot, 0, 1)$ een linker bijna-ring zijn, dan is een *deelbijna-ring* van R een deelverzameling $R' \subseteq R$ zo dat $(R', +, \cdot, 0, 1)$ een bijna-ring is. Equivalent is een deelbijna-ring een deelverzameling $R' \subseteq R$, zo dat de optelgroep van R' een ondergroep is van die van R, dat R' gesloten is onder vermenigvuldiging en dat $1 \in R$.

Definitie 2.11 (Deelbijna-lichaam)**.** Laat $(B, +, \cdot, 0, 1)$ een linker bijna-lichaam zijn, dan is een *deelbijna-lichaam* B' een deelbijna-ring van B zo dat B' bovendien een linker bijna-lichaam is (oftewel $B'\backslash\{0\}$ is gesloten onder multiplicatieve inverse).

Net zo kunnen we voor rechter bijna-ringen en rechter bijna-lichamen een deelbijna-ring dan wel deelbijna-lichaam definiëren.

Bovendien hebben veel eigenschappen van linker bijna-ringen en bijna-lichamen analoga in de rechter bijna-ringen en bijna-lichamen. Dit is te zien door de omgekeerde te definiëren.

Definitie 2.12 (Omgekeerde bijna-ring en bijna-lichaam)**.** Laat $(R, +, \cdot, 0, 1)$ een linker bijna-ring zijn en $(B, +, \cdot, 0, 1)$ een linker bijna-lichaam. De *omgekeerde bijna-ring* van R en *omgekeerde bijna-lichaam* van B zijn respectievelijk $(R^{\text{op}}, +, \circ, 0, 1)$ en $(B^{\text{op}}, +, \circ, 0, 1)$, met $R^{\text{op}} = R$, $B^{\text{op}} = B$ en $\circ = ((x, y) \mapsto y \cdot x)$. Analoog worden ook de omgekeerde voor rechter bijna-ringen en bijna-lichamen gedefinieerd.

Lemma 2.13. *Laat R een linker bijna-ring zijn, dan is R^{op} een rechter bijna-ring. Zo ook geldt dat als R een rechter bijna-ring is, R^{op} een linker bijna-ring is. Bovendien geldt voor elke bijna-ring R (zowel linker als rechter), dat $(R^{op})^{op}$ weer gelijk is aan R.*

De bovenstaande bewering is niet moeilijk te bewijzen. Bovendien geldt deze ook nog als de bijna-ring door een bijna-lichaam vervangen wordt.

2.3 Homomorfismen

Net als bij ringtheorie, is het belangrijk om een concept van homomorfismen te hebben dat ons in staat stelt om via functies bijna-ringen en bijna-lichamen met elkaar te vergelijken.

Definitie 2.14 (Homomorfisme)**.** Een *linker bijna-ringhomomorfisme* is een afbeelding $f : R \to R'$, waarbij R en R' linker bijna-ringen zijn, zo dat voor elke $a, b \in R$ geldt dat $f(a + b) = f(a) + f(b)$, $f(a \cdot b) = f(a) \cdot f(b)$ en $f(1) = 1$. Een *linker bijna-lichaamshomomorfisme* is een linker bijna-ringhomomorfisme $f : B \to B'$, waarbij B en B' bijna-lichamen zijn. Een bijectief homomorfisme heet een isomorfisme.

Voor de rechter bijna-ringen en rechter bijna-lichamen definiëren we analoog ook een rechter bijna-ringhomomorfisme en rechter bijna-lichaamshomomorfisme. Merk bovendien op dat elk bijna-ringhomomorfisme f in het bijzonder een groepshomomorfisme is en er dus ook geldt dat $f(0) = 0$.

Aangezien we al gezien hebben dat $\cdot^{\mathrm{op}}$ ons een rechter bijna-ring geeft uit een linker en andersom, is het logisch om ook een manier te willen hebben om rechter en linker bijna-ringen met elkaar te kunnen vergelijken. Hiervoor zullen wij het begrip antihomomorfisme introduceren.

Definitie 2.15. Laat R een linker bijna-ring zijn en R' een rechter bijna-ring. Een *antibijna-ringhomomorfisme* is een functie $f : R \to R'$ of $f : R' \to R$ zo dat $f : R \to (R')^{\mathrm{op}}$ dan wel $f : R' \to R^{\mathrm{op}}$ een bijna-ringhomomorfisme is.

Lemma 2.16. *Laat R een bijna-ring zijn, dan is $\pi : R \to R^{op}, x \mapsto x$ een natuurlijk anti-isomorfisme.*

We laten het bewijs als een opgave voor de lezer.

Net als bij lichamen, geldt bij bijna-lichamen dat homomorfismen injectief zijn.

Definitie 2.17. Laat R en R' bijna-ringen zijn en $f : R \to R'$ een homomorfisme, dan definiëren we de kern van f als volgt:

$$\ker(f) = \{b \in B \mid f(b) = 0\}$$

Gevolg 2.18. *Laat $f : R \to R'$ een homomorfisme van linker bijna-ringen zijn, dan geldt dat f injectief is dan en slechts dan als $ker(f) = \{0\}$.*

Deze bewering volgt direct uit het feit dat bijna-ringhomomorfismen in het bijzonder groepshomomorfismen zijn.

Gevolg 2.19. *Laat B en B' bijna-lichamen zijn en $f : B \to B'$ een homomorfisme, dan is f injectief.*

Dit bewijs is analoog aan het geval voor lichamen en we laten deze daarom als opgave voor de lezer.

Propositie 2.20. *Laat R en R' linker bijna-ringen zijn en $f : R \to R'$ een homomorfisme. Dan geldt dat $f(R)$ een deelbijna-ring van R' is.*

Bewijs. Merk op dat we meteen weten dat $1 = f(1) \in f(R)$ en $0 = f(0) \in f(R)$. Omdat f bovendien een groepshomomorfisme van de optelgroepen is, is $(f(R), +, 0)$ een groep. Laat $f(x), f(y) \in f(R)$ willekeurig gegeven zijn, dan volgt dat $f(x) \cdot f(y) = f(x \cdot y) \in f(R)$, dus $f(R)$ is gesloten onder vermenigvuldiging en is dus een deelbijna-ring van R'. □

De voorgaande propositie is volledig analoog te bewijzen voor rechter bijna-ringen. Ook geldt deze propositie voor bijna-lichamen (zowel rechter als linker).

Propositie 2.21. *Laat B en B' linker bijna-lichamen zijn en $f : B \to B'$ een homomorfisme, dan is $f(B)$ een deelbijna-lichaam van B'.*

Het bewijs is niet veel verschillend van de versie voor bijna-ringen.

2.4 Constructies

We zullen nu zien dat elke rechter bijna-ring isomorf is aan een deelbijna-ring van de afbeeldingsbijna-ring van zijn optelgroep.

Stelling 2.22. *Laat R een rechter bijna-ring zijn en schrijf R^+ voor zijn optelgroep. R is dan isomorf met een deelbijna-ring $R' \subseteq \mathrm{Map}(R^+)$.*

Bewijs. Beschouw voor elke $r \in R$ de afbeelding $\lambda_r : R \to R, x \mapsto r \cdot x$. Het is gemakkelijk in te zien dat de afbeelding $\alpha : R \to \mathrm{Map}(R^+), r \mapsto \lambda_r$ een homomorfisme is. Laat nu $x, y \in R$ willekeurig gegeven zijn en stel dat $\alpha(x) = \alpha(y)$ geldt. Dan geldt voor elke $r \in R$ dat $\lambda_x(r) = \lambda_y(r)$, oftewel $x \cdot r = y \cdot r$. Dit geldt dus in het bijzonder voor $r = 1$, oftewel $x = y$. Dus α is ook injectief. Omdat $\alpha(R)$ een bijna-ring is, geeft $\alpha : R \to \alpha(R)$ dus een bijna-ringisomorfisme. □

Nu dat we weten dat elke rechter bijna-ring R isomorf is met een deelbijna-ring van $\mathrm{Map}(R^+)$, kunnen we bijna-ringen construeren door een inbedding te geven van een groep G in $\mathrm{Map}(G)$. Vervolgens zal de vermenigvuldiging op G geïnduceerd worden door de samenstelling op $\mathrm{Map}(G)$.

Voorbeeld 2.23. We zullen een voorbeeld van een rechter bijna-ring geven die gevonden kan worden door een inbedding van de diëdergroep $D_4 = \{\sigma^n \rho^m \mid n \in \mathbb{Z}/2\mathbb{Z}, m \in \mathbb{Z}/4\mathbb{Z}\}$ in $\mathrm{Map}(D_4)$, zo dat dit een groepshomomorfisme is en dat het beeld gesloten onder samenstelling is. Dan is $(D_4, \cdot, \circ, e, \rho)$ een bijna-ring, met $\cdot$ de groepsstructuur en $\circ : D_4 \times D_4 \to D_4$ gegeven als:

$$\forall x \in D_4, \forall n \in \mathbb{Z}/2\mathbb{Z}, m \in \mathbb{Z}/4\mathbb{Z} : \sigma^n \rho^m \circ x = \begin{cases} \sigma x^m, \text{ als } n = 1 \text{ en } x \in \{\rho, \rho^3\} \\ x^m, \text{ anders} \end{cases}$$

We laten het als opgave aan de lezer om de inbedding te vinden die deze vermenigvuldiging geeft.

We hebben nu gezien dat elke rechter bijna-ring gegeven kan worden als een deelbijna-ring van $\mathrm{Map}(G)$ voor een zekere groep G. Bovendien volgt natuurlijk ook dat elke linker bijna-ring dan gegeven kan worden als een deelbijna-ring van $\mathrm{Map}(G)^{\mathrm{op}}$ voor een zekere groep G. Oftewel stelling 2.22 is een analogon van de stelling van Cayley, maar dan voor bijna-ringen. In dit licht is het dus ook redelijk om bij voorbeelden van bijna-ringen $\mathrm{Map}(G)$ als "Hoofdvoorbeeld" te nemen. Het blijkt dat er ook een manier is om een bijna-ring volledig in het kader van de groepen theorie op te vatten.

