Definitielijst

Definitie 1 $JA_n(\mathbb{K}) :=$ *afbeeldingen van de vorm* $(X_1, ..., X_n) \in \mathbb{K}^n$ *gaat naar* $(X_1 + f_1(X_2, ..., X_n), X_2 + f_2(X_3, ...X_n), ..., X_{n-1} + f_n(X_n))$ *met* f_i *polynomen.*

Definitie 2 $GL_n(\mathbb{K}) :=$ *de verzameling van alle inverteerbare* $n \times n$ *matrices.*

Definitie 3 $Aff_n(\mathbb{K}) :=$ *afbeeldingen* $\mathbb{K}^n \to \mathbb{K}^n$ *van de vorm* $x \to Mx+b$, *met* $M \in GL_n(\mathbb{K})$ *en* $b \in \mathbb{K}^n$.

Definitie 4 $TA_n(\mathbb{K}) :=$ *Alles wat je kunt maken door eindig veel elementen uit* $JA_n(\mathbb{K})$ *en* $Aff_n(\mathbb{K})$ *samen te stellen.*

Definitie 5 $Bij_n(\mathbb{K}) :=$ *de verzameling van bijecties van* $\mathbb{K}^n$ *naar* $\mathbb{K}^n$.

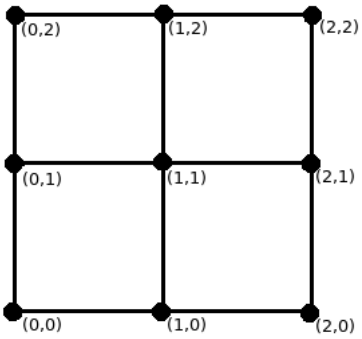
Definitie 6 $Bij_n(\mathbb{K}) :=$ *de verzameling van bijecties van* $\mathbb{K}^n$ *naar* $\mathbb{K}^n$.

Definitie 7 $\tau : TA_n(\mathbb{K}) \to Bij_n(\mathbb{K})$ *is de afbeelding die aan een element* $F \in TA_n(\mathbb{K})$ *de bijectie* $\tau(F) : \mathbb{K}^n \to \mathbb{K}^n$ *toevoegt. Merk op dat er* $F, G \in TA_n(\mathbb{K})$ *zijn met* $F \neq G$ *zodat* $\tau(f) = \tau(G)$ *want* $TA_n(\mathbb{K})$ *is oneindig en* $Bij_n(\mathbb{K})$ *is eindig.*

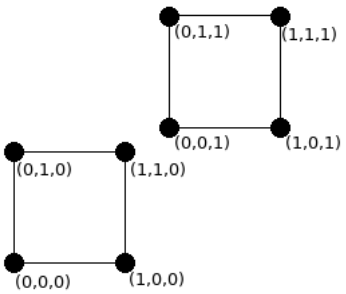
Definitie 8 x *is variant onder een bepaalde afbeelding* f *als* $f(x) \neq x$

Definitie 9 x *is invariant onder een bepaalde afbeelding* f *als* $f(x) = x$

Definitie 10 *De coördinaten(vectoren) van de roosters van* $\mathbb{F}_3^2$ *zijn als volgt:*



Definitie 11 *De coördinaten van de roosters van* $\mathbb{F}_2^3$ *zijn als volgt:*



Definitie 12 $\mathbb{F}_p^n$ *is de vectorruimte van dimensie* n *over het lichaam* $\mathbb{F}_p$ *met* p *een priemgetal en* $n \in \mathbb{N}$

Definitie 13

$$\pi_{a,b}(x) := \begin{cases} a & \text{als} \quad x = b \\ b & \text{als} \quad x = a \\ x & \text{als} \quad x \neq a, b \end{cases}$$

Vraag Wat is $\tau(TA_n(\mathbb{K}))$ als $\mathbb{K}^n = \mathbb{F}_3^2$ of $\mathbb{K}^n = \mathbb{F}_2^3$? Daarop zullen we in dit artikel een antwoord op geven.