Stelling 2.24. *Laat $(R, +, \cdot, 0, 1)$ een linker bijna-ring zijn en beschouw $\Lambda_R = \{(x \mapsto r \cdot x) \mid r \in R\}$. Dan is Λ_R een deelmonoïde van $\mathrm{End}(R^+)$ (met R^+ de optelgroep van R) en de afbeelding $\mathrm{ev}_1 : \Lambda_R \to R^+, \lambda \mapsto \lambda(1)$ is bijectief. Omgekeerd geldt dat als G een groep is, $1 \in G$ met 1 niet noodzakelijk het eenheidselement 0 en $\Lambda \subseteq \mathrm{End}(G)$ een deelmonoïde zo dat de afbeelding $\mathrm{ev}_1 : \Lambda \to G, \lambda \mapsto \lambda(1)$ bijectief is, dan is $(G, +, \cdot, 0, 1)$ een linker bijna-ring, met $+$ de groepsoperatie van G en $\cdot : G \times G \to G$ gedefiniëerd als $\forall x, y \in G : x \cdot y = \mathrm{ev}_1^{-1}(x)(y)$.*

Bewijs. Laat R een linker bijna-ring zijn. Dan geldt vanwege de linksdistributiviteit dat elk element in Λ_R een groepsendomorfisme is. Aangezien $\mathrm{id} = (x \mapsto 1 \cdot x)$, weten we dat $\mathrm{id} \in \Lambda_R$ en dan is het duidelijk dat Λ_R gesloten is onder samenstelling en dus een monoïde is. Merk bovendien op dat omdat voor elke $r \in R$ geldt dat $r \cdot 1 = r$, we zien dat ev_1 bijectief moet zijn.

Laat nu $(G, +, 0)$ een groep zijn en $\Lambda \subseteq \mathrm{End}(G)$ een deelmonoïde zo dat ev_1 bijectief is. Schrijf dan $\forall x \in G : \lambda_x := \mathrm{ev}_1^{-1}(x)$. Dan volgt dat $\cdot$ linksdistributief is: $\forall x, y, z \in G : x \cdot (y + z) = \lambda_x(y + z) = \lambda_x(y) + \lambda_x(z) = x \cdot y + x \cdot z$. Bovendien is $\cdot$ associatief: $\forall x, y, z \in G : x \cdot (y \cdot z) = \mathrm{ev}_1^{-1}(x) \circ \mathrm{ev}_1^{-1}(y)(z) = \mathrm{ev}_1^{-1}(x \cdot y)(z) = (x \cdot y) \cdot z$, want $\mathrm{ev}_1^{-1}(x) \circ \mathrm{ev}_1^{-1}(y)(1) = x \cdot y$ en Λ is gesloten onder samenstelling. □

Natuurlijk kan de nul ring ook gegeven worden door $G = \{0\}$ en $\Lambda = \{0\}$, maar in alle andere gevallen, zal $1 \neq 0$ gelden. De voorgaande stelling geeft ons dus dat de vermenigvuldigings monoïde van een linker bijna-ring op zijn optelgroep als een deelmonoïde van de endomorfismen van de optelgroep werkt. Merk bovendien op dat dit argument geheel analoog is voor rechter bijna-ringen, met Λ_R alle rechter vermenigvuldigingen en voor groep G de vermenigvuldiging $x \cdot y := \mathrm{ev}_1^{-1}(y)(x)$.

Deze representatie van bijna-ringen is ook nuttig voor de theorie van bijna-lichamen. Hij geeft namelijk aanleiding tot de volgende stelling.

Stelling 2.25. *Laat $(B, +, \cdot, 0, 1)$ een bijna-lichaam zijn. Vat B als een bijna-ring op en laat (B^+, Λ_B) de representatie daarvan zijn zoals in stelling 2.24, waarbij B^+ dus de optelgroep van B is. Dan is Λ_B niet alleen een deelmonoïde van $\mathrm{End}(B^+)$, maar $\Lambda_B \backslash \{0\}$ is zelfs een ondergroep van $\mathrm{Aut}(B^+)$. Omgekeerd geldt ook weer dat $(G, \Lambda, 0, 1)$ als in stelling 2.24, met G een groep, $0, 1 \in G$, $0 \neq 1$ en $\Lambda \backslash \{0\}$ een ondergroep van $\mathrm{Aut}(G)$ met $0 \in \Lambda$ een bijna-lichaam geeft. (Dus als $\mathrm{ev}_1 : \Lambda \to G, \lambda \mapsto \lambda(1)$ bijectief is.)*

Bewijs. Laat $\lambda \in \Lambda_B \backslash \{0\}$ willekeurig gegeven zijn, dan is er een $b \in B$ zo dat $\lambda = (x \mapsto b \cdot x)$. Nu weten we dat $\lambda_{b^{-1}} = (x \mapsto b^{-1} \cdot x) \in B$. Omdat duidelijk geldt dat $\lambda_{b^{-1}} = \lambda^{-1}$, weten we dus dat $\Lambda_B \backslash \{0\}$ gesloten is onder inversie, dus $\Lambda_B \backslash \{0\}$ is een groep.

We weten al dat $(G, +, \cdot, 0, 1)$ voor zekere $0, 1 \in G$ een bijna-ring is uit stelling 2.24. Schrijf voor elke $b \in B : \lambda_b = \mathrm{ev}_1^{-1}(b)$. Dan volgt uit de associativiteit van vermenigvuldiging dat voor elke $x, y \in B$ geldt $x \cdot y = x \cdot y \cdot 1 = \lambda_x \circ \lambda_y(1)$. Omdat $\Lambda \backslash \{0\}$ een groep is, is er voor elke $x \in B^*$ een $\lambda \in \Lambda$ zo dat $\lambda_x = \lambda^{-1}$. Oftewel $x \cdot \lambda(1) = 1$, dus $x^{-1} = \lambda(1) \in G$. Dus $G \backslash \{0\}$ is gesloten onder multiplicatieve inversie, dus $(G, +, \cdot, 0, 1)$ is een linker bijna-lichaam. □

Wat we nu dus gezien hebben is dat de multiplicatieve groep van een bijna-lichaam op de optelgroep werkt.

Gevolg 2.26. *Laat $(B, +, \cdot, 0, 1)$ een linker bijna-lichaam zijn, dan geldt dat $B^* \cong \Lambda_B\backslash\{0\}$, met Λ_B als in stelling 2.25. Het isomorfisme is gelijk aan $\mathrm{ev}_1|_{\Lambda_B\backslash\{0\}}$ Bovendien volgt nu dus dat B^* werkt op B via linksvermenigvuldiging, of equivalent dat $\Lambda_B\backslash\{0\}$ op B werkt via evaluatie.*

Dit volgt direct uit stelling 2.25.

Stelling 2.27. *Laat $(B, +, \cdot, 0, 1)$ een bijna lichaam zijn, dan geeft de werking van $\Lambda_B\backslash\{0\}$ op B een vrije en transitieve werking op $B\backslash\{0\} = B^*$.*

Bewijs. Laat $x \in B^*$ en $\lambda \in \Lambda_B\backslash\{0\}$ willekeurig gegeven zijn en stel dat $\lambda(x) = x$. Er is een $g \in B$ zo dat $\lambda = (z \mapsto g \cdot z)$. We weten dat $x^{-1} \in B$, dus geeft $g \cdot x \cdot x^{-1} = x \cdot x^{-1}$ dat $g = 1$. Dus $\Lambda_B\backslash\{0\}$ werkt vrij op B^*. Omdat ev_1 een bijectie is, weten we dat de baan van 1 gelijk is aan heel B^* (want $\mathrm{ev}_1(0) = 0$), dus $\Lambda_B\backslash\{0\}$ werkt transitief op B^*. □

Alternatief kunnen we ook inzien dat ev_1 de werkingen behoudt en dat B^* vrij en transitief op zichzelf werkt via linksvermenigvuldiging.

Nu zou het natuurlijk ook nuttig zijn om te weten dat (G, Λ) met G een groep, $0 \in \Lambda$ en $\Lambda\backslash\{0\} \subseteq \mathrm{Aut}(G)$ een ondergroep, al een bijna-lichaam zouden geven, als we weten dat $\Lambda\backslash\{0\}$ vrij en transitief op G werkt. (Dus zonder te weten dat ev_1 bijectief is.)

Stelling 2.28. *Laat G een groep zijn met $0, 1 \in G$, $0 \neq 1$ en Λ een deelverzameling van $\mathrm{End}(G)$, zo dat $0 \in \Lambda$ en $\Lambda\backslash\{0\}$ een ondergroep van $\mathrm{Aut}(G)$ is. Als $\Lambda\backslash\{0\}$ vrij en transitief op $G\backslash\{0\}$ werkt, dan is ev_1 bijectief en is $(G, +, \cdot, 0, 1)$ dus een linker bijna-lichaam, waarbij $+$ de groepsoperatie van G is en $\cdot : G \times G \to G$ gegeven is als $x \cdot y = \mathrm{ev}_1^{-1}(x)(y)$.*

Bewijs. Omdat de werking vrij en transitief is, is er voor elke $x, y \in G\backslash\{0\}$, een unieke $\lambda \in \Lambda$ zo dat $\lambda(x) = y$, dus in het bijzonder geldt dit als $x = 1$. Aangezien ook geldt dat $0(1) = 0$, weten we nu dat ev_1 bijectief is en dan volgens stelling 2.25 dat $(G, +, \cdot, 0, 1)$ dus een linker bijna-lichaam is. □

Uit deze voorgaande stellingen zal nu ook volgen dat de optelgroep van een bijna-lichaam Abels moet zijn. Hiervoor zullen wij wel eerst het volgende lemma nodig hebben.

Lemma 2.29. *Laat G een groep zijn zo dat voor elke $x \in G$ er een unieke $y \in G$ is met $y^2 = x$. Stel dat er een $\sigma \in \mathrm{Aut}(G)$ is zo dat $\sigma^2 = \mathrm{id}$, dan geldt voor elke $a \in G$ dat er unieke $b, c \in G$ zijn zo dat $\sigma(b) = b$, $\sigma(c) = c^{-1}$ en $a = bc$.*

Bewijs. Beschouw $\sigma(a)^{-1}a$, dan weten we dat er een unieke $c \in G$ is zo dat $\sigma(a)^{-1}a = c^2$, oftewel $a = \sigma(a)c^2$. Dan vinden wij dus ook $\sigma(a) = a\sigma(c^2)$, aangezien $\sigma^2 = \mathrm{id}$ geldt. Bovendien volgt nu $a = \sigma(a)c^2 = a\sigma(c)^2c^2$. Dus vinden we dat $\sigma(c)^2 = (c^{-1})^2$ en vanwege de eis voor G, vinden we ook $\sigma(c) = c^{-1}$. Laat nu $b = ac^{-1}$, dan vinden wij $\sigma(b) = \sigma(a)\sigma(c^{-1}) = a\sigma(c)^2\sigma(c^{-1}) = a\sigma(c) = ac^{-1} = b$. Stel nu dat we $x, y \in G$ hebben zo dat $\sigma(x) = x$, $\sigma(y) = y^{-1}$ en $a = xy$. Dan geldt dus $\sigma(a) = xy^{-1}$, oftewel $x = \sigma(a)y$. Vervolgens vinden we $a = \sigma(a)y^2$, maar omdat c het unieke element was zo dat $a = \sigma(a)c^2$, moet gelden dat $y = c$ en $x = b$. Dus hiermee is dit lemma bewezen. □

Lemma 2.30. *Laat G een groep zijn en $\Lambda \subseteq \mathrm{Aut}(G)$ een ondergroep die vrij en transitief op $G\backslash\{e\}$ werkt, dan is G Abels.*

Bewijs. We zullen nu een $\sigma \in \Lambda$ construeren zo dat voor alle $g \in G$ geldt dat $\sigma(g) = g^{-1}$, want als deze bestaat, is G Abels, omdat σ een automorfisme is.

Stel dat voor elke $g \in G$ geldt dat $g^{-1} = g$, dan kunnen we $\sigma = \mathrm{id} \in \Lambda$ kiezen. Stel nu dat er een $g \in G$ is zo dat $g^{-1} \neq g$, of equivalent $g^2 \neq e$ en houd deze g vast. Natuurlijk weten we dan dat $g \neq e$. We zullen bewijzen dat voor elke $x \in G$ er een unieke $y \in G$ is zo dat $y^2 = x$. Laat $a \in G\backslash\{e\}$ willekeurig gegeven zijn. Omdat Λ vrij en transitief werkt op $G\backslash\{e\}$, is er een unieke $\lambda \in \Lambda$ zo dat $a = \lambda(g)$, dus $a^2 = \lambda(g^2) \neq e$. Om deze reden geldt dat als $x = e$, dat $y = e$ het unieke element is, zo dat $y^2 = x$. Stel dat $x \neq e$, laat dan $\tau \in \Lambda$ het unieke automorfisme zijn, zo dat $\tau(g^2) = x$, dan is $y = \tau(g)$ een element waarvoor geldt dat $y^2 = x$. Stel dat er een $z \in G$ is zo dat $z^2 = x$, dan geldt $z \neq e$, dus is er een unieke $\lambda \in \Lambda$ zo dat $\lambda(y) = z$. Dan geldt dus $y^2 = x = z^2 = \lambda(y^2)$, dus omdat Λ vrij op $G\backslash\{e\}$ werkt, geldt $\lambda = \mathrm{id}$ en dus ook $z = y$. Oftewel het element $y = \tau(g)$ is het unieke element zo dat $y^2 = x$. Omdat Λ vrij en transitief werkt op $G\backslash\{e\}$, is er een unieke $\sigma \in \Lambda$ zo dat $\sigma(g) = g^{-1}$. Dus omdat $\sigma^2(g) = g$ en $\sigma^2 \in \Lambda$, moet gelden dat $\sigma^2 = \mathrm{id}$. Dus volgens lemma 2.29 geldt voor elke $a \in G$ dat er unieke $b, c \in G$ zijn, zo dat $a = bc$ en $\sigma(b) = b$, $\sigma(c) = c^{-1}$. Maar omdat Λ vrij op $G\backslash\{e\}$ werkt en $\sigma \neq \mathrm{id}$, moet wel gelden dat $b = e$, oftewel $\sigma(a) = a^{-1}$.

Hiermee is dus bewezen dat G een Abelse groep is. □

Stelling 2.31. *Laat $(B, +, \cdot, 0, 1)$ een linker bijna-lichaam zijn, dan is $(B, +, 0)$ een Abelse groep.*

Bewijs. Beschouw B als een paar (B^+, Λ_B), zoals in stelling 2.25, dus $\Lambda_B\backslash\{0\}$ is een ondergroep van $\mathrm{Aut}(B^+)$. Volgens stelling 2.27 geldt dat $\Lambda_B\backslash\{0\}$ vrij en transitief op $B^+\backslash\{0\}$ werkt. Dus lemma 2.30 geeft ons dat $(B, +, 0)$ een Abelse groep is. □

Stelling 2.32. *Laat D een delingsring zijn en $\rho : D^* \to \mathrm{Aut}(D)$ een afbeelding zo dat voor elke $a, b \in D^*$ geldt dat $\rho(a) \circ \rho(b) = \rho(a \cdot \rho(a)(b))$. Definieer $* : D \times D \to D$ als volgt:*

$$\forall a, b \in D : \ a * b = \begin{cases} 0, & \text{als } a = 0 \\ a \cdot \rho(a)(b), & \text{als } a \neq 0 \end{cases}$$

Nu geldt dat $\rho(1) = \mathrm{id}$ en dan is $(D, +, *, 0, 1)$ een linker bijna-lichaam. Bijna-lichamen die op deze manier verkregen kunnen worden, noemen we Dicksonse *bijna-lichamen.*

Bewijs. Merk op dat $\rho(a) \circ \rho(1) = \rho(a \cdot \rho(a)(1)) = \rho(a)$, dus omdat $\mathrm{Aut}(D)$ een groep is, moet gelden dat $\rho(1) = \mathrm{id}$. Het is meteen duidelijk dat $(D, +, 0)$ een Abelse groep is en $1 \neq 0$. Laat $a \in D^*$ willekeurig gegeven zijn. Er geldt $1 * a = 1 \cdot \rho(1)(a) = \mathrm{id}(a) = a$ en $a * 1 = a \cdot \rho(a)(1) = a \cdot 1 = a$, want $\rho(a)$ is een homomorfisme. Ook geldt voor alle $a, b \in D^*, c \in D$

$$a * (b * c) = a \cdot \rho(a)(b \cdot \rho(b)(c)) = (a \cdot \rho(a)(b)) \cdot \rho(a)(\rho(b)(c)) = (a \cdot \rho(a)(b)) \cdot (\rho(a) \circ \rho(b))(c)$$

en

$$(a * b) * c = (a \cdot \rho(a)(b)) \cdot \rho(a \cdot \rho(a)(b))(c) = (a \cdot \rho(a)(b)) \cdot (\rho(a) \circ \rho(b))(c)$$

Aangezien het geval $(a * b) * c = a * (b * c)$ triviaal is als $a = 0$ of $b = 0$, geldt voor alle $a, b, c \in D$ dat $a * (b * c) = (a * b) * c$. Omdat we voor alle $a \in D^*$ weten dat $\rho(a)$ een automorfisme is, is er een $a' \in D$ zo dat $\rho(a)(a') = a^{-1}$.

Dus $a * a' = a \cdot \rho(a)(a') = a \cdot a^{-1} = 1$, oftewel a' is een linker inverse voor a met betrekking tot $*$. De groepentheorie geeft ons nu dat als er een linker inverse bestaat, dat er ook een rechter inverse bestaat en dat deze bovendien gelijk zijn. Nu volgt dus dat $(D, +, *, 0, 1)$ een linker bijna-lichaam is. □

We zullen nu een aantal constructies van Dicksonse bijna-lichamen geven.

Voorbeeld 2.33. 1. $(\mathbb{F}_9, +, \cdot, 0, 1)$ uit voorbeeld 2.5 is een Dicksons bijna-lichaam. We zullen dit laten zien door een constructie te geven van een bijna-lichaam $(\mathbb{F}_9, +, *, 0, 1)$ zo dat $* = \circ$ als operators. We weten dat $\mathrm{Aut}(\mathbb{F}_9) = \langle \mathrm{Frob} \rangle$, waarbij Frob: $\mathbb{F}_9 \to \mathbb{F}_9, x \mapsto x^3$ het Frobenius automorfisme is. Bovendien weten we ook dat Frob als de identiteit op $\mathbb{F}_3$ werkt, dus geldt: Frob $= (x \mapsto \overline{x})$ (met $\overline{x}$ als in voorbeeld 2.5). (Aangezien ook $[\mathbb{F}_9 : \mathbb{F}_3] = 2$.) Laat nu $\rho : \mathbb{F}_9^* \to \mathrm{Aut}(\mathbb{F}_9)$ gegeven door $\rho(x) = \mathrm{id}$ als $x \in \langle i \rangle$, $\rho(x) = \mathrm{Frob}$ als $x \notin \langle i \rangle$, met $\langle i \rangle$ de ondergroep van $\mathbb{F}_9^*$ voortgebracht door i. Merk op dat ρ een homomorfisme is. Bovendien geldt dat $\forall \sigma \in \rho(K^*) : \rho \circ \sigma = \rho$ (want $\rho \circ \mathrm{id} = \rho$ en $\rho \circ \mathrm{Frob}(x) = \rho(\overline{x}) = \rho(x)$). Nu volgt dus dat $\rho(a \cdot \rho(a)(b)) = \rho(a) \circ \rho(\rho(a)(b)) = \rho(a) \circ \rho(b) = \rho(a \cdot b)$. Dus ρ geeft ons een Dicksons bijna-lichaam $(\mathbb{F}_9, +, *, 0, 1)$, waarbij $* : \mathbb{F}_9 \times \mathbb{F}_9 \to \mathbb{F}_9$ als volgt gedefinieerd is:

$$\forall a, b \in \mathbb{F}_9 : \ a * b = \begin{cases} 0, \text{ als } a = 0 \\ a \cdot \rho(a)(b), \text{ als } a \neq 0 \end{cases}$$

oftewel

$$\forall a, b \in \mathbb{F}_9 : \ a * b = \begin{cases} 0, \text{ als } a = 0 \\ a \cdot b, \text{ als } a \in \langle i \rangle \\ a \cdot \overline{b}, \text{ als } a \neq 0 \text{ en } a \notin \langle i \rangle \end{cases}$$

Maar dan geldt dus dat $\circ = *$, dus $(\mathbb{F}_9, +, \circ, 0, 1)$ is een Dicksons bijna-lichaam.

2. Laat K een willekeurig lichaam zijn, we zullen $\mathrm{Aut}_K(K(t)) = \{\sigma \in \mathrm{Aut}(K(t)) \mid \sigma|_K = \mathrm{id}\}$ bepalen. Aangezien elk element in $K(t)$ uitgedrukt kan worden in t en elementen uit K, weten we dat elk homomorfisme bepaald wordt door zijn beeld onder t. Laat $\sigma \in \mathrm{Aut}_K(K(t))$ willekeurig gegeven zijn, dan weten we, omdat $\sigma(t) \notin K$, dat er $f, g \in K[t]$ copriem en niet beide in K zijn, zo dat $\sigma(t) = \frac{f}{g}$. Bovendien geldt $[K(t) : K(\frac{f}{g})] = \max\{\deg(f), \deg(g)\}$, dus omdat σ een automorfisme van $K(t)$ is, moet gelden dat $K(\frac{f}{g}) = K(t)$, oftewel f en g hebben een graad van ten hoogste 1. Dus $\sigma(t) = \frac{at+b}{ct+d}$ voor zekere $a, b, c, d \in K$. Bovendien geldt $ad - bc \neq 0$, want f en g zijn copriem.