Voor ons bewijs maken wij van roosters gebruik om aan te tonen dat er een verwisseling mogelijk is. De coördinaten van de roosters staan in de definities en zijn vectoren van een bepaald lichaam (in ons geval $\mathbb{F}_3^2$ of $\mathbb{F}_2^3$). Een pijl van een "punt' a naar een ander 'punt' b geeft aan dat de vector a door de bijbehorende afbeelding afgebeeld wordt op de vector b. Zo kunnen we elke bijectie dus omzetten naar een plaatje.
Als eerst laten we zien dat je als je een verwisseling kan maken dat je dan alle bijecties kan maken.

Lemma 1 *Neem* $a, b, q, r \in \mathbb{F}_p^n$ *met* $q \neq r$ *en* $a \neq b$. *Dan is er een* $M \in Aff_n(\mathbb{F}_p^n)$ *zodat* $M(q) = a$ *en* $M(r) = b$.

Bewijs Neem L lineair zodat $L(q-r) = a-b$ en neem $v = a - Lq$ Dan voldoet de afbeelding $M(x) = Lx + v$ want $M(q) = Lq + v = Lq + a - Lq = a$ en $M(r) = Lr + v = Lr + a - Lq = L(r-q) + a = -L(q-r) + a = -a + b + a = b$. □

Lemma 2 *Stel dat* $a, b \in \mathbb{F}_p^n$ *en* $T \in Aff_n(\mathbb{F}_p^n)$, *dan*

$$\pi_{Ta,Tb} = T\pi_{a,b}T^{-1}$$

Bewijs Stel $c \in \mathbb{F}_p^n$ en stel dat $c \neq Ta, Tb$,dan $T^{-1}c \neq a, b$, dan:

$$T\pi_{a,b}T^{-1}(c) = T\pi_{a,b}(T^{-1}c) = T(T^{-1}c) = c = \pi_{Ta,Tb}(c)$$

Dus als $c \neq Ta, Tb$ dan $T(a,b)T^{-1}(c) = \pi_{Ta,Tb}(c)$.
Als $c = Ta$, dan $\pi_{Ta,Tb}(Ta) = Tb = T\pi_{a,b}(a) = \pi_{Ta,Tb} = T\pi_{a,b}T^{-1}(Ta)$, zo ook voor $c = Tb$
Dus voor elke $c \in \mathbb{F}_p^n$ geldt dat $\pi_{Ta,Tb}(c) = T\pi_{a,b}T^{-1}(c)$ dus

$$\pi_{Ta,Tb} = T\pi_{a,b}T^{-1}$$

□

Propositie 1 *Stel $q, r, a, b \in \mathbb{F}_p^n (q \neq r$ en $a \neq b)$ willekeurig en dat $\pi_{r,q} \in TA_n(\mathbb{F}_p^n$ dan $\pi_{a,b} \in TA_n(\mathbb{F}_p^n)$.*

Bewijs Volgens lemma 1 is er een $M \in Aff_n$ zdd $M(q) = a$ en $M(r) = b$ en volgens lemma 2 geldt dat $\pi_{a,b} = \pi_{M(q),M(r)} = M\pi_{r,q}M^{-1}$. Omdat $\pi_{r,q} \in TA_n(\mathbb{F}_p^n)$ geldt dat $\pi_{M(q),M(r)} = M\pi_{r,q}M^{-1} \in TA_n(\mathbb{F}_p^n)$, dus $\pi_{a,b} \in TA_n(\mathbb{F}_p^n)$.
□

Gevolg 1 *Als we een verwisseling kunnen maken dan kunnen we elke verwisseling maken.*

$$f_q(x) := \begin{cases} f(x) & \text{als} \quad x \neq q, f(q) \\ f(q) & \text{als} \quad x = f(q) \\ f(f(q)) & \text{als} \quad x = f(q) \end{cases}$$

Definitie 14 *Stel $f : \mathbb{F}_p^n \to \mathbb{F}_p^n$ en f heeft minstens een variant punt, dus er is een q zdd $f(q) \neq q$ dan:*

$$f_q(x) := \begin{cases} f(x) & \text{als} \quad x \neq q, f(q) \\ f(q) & \text{als} \quad x = f(q) \\ f(f(q)) & \text{als} \quad x = f(q) \end{cases}$$