   We construeren nu een Dicksons bijna-lichaam voor $K = \mathbb{F}_2$. Merk op dat omdat $\mathbb{F}_2$ een priemlichaam is, we hebben dat $\mathrm{Aut}_{\mathbb{F}_2}(\mathbb{F}_2(t)) = \mathrm{Aut}(\mathbb{F}_2(t))$. Laat nu $\sigma \in \mathrm{Aut}(\mathbb{F}_2(t))$ gegeven zijn door $\sigma(t) = t + 1$. Dan geldt bovendien dat $\sigma^2(t) = \sigma \circ \sigma(t) = \sigma(t + 1) = t$, dus $\sigma^2 = \mathrm{id}$. We geven de functie ord: $\mathbb{F}_2[t] \to \mathbb{Z}$ als het aantal irreducibele factoren in een polynoom (met multipliciteit meegerekend). Dit laat zich uitbreiden tot een functie ord: $\mathbb{F}_2(t) \to \mathbb{Z}$, $\mathrm{ord}(\frac{f}{g}) = \mathrm{ord}(f) - \mathrm{ord}(g)$, met $f, g \in \mathbb{F}_2[t]$. Merk bovendien op dat $\mathrm{ord}(s_1 \cdot s_2) = \mathrm{ord}(s_1) + \mathrm{ord}(s_2)$. Definiëer nu de functie $\rho : \mathbb{F}_2(t)^* \to \mathrm{Aut}(\mathbb{F}_2(t))$ als $\rho(s) = \sigma^{\mathrm{ord}(s)}$. Dan geldt dus $\rho(1) = \mathrm{id}$ en voor alle $s_1, s_2 \in \mathbb{F}_2(t)^* \backslash \{1\} : \rho(s_1) \circ \rho(s_2) = \sigma^{\mathrm{ord}(s_1)} \circ \sigma^{\mathrm{ord}(s_2)} = \sigma^{\mathrm{ord}(s_1 \cdot s_2)} = \rho(s_1 \cdot s_2)$, dus ρ is een homomorfisme.

Bovendien geldt dat $\rho \circ \sigma = \rho$, omdat σ een automorfisme is en dus het aantal irreducibele elementen in de teller en noemer gelijk houdt. Net zoals in voorbeeld 1. voldoet ρ dus aan de eigenschap die geëist wordt voor de Dickson constructie. Dus krijgen we een Dicksons bijna-lichaam $(\mathbb{F}_2(t), +, *, 0, 1)$, waarbij $* : \mathbb{F}_2(t) \times \mathbb{F}_2(t) \to \mathbb{F}_2(t)$ gedefinieerd is als volgt:

$$\forall a, b \in \mathbb{F}_2(t) : a * b = \begin{cases} 0, \text{ als } a = 0 \\ a \cdot b, \text{ als } 2 \mid \text{ord}(a) \\ a \cdot \sigma(b), \text{ als } 2 \nmid \text{ord}(a) \end{cases}$$

3. Merk op dat de voorgaande constructie ook werkt voor $\mathbb{Q}(t)$ of $\mathbb{F}_p(t)$, p priem, met elke σ waarvoor geldt dat ord invariant is onder σ.

4. We zullen nu een ander bijna-lichaam construeren voor $\mathbb{Q}(t)$. Laat $p \in \mathbb{Z}$ een willekeurig gegeven priemgetal zijn en laat $\sigma \in \text{Aut}(\mathbb{Q}(t)) = \text{Aut}_{\mathbb{Q}}(\mathbb{Q}(t))$ gegeven zijn door $\sigma(t) = t+p$. Merk op dat elke $x \in \mathbb{Q}[t]\backslash\{0\}$ te schrijven is als $x = p^k \cdot s_x$, voor zekere $k \in \mathbb{Z}$ en $s_x = \sum_{i=0}^{n} \frac{a_i}{b_i} t^i$, met $n \in \mathbb{Z}_{\geq 0}$ en $a_i, b_i \in \mathbb{Z}$ zo dat $p \nmid a_n$ en $p \nmid b_n$. Omdat elke $z \in \mathbb{Q}(t)\backslash\{0\}$ te schrijven is als $\frac{x}{y}$ voor zekere $x, y \in \mathbb{Q}[t]\backslash\{0\}$, kunnen we z schrijven als $z = p^k \cdot \frac{s_x}{s_y}$ voor zekere $k \in \mathbb{Z}$ en met s_x en s_y als hierboven. We definiëren nu $\rho : \mathbb{Q}(t)^* \to \text{Aut}(\mathbb{Q}(t))$ als $\rho(p^k s') = \sigma^k$ (met $s' = \frac{s_x}{s_y}$ als voorheen). Nu volgt dat voor elke $x, y \in \mathbb{Q}(t)\backslash\{0\}$ er geldt $\rho(xy) = \rho(p^{k_x} s_x \cdot p^{k_y} s_y) = \rho(p^{k_x+k_y} s_x s_y) = \sigma^{k_x+k_y} = \sigma^{k_x} \circ \sigma^{k_y} = \rho(x) \circ \rho(y)$, dus ρ is een homomorfisme. Merk bovendien op dat voor elke $a, b, k \in \mathbb{Z}$ met $p \nmid a$ en $p \nmid b$ geldt $\sigma(\frac{a}{b} t^k) = \frac{a}{b}(t+p)^k$, maar dat betekent dus dat de coëfficiënt voor t^k in $\frac{a}{b}(t+p)^k$ gelijk is aan $\frac{a}{b}$. Omdat elk element $x \in \mathbb{Q}(t)$ dus geschreven kan worden als $x = p^k \cdot \frac{s_1}{s_2}$, weten we bovendien $\sigma(x) = p^k \cdot \frac{\sigma(s_1)}{\sigma(s_2)}$. Dus omdat s_1 en s_2 beide van de vorm $\sum_{i=0}^{n} \frac{a_i}{b_i} t^i$ met $p \nmid a_n$ en $p \nmid b_n$ zijn, zien we dat $\sigma(s_1)$ en $\sigma(s_2)$ beide als coëfficiënt van de term met de hoogste graad een getal van de vorm $\frac{a}{b}$ hebben met $p \nmid a$ en $p \nmid b$. Dan weten we ook dat $\rho \circ \sigma(p^k s) = \rho(p^k \sigma(s)) = \sigma^k = \rho(p^k s)$, oftewel $\rho \circ \sigma = \rho$. Dus bovendien geldt $\rho(a \cdot \rho(a)(b)) = \rho(a) \circ \rho(b)$, en krijgen we dat $(\mathbb{Q}(t), +, *, 0, 1)$ een Dicksons bijna-lichaam is, met $* : \mathbb{Q}(t) \times \mathbb{Q}(t) \to \mathbb{Q}(t)$ gedefinieerd als:

$$\forall a, b \in \mathbb{Q}(t) : \quad p^{k_a} s_a * p^{k_b} s_b = \begin{cases} 0, \text{ als } a = 0 \\ a \cdot \sigma^{k_a}(b), \text{ anders} \end{cases}$$

Merk op dat deze constructie nog steeds werkt als we naar eindig veel priemgetallen als factoren kijken (met bijbehorende automorfismen). Wel moet men controleren dat zulke automorfismen commuteren en bovendien moet elk van deze automorfismen γ voldoen aan de regel $\rho \circ \gamma = \rho$.

5. We zullen nu Dicksonse bijna-lichamen maken uit de delingsring $\mathbb{H}$ van de quaternionen. Merk op dat als $f \in \mathrm{Aut}(\mathbb{H})$, dan weten we dat voor elke $x \in \mathbb{R}$ geldt dat $x \in Z(\mathbb{H})$ dan en slechts dan als $f(x) \in Z(\mathbb{H})$. Oftewel $f|_{\mathbb{R}}$ is een automorfisme van $\mathbb{R}$, maar omdat id het enige automorfisme op $\mathbb{R}$ is, moet f dus $\mathbb{R}$-lineair zijn (als $\mathbb{R}$-algebra). Nu geeft de stelling van Skolem-Noether ons dat er een $q \in \mathbb{H}^*$ zo dat er voor alle $x \in \mathbb{H}$ geldt $f(x) = q \cdot \mathrm{id}(x) \cdot q^{-1} = qxq^{-1}$, omdat $\mathrm{id} \in \mathrm{Aut}(\mathbb{H})$. Nu weten we dus dat alle automorfismen van $\mathbb{H}$ inwendig zijn. Schrijf dan f_q voor het inwendige automorfisme gegeven door $q \in \mathbb{H}^*$. We zullen nu ρ gaan definiëren als samenstelling van homomorfismen. Als eerste, schrijven we voor alle $a, b, c, d \in \mathbb{R} : \overline{a + bi + cj + dk} = a - bi - cj - dk$, dan vinden we dat er een homomorfisme $\phi : \mathbb{H}^* \to \mathbb{R}^*_{>0}, x \mapsto x \cdot \overline{x}$. Ook $\psi_t : \mathbb{R}^*_{>0} \to \mathbb{C}^*, z \mapsto z^t$ is voor elke $t \in \mathbb{C}$ een homomorfisme, met $z^t = e^{t \log(z)}$. Vervolgens hebben we nog de natuurlijke homomorfismen $\tau : \mathbb{C}^* \to \mathbb{C}^*/\mathbb{R}^*$ en $\iota : \mathbb{C}^*/\mathbb{R}^* \to \mathbb{H}^*/\mathbb{R}^*$ (waarbij ι dus de inclusie is).
Als laatste is $\zeta : \mathbb{H}^*/\mathbb{R}^* \to \mathrm{Aut}(\mathbb{H}), q\mathbb{R}^* \mapsto f_q$ een isomorfisme, want alleen elementen van $\mathbb{R}^*$ liggen in het centrum van $\mathbb{H}^*$. Nu is dan $\rho = \zeta \circ \iota \circ \tau \circ \psi_t \circ \phi$ een homomorfisme. We zullen bewijzen dat voor elke $a, b \in \mathbb{H}$ er geldt $\rho \circ \rho(a) = \rho$, oftewel $\rho(\rho(a)(b)) = \rho(b)$. Hiervoor zullen we ook het homomorfisme $\rho' = \zeta \circ \iota \circ \tau \circ \psi_t$ gebruiken.

   We weten dat $\rho(a)(b) = qbq^{-1}$ voor zekere $q \in \mathbb{H}^*$, dus dan geldt het volgende:

$$\begin{aligned}
\rho(\rho(a)(b)) &= \rho'(\rho(a)(b)\overline{\rho(a)(b)}) \\
&= \rho'(qbq^{-1} \cdot \overline{q^{-1}}\overline{b}\overline{q}) \\
&= \rho'(b\overline{b}) \\
&= \rho(b)
\end{aligned}$$

   Want $x\overline{x} \in \mathbb{R}^*_{>0}$. Dus dan is $(\mathbb{H}, +, *, 0, 1)$ een Dicksons bijna-lichaam met $* : \mathbb{H} \times \mathbb{H} \to \mathbb{H}$ gegeven door

$$\forall a, b \in \mathbb{H} : a * b = \begin{cases} a \cdot \rho(a)(b), \text{ als } a \neq 0 \\ 0, \text{ als } a = 0 \end{cases}$$

   We geven ook een concrete uitwerking voor $t = \frac{1}{2}\pi i$ en $a = \sqrt{e}$ en $b = j$. Dan vinden wij $\rho(\sqrt{e}) = f_{e^{\frac{1}{2}\pi i}} = f_i$, dus $\sqrt{e} * j = \sqrt{e} \cdot f_i(j) = \sqrt{e} \cdot i \cdot j \cdot -i = \sqrt{e} \cdot k \cdot -i = -\sqrt{e}j$

Stelling 2.34 (Zassenhaus)**.** *Er zijn precies 7 paarsgewijs niet-isomorfe eindige niet-Dicksonse bijna-lichamen. We geven deze als volgt in de vorm van* (G, Λ)*, zoals in stelling 2.25:*

- $G = C_5^2$, $\Lambda = 2T$
- $G = C_{11}^2$, $\Lambda = 2T \times C_5$
- $G = C_7^2$, $\Lambda = 2O$
- $G = C_{23}^2$, $\Lambda = 2O \times C_{11}$
- $G = C_{11}^2$, $\Lambda = 2I$
- $G = C_{29}^2$, $\Lambda = 2I \times C_7$
- $G = C_{59}^2$, $\Lambda = 2I \times C_{29}$

waarbij C_p *de cyclische groep van orde* p *is en* $2T, 2O$ *en* $2I$ *zijn respectievelijk de binaire tetraëdergroep, de binaire octaëdergroep en de binaire icosaëdergroep. In dit geval kiezen we als multiplicatieve eenheid, een element van* G *ongelijk aan het additieve eenheidselement.*

Deze tabel is in [4] ook te vinden, hierin wordt bovendien verder ingegaan op de structuur van deze bijna-lichamen. Zie ook [3] voor verdere toelichting, definities van de groepen en het bewijs van deze stelling.

3 Scherp tweevoudig transitieve werkingen

3.1 Introductie

We gaan in dit hoofdstuk eerst definiëren wat een *scherp tweevoudig transitieve werking* is. Later zullen we bewijzen dat er een 1-op-1 correspondentie op isomorfie na is tussen eindige bijna-lichamen en eindige scherp tweevoudig transitieve werkingen. Dit feit is al langer bekend, zie bijvoorbeeld [3]. Minder lang is bekend dat niet alle scherp tweevoudig transitieve werkingen ook aanleiding tot een bijna-lichaam geven. Wel zullen we zogenaamde *sterke* scherp tweevoudig transitieve werkingen tegenkomen, welke wel allemaal aanleiding geven tot een bijna-lichaam. Voor verdere literatuur over dit onderwerp, zie [2]. De stellingen 3.10 en 3.15 zullen concreet deze correspondenties geven.

3.2 Relatie tussen bijna-lichamen en scherp tweevoudig transitieve werkingen

Laat G een groep zijn en X een verzameling. Stel dat G op X werkt, dan is er een geïnduceerde werking van G op $(X \times X)\backslash\Delta$, met $\Delta = \{(x, x) \mid x \in X\}$. Deze wordt gegeven door voor elke $x, y \in X$ met $x \neq y$ en $g \in G$ de werking gegeven te laten zijn door de coördinaatsgewijze werking: $g \cdot (x, y) = (gx, gy)$. Deze werking is welgedefinieerd, omdat de functie $f : X \to X, x \mapsto g \cdot x$ een bijectie is, dus $g(x, y) \notin \Delta$.

Definitie 3.1. Laat G een groep zijn en X een verzameling. Een *scherp tweevoudig transitieve* werking van G op X is een werking, zo dat de geïnduceerde werking van G op $(X \times X)\backslash\Delta$ transitief en vrij is. Oftewel voor alle $z_1, z_2 \in (X \times X)\backslash\Delta$ is er een $g \in G$ zo dat $gz_1 = z_2$ en voor alle $g, h \in G$ geldt dat als er een $z \in (X \times X)\backslash\Delta$ is zo dat $gz = hz$, dan geldt ook dat $g = h$.

We zullen eerst laten zien dat elk bijna-lichaam aanleiding geeft tot een scherp tweevoudig transitieve werking.

Propositie 3.2. *Laat B een linker bijna-lichaam zijn. Definieer $G = \{\sigma_{a,b} \mid a \in B^*, b \in B\}$, met $\sigma_{a,b} : B \to B, x \mapsto ax + b$. Dan is G een groep en er is een natuurlijke werking van G op B, deze is bovendien scherp tweevoudig transitief.*

Bewijs. Duidelijk geldt voor alle $a, a' \in B^*$ en $b, b', z \in B$ dat

$$\sigma_{a,b} \circ \sigma_{a',b'}(z) = \sigma_{a,b}(a'z + b') = aa'z + ab' + b = \sigma_{a \cdot a', ab'+b}(z)$$

dus $\sigma_{a,b} \circ \sigma_{a',b'} \in G$. Bovendien vinden we $\sigma_{1,0} = \mathrm{id}$ en $\sigma_{a,b} \circ \sigma_{a^{-1},-a^{-1}b} = \mathrm{id}$, dus G is een groep. Bovendien geldt dat elke $\sigma \in G$ een bijectie is, dus G is een ondergroep van $S(B)$ en dit geeft dus de natuurlijke werking van G op B. Beschouw nu de werking van G op $(B \times B)\backslash\Delta$. Laat $\sigma_{a,b} \in G$ willekeurig gegeven zijn. Stel nu dat er voor zekere $x, y \in B$ met $x \neq y$ geldt dat $\sigma_{a,b}(x, y) = (x, y)$, dan geldt dus $ax + b = x$ en $ay + b = y$, dus $a(x - y) = ax - ay = x - y$, dus omdat $x - y \neq 0$, weten we dat $(x - y)^{-1} \in B$ en dan volgt dus dat $a = 1$. Aangezien dus geldt dat $x + b = x$ en $y + b = y$, volgt meteen dat $b = 0$. Dus G werkt vrij op $(B \times B)\backslash\Delta$. Merk op dat voor elke $x \in B^*$ geldt dat $\sigma_{x,0}(1, 0) = (x, 0)$, $\sigma_{-x,x}(1, 0) = (0, x)$. Laat nu $x, y \in B^*$ met $x \neq y$ willekeurig gegeven zijn, dan vinden we $\sigma_{x,y}\sigma_{1-x^{-1}y,0}(1, 0) = \sigma_{x,y}(1 - x^{-1}y, 0) = (x, y)$. Gecombineerd met de vorige opmerking, vinden we dat $G(1, 0) = B$. Dus de werking van G op $(B \times B)\backslash\Delta$ is transitief. Nu hebben we dus bewezen dat de werking van G op B scherp tweevoudig transitief is. □

Er is ook al bekend dat er een omgekeerd proces is, dat bij een scherp tweevoudig transitieve werking van een groep G op een verzameling X een bijna-lichaam geeft, als G en X eindig zijn. Hiervoor moeten we een zwakkere versie van de stelling van Frobenius gebruiken. Deze versie is zwakker, omdat we hem niet voor alle Frobenius groepen gaan bewijzen, maar alleen voor eindige groepen met een scherp tweevoudig transitieve werking.

Definitie 3.3. Laat G een groep zijn en X een verzameling. Als G op X werkt en $g \in G$ gegeven is, dan is de verzameling van *vaste punten* onder g gegeven als:

$$X^g = \{x \in X \mid gx = x\}$$

Definitie 3.4 (Frobenius groep en kern)**.** Een *Frobenius groep* is een eindige groep G die werkt op een eindige verzameling X zo dat voor elke $g \in G\backslash\{e\}$ geldt dat $|X^g| \leq 1$. De *Frobenius kern* van G is $N = \{g \in G \mid X^g = \varnothing\} \cup \{e\}$.

Lemma 3.5. *Een scherp tweevoudig transitieve werking is ook transitief. Bovendien is een eindige groep met een scherp tweevoudig transitieve werking op een eindige verzameling ook een Frobenius groep.*

Bewijs. Laat G een groep zijn, X een verzameling en neem aan dat er een scherp tweevoudig transitieve werking van G op X is. Dan geldt dat voor elke $x_1, x_2, y_1, y_2 \in X$ met $x_1 \neq y_1$ en $x_2 \neq y_2$, er een $g \in G$ is zo dat $g(x_1, y_1) = (gx_1, gy_1) = (x_2, y_2)$, oftewel $gx_1 = x_2$. Dus G werkt transitief op X. Laat $g \in G$ willekeurig gegeven zijn en stel dat er $x, y \in X$ zijn met $x \neq y$ zo dat $gx = x$ en $gy = y$, oftewel dat g minstens twee vaste punten heeft. Omdat G vrij op $(X \times X)\backslash\Delta$ werkt, geldt dus dat $g = e$, omdat $g(x, y) = (x, y)$. Dus voor elke $g \in G\backslash\{e\}$ geldt $|X^g| \leq 1$. Als G en X dan ook eindig zijn, is G dus een Frobenius groep. □

Definitie 3.6 (Stabilisator en baan)**.** Laat G een groep zijn die werkt op een verzameling X. Voor elke $x \in X$ is de *stabilisator* van x gedefinieerd als:

$$G_x := \{g \in G \mid gx = x\}$$

en de *baan* van x is gedefinieerd als:

$$Gx := \{gx \mid g \in G\}$$

Uit de groepen theorie weten we bovendien dat elke stabilisator een groep is. Merk voor de volgende stelling ook op dat er geen verzameling X is met $|X| = 1$, zodat er een groep G is die scherp tweevoudig transitief werkt op X.