Lemma 3 *f_q is een bijectie*

Bewijs Stel $x \in \mathbb{F}_p^n$ dan is er een $a \in \mathbb{F}_p^n$ zdd $f(a) = x$, omdat f surjectief is.
Stel $a \neq q, f(q)$ dan $x = f(a) = f_q(a)$
Stel $a = q$ dan $x = f(q) = f_q(f(q))$
Stel $a = f(q)$ dan $x = f(f(q)) = f_q(q)$
Dus voor alle $x \in \mathbb{F}_p^n$ geldt dat er een $b \in \mathbb{F}_p^n$ zdd $x = f_q(b)$. Dus f_q is surjectief, omdat f_q een transformatie is over een verzameling met een eindig aantal elementen is f_q ook een bijectie.

□

Lemma 4 *Stel f heeft minstens een variant punt dan $f_q\pi_{f(q),q} = f$*

Bewijs Stel $x \neq f(q), q$ dan $f_q\pi_{f(q),q}(x) = f_q(x) = f(x)$.
Stel $x = f(q)$ dan $f_q\pi_{f(q),q}(x) = f_q(q) = f(f(q)) = f(x)$.
Stel $x = q$ dan $f_q\pi_{f(q),q}(x) = f_q(f(q)) = f(q) = f(x)$.
Dus voor alle $x \in \mathbb{F}_p^n$ is $f_q\pi_{f(q),q}(x) = f(x)$, dus $f_q\pi_{f(q),q} = f$.

□

Lemma 5 *Stel x is een variant punt onder f_q dan is x ook een variant punt onder f*

Bewijs Stel voor een willekkeurig x geldt dat $f_q(x) \neq x$
Dan $x \neq f(q)$ want als $x = f(q)$ dan $f_q(f(q)) = f(q)$ en dat is een tegenspraak met dat x variant is.
als $x \neq q$ dan omdat ook $x \neq f(q)$ geldt dat $x \neq f_q(x) = f(x)$
als $x = q$ dan $f(x) \neq x$ (definitie f_q)
dus als x een variant punt onder f_q is, dan is x ook een variant punt onder f.

□

Gevolg 2 *Stel dat de bijectie $f(x)$ $m+1$ variante punten heeft, dan heeft f_q hoogstens m variante punten.*

Bewijs $\#\{x|x \neq f_q(x)\} \leq \#\{x|x \neq f(x)\}$ want als x een variant punt is onder f_q dan ook onder f. Omdat beide verzamelingen eindig zijn en onder f_q het punt $f(q)$ invariant blijft, geldt $\#\{x|x \neq f_q(x)\} \neq \#\{x|x \neq f(x)\}$. Dus $\#\{x|x \neq f_q(x)\} \leq n$ Dus heeft f_q hoogstens m variante punten.

□

Lemma 6 *Stel dat alle bijectie gemaakt kunnen worden waarbij m punten variant zijn, dan kunnen ook alle bijectie worden gemaakt waarbij $m+1$ punten variant zijn.*

Bewijs Neem een willekeurige bijecite $f(x)$ waarbij $m+1$ punten variant zijn, dan is er een $q \in \mathbb{F}_p^n$ zdd $f(q) \neq q$, maak dan de volgende functie:

$f_q\pi_{f(q),q}$

Waarbij q een variant punt is onder f, dus $f(q) \neq q$. En deze kunnen allemaal gemaakt worden.