Stelling 3.7 (Frobenius)**.** *Laat G een groep zijn die scherp tweevoudig transitief werkt op een eindige verzameling X, dan is de Frobenius kern N een abelse normaaldeler van orde $|X|$. Bovendien werkt N, via de geïnduceerde werking van G, transitief en vrij op X. Ook geldt voor elke $x \in X$ dat $|G_x| = |X| - 1$ en dat G_x transitief en vrij op $N\backslash\{e\}$ werkt via conjugatie.*

Bewijs. Laat G een eindige groep zijn, X een eindige verzameling en schrijf $n = |X|$.

Laat $\sigma, \tau \in G$ willekeurig gegeven zijn, dan geldt voor elke $x \in X^\sigma$ geldt dat $\tau\sigma\tau^{-1}(\tau x) = \tau x$, dus $\tau x \in X^{\tau\sigma\tau^{-1}}$. Ook geldt voor elke $y \in X^{\tau\sigma\tau^{-1}}$ dat $\sigma\tau^{-1}y = \tau^{-1}y$, dus $\tau^{-1}y \in X^\sigma$, oftewel $y \in \tau(X^\sigma)$. Nu vinden we dus dat $\tau(X^\sigma) = X^{\tau\sigma\tau^{-1}}$. Laat nu $\tau \in G$ en $\sigma \in N\backslash\{e\}$ willekeurig gegeven zijn, dan vinden we dus $X^{\tau\sigma\tau^{-1}} = \tau(X^\sigma) = \varnothing$, oftewel $\tau\sigma\tau^{-1} \in N$. Maar dan weten we dus dat G op $N\backslash\{e\}$ werkt via conjugatie.

Omdat G scherp tweevoudig transitief werkt op X, werkt hij ook transitief op X. Ook weten we dat $|G| = |(X \times X)\backslash\Delta| = n^2 - n = n(n-1)$. Laat $x \in X$ willekeurig gegeven zijn. Aangezien G transitief op X werkt, weten we ook dat er maar 1 baan is, dus $|Gx| = |X| = n$. Bovendien geldt voor alle eindige groepswerkingen dat $|Gx| \cdot |G_x| = |G|$, dus nu weten we dat $|G_x| = n - 1$.
Verder werkt G_x natuurlijk vrij op $X\backslash\{x\}$, aangezien voor elke $\sigma \in G\backslash\{e\}$ geldt dat $|X^\sigma| \leq 1$, dus in het bijzonder geldt voor elke $\sigma \in G_x\backslash\{e\}$ dat $|X^\sigma| = 1$. Dus omdat $|G_x| = |X\backslash\{x\}|$, moet deze werking ook transitief zijn. Laat $\sigma \in G_x\backslash\{e\}$ en $\tau \in N\backslash\{e\}$ willekeurig gegeven zijn.
Omdat $\tau x \neq x$, vinden we dat geldt $\sigma\tau x \neq \tau x = \tau\sigma x$, maar dan geldt dus $\tau\sigma \neq \sigma\tau$, oftewel $\sigma\tau\sigma^{-1} \neq \tau$. Omdat G op $N\backslash\{e\}$ werkt via conjugatie, werkt G_x ook op $N\backslash\{e\}$ via conjugatie. Bovendien weten we dus dat deze werking vrij is. Omdat G een Frobenius groep is, weten we dat elk element van $G\backslash\{e\}$ hoogstens 1 vast punt heeft, dus $G\backslash N = \bigcup_{y\in X} G_y\backslash\{e\}$. Bovendien geldt voor elke $y, z \in X$ met $y \neq z$ dat $G_y \cap G_z = \{e\}$, want G is een Frobenius groep. Nu vinden we dus $|N| = |G| - |G\backslash N| = n(n-1) - n(n-2) = n$. Omdat G_x vrij werkt op $N\backslash\{e\}$ en ook $|G_x| = |N\backslash\{e\}|$ weten we dat G_x bovendien transitief werkt op $N\backslash\{e\}$.

Laat nu $\tau \in N\backslash\{e\}$ willekeurig gegeven zijn en beschouw dan de centralisator van τ onder de conjugatiewerking van G:

$$H = C_G(\tau) = \{\sigma \in G \mid \sigma\tau\sigma^{-1} = \tau\}$$

Eerder hadden we al gezien dat $G\backslash N = \bigcup_{y\in X} G_y\backslash\{e\}$. Laat $\sigma \in G\backslash N$ willekeurig gegeven zijn, dan is er een $y \in X$ zo dat $\sigma \in G_y$. Nu zien we dat $\tau\sigma y = \tau y \neq \sigma\tau y$, want $\tau y \neq y$. Dus moet wel gelden dat $\tau\sigma \neq \sigma\tau$, oftewel $\sigma\tau\sigma^{-1} \neq \tau$. Maar dan vinden we dus dat moet gelden $H \subset N$. Omdat G_x transitief op $N\backslash\{e\}$ werkt, geldt in het bijzonder dat G ook transitief op $N\backslash\{e\}$ werkt. Dus de enige baan van deze werking is $N\backslash\{e\}$. Dit geeft ons dus dat $|G| = |H| \cdot |N\backslash\{e\}|$, oftewel $|H| = n = |N|$. Maar dan moet ook gelden $H = N$. Omdat de centralisator H een stabilisator voor de conjugatie werking van G op $N\backslash\{e\}$ is, is H in het bijzonder een ondergroep van G. Nu vinden we dus dat N een Abelse ondergroep is, omdat voor elke $\sigma, \tau \in N$ geldt $\sigma\tau\sigma^{-1} = \tau$, oftewel $\sigma\tau = \tau\sigma$. Bovendien is N een normaaldeler, omdat de conjugatie van G op $N\backslash\{e\}$ een werking geeft.

Het is duidelijk dat de werking van N op X (geïnduceerd door de G werking op X) vrij is. Omdat bovendien geldt dat $|N| = |X|$, weten we dat N ook transitief op X werkt. □

Gevolg 3.8. *Laat G een eindige groep zijn en X een eindige verzameling. Stel dat er een scherp tweevoudig transitieve werking van G op X is. Laat $x \in X$ willekeurig gegeven zijn, dan is er een injectief homomorfisme $\phi : G_x \to \mathrm{Aut}(N)$, waarbij N de Frobenius kern van G is. Kies een element $1 \in N$ met $1 \neq e$ en schrijf $0 = e$, dan vinden we dat $(N, +, \cdot, 0, 1)$ een linker bijna-lichaam is, waarbij $+ : N \times N \to N$ de groepsoperatie van N is en $\cdot : N \times N \to N$ gegeven is als $x \cdot y = \mathrm{ev}_1^{-1}(x)(y)$, met $\mathrm{ev}_1 : \phi(G_x) \cup \{(x \mapsto 0)\} \to N, f \mapsto f(1)$.*

Bewijs. Aangezien G_x via conjugatie op $N\backslash\{e\}$ vrij en transitief werkt, geeft elk element $\sigma \in G_x$ een automorfisme $f_\sigma : N \to N, n \mapsto \sigma n\sigma^{-1}$. Op deze manier kunnen we G_x als ondergroep van $\mathrm{Aut}(N)$ opvatten, oftewel $\phi : G_x \to \mathrm{Aut}(N), \sigma \mapsto f_\sigma$ is een injectief homomorfisme. Bovendien is deze ondergroep $\phi(G_x)$ van $\mathrm{Aut}(N)$ onafhankelijk van de keuze van x. We kunnen namelijk ϕ uitbreiden tot een homomorfisme $\phi : G \to \mathrm{Aut}(N), \sigma \mapsto f_\sigma$ (omdat G ook transitief op $N\backslash\{e\}$ via conjugatie werkt). Omdat N abels is, weten we dat $N \subseteq \ker(\phi)$. Laat dan $y \in X$ willekeurig gegeven zijn, dan geldt omdat N transitief op X werkt, dat er een $\tau \in N$ is zo dat $\tau x = y$, dus $G_y = G_{\tau x} = \tau G_x \tau^{-1}$. Nu volgt dus $\phi(G_y) = \phi(\tau G_x \tau^{-1}) = \phi(G_x)$. Oftewel de ondergroep $\phi(G_x)$ is inderdaad onafhankelijk van de keuze van x. Laat nu $\Lambda = \phi(G_x) \cup \{(x \mapsto 0)\}$. Omdat (N, Λ) voldoet aan de eisen van stelling 2.28, vinden we dat $(N, +, \cdot, 0, 1)$ een bijna-lichaam is. □

Merk op dat de bijna-lichaam structuur op N afhangt van de keuze van het element 1. Wel zullen alle mogelijke bijna-lichamen op N via de werking van G op X isomorf met elkaar zijn.

Propositie 3.9. *Laat G een eindige groep zijn die scherp tweevoudig transitief werkt op een eindige verzameling X. Laat ook $x, y \in N$ met $x \neq 0$ en $y \neq 0$ willekeurig gegeven zijn. De resulterende linker bijna-lichamen $(N, +, \cdot, 0, x)$ en $(N, +, \cdot, 0, y)$ zijn isomorf.*

Bewijs. Laat $z \in X$ willekeurig gegeven zijn, dan krijgen we de twee bijna-lichamen door de werking van G_z op N. Omdat deze werking vrij en transitief is, is er een unieke $g \in G_z$ zo dat $gxg^{-1} = y$. De functie $f_g : N \to N, n \mapsto gng^{-1}$ is een groepsautomorfisme dat x naar y stuurt. Omdat $f_g \in \phi(G_z)$, vinden we dat voor elke $n, n' \in N$ geldt, met $h \in G_z$ zo dat $hxh^{-1} = n$:

$$\begin{aligned} f_g(n \cdot n') &= f_g(f_h(n')) \\ &= ghn'h^{-1}g^{-1} \\ &= ghg^{-1} \cdot gn'g^{-1} \cdot gh^{-1}g \\ &= f_{ghg^{-1}}(f_g(n')) \\ &= f_{ghg^{-1}}(y) \cdot f_g(n') \\ &= f_{gh}(x) \cdot f_g(n') \\ &= f_g(n) \cdot f_g(n') \end{aligned}$$

Dus nu is hebben we bewezen dat f_g zelfs een bijna-lichaamsisomorfisme is van $(N, +, \cdot, 0, x)$ naar $(N, +, \cdot, 0, y)$. □

Deze propositie laat dus zien dat de scherp tweevoudig transitieve werking een bijna-lichaam op isomorfie na uniek bepaalt.

De correspondentie van de volgende stelling is een correspondentie in de zin dat als we met een bijna-lichaam starten en eerst propositie 3.2 en vervolgens gevolg 3.8 toepassen, we een bijna-lichaam krijgen dat isomorf is met ons originele. Andersom geldt ook dat een groep G met een scherp tweevoudig transitieve werking via gevolg 3.8 en propositie 3.2 een scherp tweevoudig transitieve werking geeft die isomorf is met de originele.

Stelling 3.10. *Er is een 1 op 1 correspondentie (op isomorfie na) tussen eindige scherp tweevoudig transitieve werkingen en eindige bijna-lichamen.*

Het bewijs van deze stelling is vooral technische controle. We laten dit over aan de lezer, waarbij men de volgende stappen kan nemen. Voor het geval waar men met een bijna-lichaam B begint en vervolgens een bijna-lichaam op de Frobenius kern N van de G behorend bij B, zoals in propositie 3.2, is het vrij simpel te bewijzen dat de afbeelding $f : N \to B, \sigma_{1,b} \mapsto b$ een bijna-lichaamsisomorfisme is.

Het bewijs voor het andere geval is wat moeilijker. Laat G een groep zijn die een scherp tweevoudig transitieve werking heeft, N zijn Frobenius kern en G_N de groep afkomstig van het bijna-lichaam $(N, +, \cdot, 0, 1)$ respectievelijk volgens propositie 3.2 en gevolg 3.8. Er moet ten eerste bewezen worden dat G en G_N semi-directe producten zijn van hun Frobenius kern en een stabilisator van de scherp tweevoudig transitieve werkingen. Nu moet een bijectie van N naar X willekeurig gegeven worden en deze legt dan op natuurlijke wijze een isomorfisme tussen de stabilisatoren van de G werking en de G_N werking vast die bovendien de werkingen respecteren via deze bijectie. Weer kan men het isomorfisme zoals f hierboven gebruiken, deze respecteert ook de werkingen. Deze twee isomorfismen leggen nu een isomorfisme op de semi-directe producten vast die bovendien de werkingen respecteert.

3.3 Oneindige werkingen

We hebben bij het proces om een bijna-lichaam te maken vanuit een eindige scherp tweevoudig transitieve werking steeds gebruik gemaakt van een Frobenius kern N. Dit werkte doordat N vrij en transitief werkte via de geïnduceerde werking. Het is dus logisch om bij een uitbreiding van dit proces voor oneindige scherp tweevoudig transitieve werkingen dit ook te gebruiken.

Definitie 3.11 (reguliere normale ondergroep)**.** Laat G een groep zijn die werkt op een verzameling X. Een reguliere normale ondergroep N is een normale ondergroep van G die regulier, oftewel vrij en transitief, werkt op X via de geïnduceerde werking.

Merk nu op dat alle Frobeniuskernen in het eindige geval dus reguliere normale ondergroepen waren. Als een groep G scherp tweevoudig transitief op een verzameling X werkt, dan vinden we bovendien voor elke $x \in X$ dat als $N \subseteq G$ een reguliere normale ondergroep is, we hebben $NG_x = G$ en $N \cap G_x = \{e\}$. Dus met de conjugatie werking van G_x op N vinden we dat $G \cong N \rtimes G_x$. Nu is meteen duidelijk dat in dit geval de constructie uit gevolg 3.8 ook werkt voor G. In het bijzonder weten we dat elk bijna-lichaam leidt tot een scherp tweevoudig transitieve werking van een groep G met een reguliere normale ondergroep.

Gevolg 3.12. *Laat $(B, +, \cdot, 0, 1)$ een linker-bijna-lichaam zijn, en $G = \{\sigma_{a,b} \mid a \in B^*, b \in B\}$ de groep die scherp tweevoudig transitief werkt op B volgens propositie 3.2. In het bijzonder is $N = \{\sigma_{1,b} \mid b \in B\}$ een reguliere normale ondergroep van G.*

Bewijs. Het is duidelijk dat $\phi : B^+ \to N, b \mapsto \sigma_{1,b}$ een groepsisomorfisme is en dat de linker reguliere werking van B^+ op B^+ overgaat in de werking van N op B (via ϕ). Dus N werkt regulier op B. Bovendien is het makkelijk na te gaan dat N normaal in G is. □

Blijkbaar is het dus zelfs noodzakelijk voor scherp tweevoudig transitieve werkingen die een bijna-lichaam kunnen geven dat er een reguliere normale ondergroep is. Dan is dus de vraag "geeft elke scherp tweevoudig transitieve werking een bijna-lichaam?" equivalent aan de vraag "heeft elke scherp tweevoudig transitieve werking een reguliere normale ondergroep?" Helaas blijkt het antwoord op deze vraag "nee" te zijn. Sterker nog, in [1] wordt de volgende stelling bewezen.

Definitie 3.13 (Involutie)**.** Laat G een groep zijn. Een involutie is een $\sigma \in G \backslash \{e\}$ zo dat $\sigma^2 = e$.

Stelling 3.14. *Elke groep G is bevat in een groep G' die scherp tweevoudig transitief werkt op een verzameling X zodat elke involutie in G' geen enkel vast punt in X heeft en dat G' geen niet triviale abelse normale ondergroep heeft.*

Omdat we weten dat elke reguliere normale ondergroep van een groep met een scherp tweevoudig transitieve werking bovendien Abels is en niet triviaal (want deze groepen geven precies de bijna-lichamen), geeft bovenstaande stelling dat niet alle scherp tweevoudig transitieve werkingen een reguliere normale ondergroep hebben en in het bijzonder dus geen bijna-lichaam geven.

Wel geldt natuurlijk de volgende stelling.

Stelling 3.15. *Er bestaat een 1 op 1 correspondentie (op isomorfie na) tussen linker bijnalichamen en scherp tweevoudig transitieve werkingen met een reguliere normale ondergroep. Deze worden op dezelfde manier gegeven als in propositie 3.2 en gevolg 3.8, waarbij de Frobenius kern vervangen wordt door een reglier normale ondergroep.*

Deze stelling is volledig ananloog te bewijzen aan stelling 3.10, als er gebruik gemaakt wordt van de feiten over de reguliere normale ondergroepen van scherp tweevoudig transitieve werkingen.

Als laatste zullen we deze speciale scherp tweevoudig transitieve werkingen nog een naam geven.

Definitie 3.16. Een *sterke* scherp tweevoudig transitieve werking is een scherp tweevoudig transitieve werking van een groep G met een reguliere normale ondergroep.

4 Categorieën

4.1 Introductie

In dit hoofdstuk laten we zien dat de correspondenties uit stellingen 3.10 en 3.15 in feite aanleiding tot equivalenties van categorieën geven. In het bijzonder geven deze dus equivalenties tussen de categorieën van eindige bijna lichamen en eindige scherp tweevoudig transitieve werkingen, dan wel tussen de categorieën van bijna-lichamen en sterke scherp tweevoudig transitieve werkingen. Dit wordt gedaan in de stellingen 4.6 en 4.7.

4.2 Equivalenties van categorieën

We zullen eerst definiëren wat de categorieën van bijna-lichamen en scherp tweevoudig transitieve werkingen zijn.

Definitie 4.1 (Categorie van bijna-lichamen)**.** We geven de categorie van bijna-lichamen aan met **BiLi**. De objecten van deze categorie zijn de linker bijna-lichamen en de morfismen zijn de homomorfismen. We geven de deelcategorie van **BiLi** van eindige bijna-lichamen aan met $\mathbf{E-BiLi}$.

Het is duidelijk dat dit daadwerkelijk categorieën zijn.

Definitie 4.2 (Categorie van sterke scherp tweevoudig transitieve werkingen)**.** We geven de categorie van sterke scherp tweevoudig transitieve werkingen aan met $\mathbf{S-STTW}$. De objecten van deze categorie zijn zestallen $(G, N, X, \phi, 1, x)$, waarbij G een groep is, N een reguliere normale ondergroep van G, X een verzameling, $\phi : G \to S(X)$ een homomorfisme dat de scherp tweevoudig transitieve werking van G op X geeft, 1 een element van N ongelijk aan het eenheidselement 0 en x een element van X. De morfismen in $\mathrm{Hom}((G, N, X, \phi, 1_G, x), (G', N, X', \phi', 1_{G'}, x'))$ zijn paren (γ, χ), waarbij $\gamma : G \to G'$ een homomorfisme van groepen is met $\gamma(1_G) = 1_{G'}$ en $\gamma(N) \subseteq N'$ en $\chi : X \to X'$ een morfisme van verzamelingen, zo dat $\chi(x) = x'$ en $\forall g \in G, \forall z \in X : \chi(\phi(g)(z)) = \phi'(\gamma(g))(\chi(z))$. De deelcategorie van eindige scherp tweevoudig transitieve werkingen geven we aan met $\mathbf{E-STTW}$. De objecten hiervan zijn $(G, N, X, \phi, 1, x)$ als in $\mathbf{S-STTW}$ waarbij ook nog vereist is dat G en X eindig zijn.

We nemen een element $x \in X$ in de objecten van $\mathbf{S-STTW}$ op, zodat dit in feite de "oriëntatie" van X vastlegt. Dat wil zeggen, we laten nu geen morfismen (γ, χ) van objecten naar zichzelf toe waarbij χ alleen de elementen van X verwisselt op een manier dat γ de werking respecteert via χ. Merk ten slotte op dat voor de objecten $(G, N, X, \phi, 1, x) \in \mathrm{Ob}(\mathbf{E-STTW})$ er altijd geldt dat N de Frobenius kern van G is, omdat voor zulke eindige groepen G er hoogstens 1 reguliere normale ondergroep is.

Lemma 4.3. *Er geldt dat* $\mathbf{S-STTW}$ *en* $\mathbf{E-SSTW}$ *categorieën zijn.*

Bewijs. Het is duidelijk dat voor elk object $C = (G, N, X, \phi, 1, x) \in \mathrm{Ob}(\mathbf{S-STTW})$ er een identiteitsmorfisme $\mathrm{id}_C = (\mathrm{id}_G, \mathrm{id}_X) \in \mathrm{Hom}(C, C)$ is. Laat $A, B, C, D \in \mathrm{Ob}(\mathbf{S-STTW})$ en $a = (\gamma_a, \chi_a) \in \mathrm{Hom}(A, B)$, $b = (\gamma_b, \chi_b) \in \mathrm{Hom}(B, C)$ en $c = (\gamma_c, \chi_c) \in \mathrm{Hom}(C, D)$ willekeurig gegeven zijn, dan geldt $(c \circ b) \circ a = (\gamma_c \circ \gamma_b, \chi_c \circ \chi_b) \circ a = (\gamma_c \circ \gamma_b \circ \gamma_a, \chi_c \circ \chi_b \circ \chi_a) = c \circ (\gamma_b \circ \gamma_a, \chi_b \circ \chi_a) = c \circ (b \circ a)$, dit geldt doordat de morfismen van $\mathbf{S-STTW}$ bestaan uit morfismen van groepen en verzamelingen, deze behouden bovendien de speciale eigenschap van morfismen van $\mathbf{S-STTW}$. Dus $\mathbf{S-STTW}$ is een categorie en $\mathbf{E-STTW}$ is een categorie als deelcategorie van $\mathbf{S-STTW}$. □

We zullen nu de functoren geven waarmee we de equivalentie van $\mathbf{E-BiLi}$ en $\mathbf{E-STTW}$ gaan aantonen.