□

Propositie 2 *Stel $\exists f \in TA_n(\mathbb{F}_p)$ met $\tau(f)$ is een verwisseling, dan $\tau(TA_n(\mathbb{F}_p)) = Bij_n(\mathbb{F}_p)$*
Bewijs $\tau(f)$ is een bijectie waarbij 2 punten variant worden gelaten. Volgens 1 kunnen we alle verwisselingen maken als we 1 verwisseling kunnen maken, en

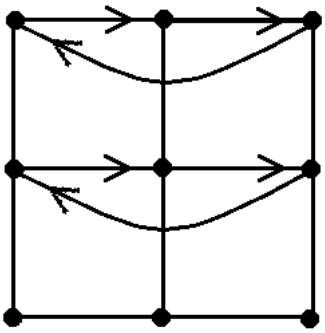
dus kunnen alle bijecties worden gemaakt met 2 variante punten. En dus volgt weer uit 6 dat we elke bijectie kunnen maken en dus $\tau(TA_n(\mathbb{F}_p)) = Bij_n(\mathbb{F}_p)$. □

Lemma 7 *Een bijectie waar slechts 1 punt variant is bestaat niet.*

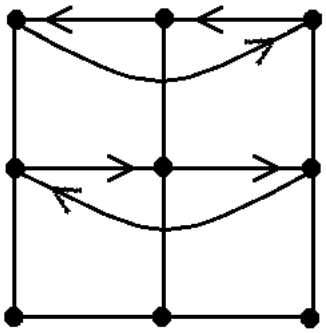
Bewijs Voor het variant punt geldt dat $f(q) \neq q$ maar $f(f(q)) = f(q)$ dus is de afbeelding dan niet injectief en dus geen bijectie wat leidt tot een tegenspraak. □

Opmerking We hoeven nu dus alleen nog te laten zien dat we een verwisseling kunnen maken.

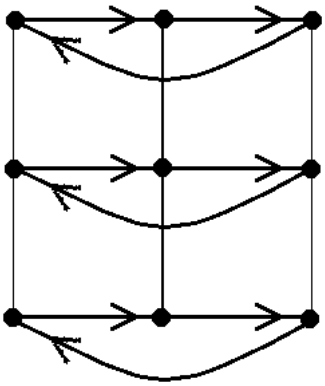
Lemma 8 *We hebben de volgende vijf transformaties op $\mathbb{F}_3^2$ met affine afbeeldingen en de transformatie $(x + y^2, y)$:*



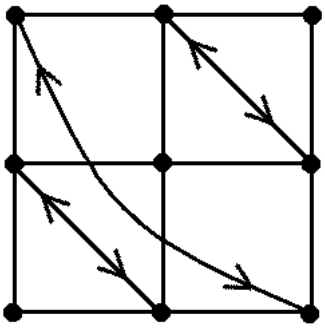
F_1 = (x+y^2,y)



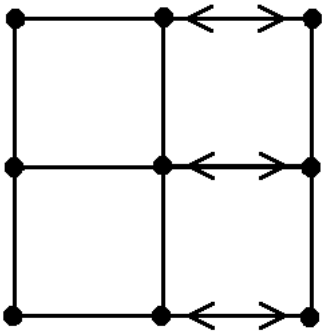
F_2 = (x+y,y)



F_3 =(x+1,y)



F_4 = (y,x)



F_5 = (2x,y)

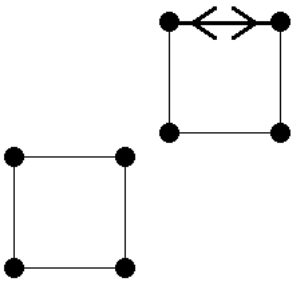
Bewijs De transformatie $(x+y^2, y)$ hebben we sowieso. Met affine afbeeldingen kunnen we op de volgende manier de anderen maken:

$$F_2 \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$
$$F_3 \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$
$$F_4 \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$
$$F_5 \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

□

Propositie 3 *Op het lichaam $\mathbb{F}_2^3$ kunnen we met affine afbeeldingen en de transformatie $(x + yz, y, z)$ een verwisseling maken en op $\mathbb{F}_3^2$ kunnen met affine afbeeldingen en de transformatie $(x + y^2, y)$ een verwisseling maken.*

Bewijs We kijken eerst op $\mathbb{F}_2^3$.