Propositie 4.4. *Het proces uit propositie 3.2 geeft een functor* $F : \mathbf{BiLi} \to \mathbf{S-STTW}$. *Deze functor kan bovendien beperkt worden op* $\mathbf{E-BiLi}$, *zodat* $F : \mathbf{E-BiLi} \to \mathbf{E-STTW}$ *ook een functor is.*

Bewijs. Laat $(B, +, \cdot, 0, 1)$ een linker bijna-lichaam zijn, dan geeft propositie 3.2 ons een scherp tweevoudig transitieve werking $(G_B, N_B, B, \phi, \sigma_{1,1}, 0)$ die volgens gevolg 3.12 zelfs een object in $\mathbf{S-STTW}$ is. (Hier is G_B de groep werkend op B, gegeven door propositie 3.2 en $N_B = \{\sigma_{1,b} \mid b \in B\} \subseteq G_B$.) We definiëren F zo dat op het niveau van objecten geldt $F(B, +, \cdot, 0, 1) = (G_B, N_B, B, \phi, \sigma_{1,1}, 0)$ zoals hierboven. Laat nu $f : A \to B$ een bijna-lichaamshomomorfisme zijn, dan definiëren we F op het niveau van morfismen als $F(f) = (\gamma_f, \chi_f)$, waarbij voor elke $\sigma_{a,b} \in G_A$ geldt $\gamma_f(\sigma_{a,b}) = \sigma_{f(a),f(b)}$ en voor elke $z \in A$ geldt $\chi_f(z) = f(z)$. Omdat f een bijna-lichaamshomomorfisme is, geldt dan $\gamma_f(\sigma_{1,1}) = \sigma_{1,1}$ en $\chi_f(0) = 0$. Ook geldt natuurlijk $\gamma_f(N_A) \subseteq N_B$. Als laatste krijgen we voor alle $x \in A$ en $\sigma_{a,b} \in G_A$ het volgende: $\chi_f(\phi(\sigma_{a,b})(x)) = f(\sigma_{a,b}(x)) = f(a)f(x) + f(b) = \sigma_{f(a),f(b)}(f(x)) = \phi'(\sigma_{f(a),f(b)})(f(x)) = \phi(\gamma_f(\sigma_{a,b}))(\chi_f(x))$, dus $F(f)$ is een morfisme. Als $f : B \to C$ en $g : A \to B$ morfismen zijn, geldt duidelijk $F(f \circ g) = (\gamma_{f\circ g}, \chi_{f\circ g}) = (\gamma_f \circ \gamma_g, \chi_f \circ \chi_g) = F(f) \circ F(g)$. Dus F is een functor. Aangezien als een linker bijna-lichaam B eindig is, $F(B, +, \cdot, 0, 1)$ dan ook eindig is, geldt dat F als beperking tot $\mathbf{E-BiLi}$ ook een functor $F : \mathbf{E-BiLi} \to \mathbf{E-STTW}$ geeft. □

Propositie 4.5. *Laat* $(G, N, X, \phi, 1, x) \in \mathrm{Ob}(\mathbf{E-STTW})$ *willekeurig gegeven zijn, dan geeft gevolg 3.8 ons een (eindig) linker bijna-lichaam* $(N, +, \cdot, 0, 1)$. *Er is een functor*
$H : \mathbf{E-STTW} \to \mathbf{E-BiLi}$ *gegeven op het niveau van objecten als*
$H(G, N, X, \phi, 1, x) = (N, +, \cdot, 0, 1)$ *en op het niveau van morfismen gegeven als* $H(\gamma, \chi) = \gamma|_N$ *voor elk morfisme* (γ, χ).

We zullen niet bewijzen dat H een functor is, omdat dit (analoog aan de vorige propositie) vrij direct volgt uit gevolg 3.8. We kunnen nu laten zien dat de functoren F en H samen een equivalentie geven.

Stelling 4.6. *Laat* I *de identiteitsfunctor op* $\mathbf{E-BiLi}$ *zijn en* J *de identiteitsfunctor op* $\mathbf{E-STTW}$. *Er zijn natuurlijke isomorfismen* $\alpha : FH \to J$ *en* $\beta : I \to HF$. *Oftewel* $\mathbf{E-BiLi}$ *en* $\mathbf{E-STTW}$ *zijn equivalente categorieën.*

Bewijs. Laat $(B, +, \cdot, 0, 1) \in \mathrm{Ob}(\mathbf{E-BiLi})$ willekeurig gegeven zijn. We weten vanwege stelling 3.10 dat er een isomorfisme $\beta_B : (B, +, \cdot, 0, 1) \to HF(B, +, \cdot, 0, 1)$ bestaat, in het bijzonder wordt β_B gegeven als $\beta_B(b) = \sigma_{1,b}$. Laat nu $(A, *, \circ, x, y) \in \mathrm{Ob}(\mathbf{E-BiLi})$ en een morfisme $f : (A, *, \circ, 0, 1) \to (B, +, \cdot, x, y)$ willekeurig gegeven zijn. Dan vinden wij dat
$\beta_B \circ I(f) = \beta_B \circ f = (a \mapsto \sigma_{1,f(a)}) = \gamma_f|_N \circ \beta_A = HF(f) \circ \beta_A$, dus als β de collectie is van alle morfismen β_C met $(C, +, \cdot, 0, 1) \in \mathrm{Ob}(\mathbf{E-BiLi})$, dan is $\beta : I \to HF$ een natuurlijk isomorfisme, omdat elke β_C een isomorfisme is.

Laat nu $(G, N, X, \phi, 1_G, x), (G', N', X', \phi', 1_{G'}, x') \in \mathrm{Ob}(\mathbf{E-STTW})$ willekeurig gegeven zijn. Dan weten we vanwege stelling 3.10 dat er een isomorfisme $\pi_G : FH(G) \to G$ is (als groepshomomorfisme) met $\pi_G(FH(N)) = N$. Bovendien geeft die stelling ons ook een bijectie
$\psi_X : FH(X) \to X$, zo dat $\psi_X(FH(x)) = x$ en dat voor elke $g \in FH(G)$ en $y \in FH(X)$ geldt dat $\psi_X(FH(\phi)(g)(y)) = \phi(\pi(g))(\psi_X(y))$ dus
$\alpha_G = (\pi_G, \psi_X) : FH(G, N, X, \phi, 1, x) \to (G, N, X, \phi, 1, x)$ is een isomorfisme (als morfisme in $\mathbf{E-STTW}$).

Ook krijgen we als $f = (\gamma, \chi) : (G, N, X, \phi, 1_G, x) \to (G', N, X', \phi', 1_{G'}, x')$ een morfisme is, dat geldt $\pi_{G'} \circ FH(\gamma) = \gamma \circ \pi_G$ en $\psi_{X'} \circ FH(\chi) = \chi \circ \psi_X$, vanwege stelling 3.10, dus ook $\alpha_{G'} \circ FH(f) = (\pi_{G'}, \psi_{X'}) \circ (FH(\gamma), FH(\chi)) = (\gamma, \chi) \circ (\pi_G, \psi_X) = FH(f) \circ \alpha_G$. Oftewel als α de collectie van alle α_G met $(G, N, X, \phi, 1, x) \in \mathrm{Ob}(\mathbf{E-STTW})$, dan is $\alpha : FH \to J$ een natuurlijk isomorfisme, omdat α_G een isomorfisme is.

Nu geldt dus in het bijzonder dat $\mathbf{E-BiLi}$ en $\mathbf{E-STTW}$ equivalente categorieën zijn. □

De voorgaande stelling geeft ons dat de correspondentie van stelling 3.10 zelfs een equivalentie van categorieën is. Er is ook een natuurlijke uitbreiding van de functor H zo dat $H : \mathbf{S-STTW} \to \mathbf{BiLi}$ een functor is. Vervolgens kan men geheel analoog aan de vorige stelling bewijzen dat de correspondentie in stelling 3.15 ook een equivalentie van categorieën is. Oftewel men kan de volgende stelling bewijzen.

Stelling 4.7. *Laat I de identiteits functor op* **BiLi** *zijn en J de identiteitsfunctor op* $\mathbf{S-STTW}$. *Er zijn natuurlijke isomorfismen $\alpha : FH \to J$ en $\beta : I \to HF$. Oftewel* **BiLi** *en* $\mathbf{S-STTW}$ *zijn equivalente categorieën.*

5 Afsluiting

We hebben nu een introductie in de bijna-lichaamstheorie gehad en gezien dat deze equivalent is met de studie van de sterke scherp tweevoudig transitieve werkingen. Als laatste willen we nog opmerken dat er wel een algebraïsche structuur is die verwant is aan het bijna-lichaam waarvoor er wel een 1-op-1 correspondentie is met de scherp tweevoudig transitieve werkingen. Deze structuur heet een bijna-domein en heeft dezelfde eisen als een bijna-lichaam, afgezien van de associativiteit van de vermenigvuldiging (bij het bijna-domein mag deze ontbreken). Deze correspondentie was al door H. Wähling bewezen in [3]. Voor wie nog meer wil lezen wordt aangeraden om [2] te lezen, hierin is onder andere een voorbeeld te vinden van een niet-sterke scherp tweevoudig transitieve werking.

Referenties

[1] Eliyahu Rips, Yoav Segev, and Katrin Tent. A sharply 2-transitive group without a non-trivial abelian normal subgroup. *Journal of the European Mathematical Society*, 19(10):2895–2910, 2017.

[2] Katrin Tent. Infinite sharply multiply transitive groups. *Jahresbericht der Deutschen Mathematiker-Vereinigung*, 118(2):75–85, 2016.

[3] Heinz Wähling. *Theorie der Fastkörper*, volume 1 of *Thales Monographs*. Thales-Verlag, Essen, 1987.

[4] Hans Zassenhaus. Über endliche Fastkörper. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 11(1):187–220, 1935.