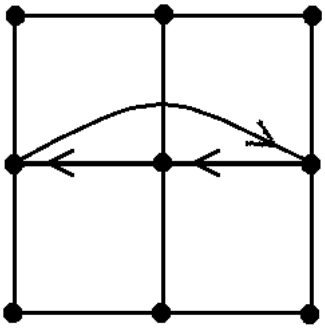


(x+yz,y,z)

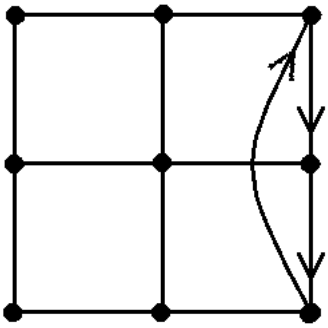
De afbeelding $(x + yz, y, z)$ is al een verwisseling dus zijn we klaar.

Nu op $\mathbb{F}_3^2$:

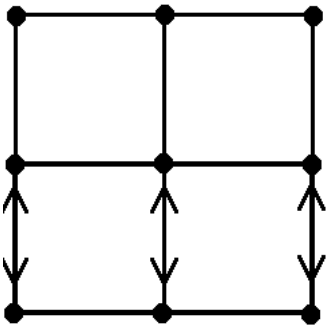
Met de transformaties F_1,F_2,F_3,F_4,F_5 kunnen we door samenstellingen hiervan de volgende transformaties maken:



$E_1 = F_1\ F_2$

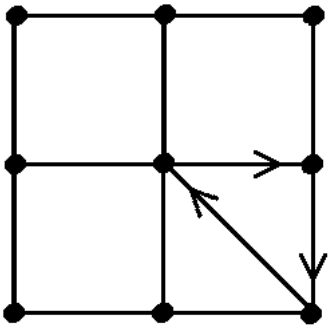


$E_2 = F_4\ E_1\ F_2\ F_4$

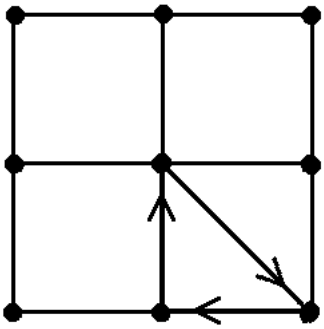


$E_3 = F_4\ F_3^{-1} F_5\ F_3\ F_4$

Waarmee we de volgende transformaties kunnen maken:

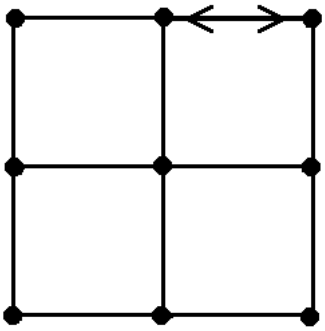


$A_1 = E_2\ E_1\ E_2^{-1} E_1^{-1}$



$A_2 = F_5\ E_3\ A_1\ E_3\ F_5$

En met deze twee transformaties gecombineert met F5 kunnen we een verwisseling van slechts twee punten maken:



$A_1^{-1}\, A_2\, F_5$

En dit is een verwisseling op $\mathbb{F}_3^2$
Dus op het lichaam $\mathbb{F}_2^3$ kunnen we met affine afbeeldingen en de transformatie $(x + yz, y, z)$ een verwisseling maken en op $\mathbb{F}_3^2$ kunnen met affine afbeeldingen en de transformatie $(x + y^2, y)$ een verwisseling maken.

□

Gevolg 3 *De volgende stelling:*

Stelling 1 *Op $\mathbb{F}_3^2$ en $\mathbb{F}_2^3$ kunnen we elke bijectie als inverteerbare veeltermafbeelding krijgen.*

Bewijs Uit Propositie 3 volgt dat we een verwisseling op $\mathbb{F}_3^2$ en $\mathbb{F}_2^3$ kunnen maken. Uit Propositie 1 volgt dan dat we elke verwisseling kunnen maken waardoor uit Propositie 2 volgt dat we elke bijectie kunnen maken met inverteerbare veeltermafbeeldingen. Dus $\tau(TA_3(\mathbb{F}_2)) = Bij_3(\mathbb{F}_2)$ en $\tau(TA_2(\mathbb{F}_3)) = Bij_2(\mathbb{F}_3)$.
□