Inleiding

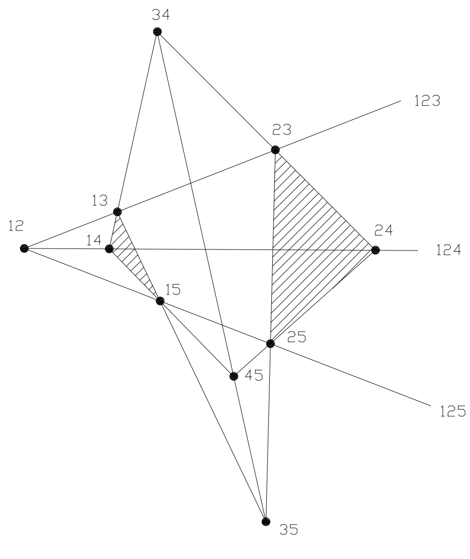
Deze syllabus bedoelt te zijn een inleiding in de Eindige Meetkunde. Een uitputtende behandeling wordt niet nagestreefd. Veeleer wordt getracht de lezers vertrouwd te maken en een eind op weg te helpen met een groot aantal begrippen en onderwerpen, waarna zij wordt gericht op de syllabus Classical groups van Higman [12] en op de boeken van Dembowski [6], Hughes-Piper [14], Gruenberg-Weir [7] en Hirschfeld [13].
Het uitgangspunt (Hoofdstuk 1) wordt gevormd door een ruimtelijke benadering van de klassieke configuraties van Desargues en Pascal. In Hoofdstuk 2 wordt de projectieve meetkunde geintroduceerd via de structuur der deelruimten, zowel axiomatisch als met behulp van vectorruimten over een (eindig) lichaam. De theorie der projectieve vlakken wordt ingeleid in Hoofdstuk 3, met het accent op de combinatorische eigenschappen. Een aantal begrippen, zoals spreads, Baer subvlakken, Singer cycles, niet-Desarguese vlakken, translatievlakken, wordt toegelicht door voorbeelden. Met enige uitvoerigheid wordt in Hoofdstuk 4 de polaire meetkunde behandeld, met speciale aandacht voor de combinatorische toepassingen van de symplectische, unitaire en orthogonale meetkunden (ook van karakteristiek 2). Hoofdstuk 5 is gewijd aan de kwadratische verzamelingen zoals ovalen en ovoiden. Ook de lijnen meetkunde, de Tits-ovoide en de meetkunden van Möbius en Hjelmslev komen aan de orde. De samensteller is dankbaar voor de goede raad van vele collegas in binnen- en buitenland. In het bijzonder vermeldt hij de medewerking van A. Blokhuis en W. Haemers.

Hoofdstuk 1

Klassieke configuraties

1.1 De configuratie van Desargues (1593–1662)

Beschouw vijf punten 1, 2, 3, 4, 5 in de ruimte, waarvan geen viertal coplanair is (d.w.z. op één vlak ligt). De tien paren der punten bepalen tien rechten, de tien tripels tien vlakken. Als we dit geheel snijden met een niet ongeschikt vlak (een vlak dat geen van de vijf punten bevat en niet evenwijdig loopt met een van de lijnen of vlakken) dan ontstaat de *configuratie van Desargues*:

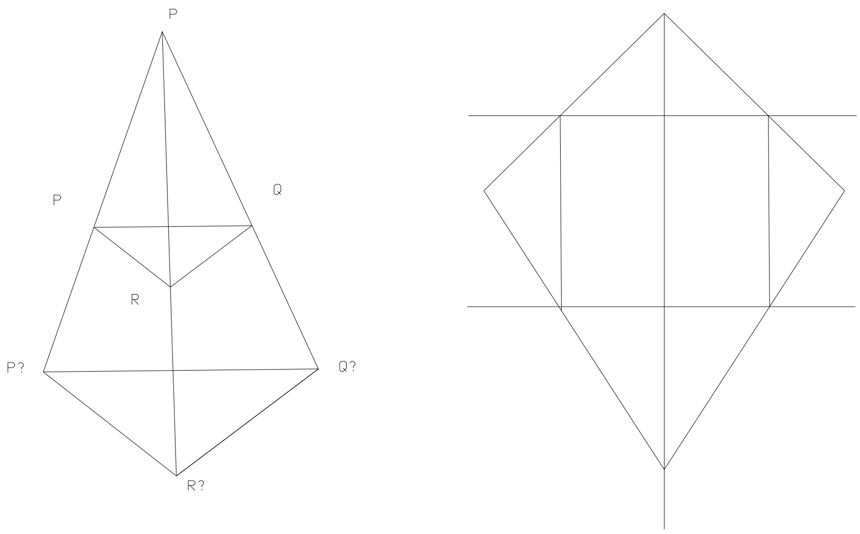


Figuur 1.1: de configuratie van Desargues

Deze configuratie ligt ten grondslag aan de volgende stelling: Laten in een vlak twee perspectivisch gelegen driehoeken gegeven zijn (d.w.z. de verbindingslijnen van “overeenkomstige” hoekpunten gaan door één punt, het perspectiviteitscentrum), zeg de driehoeken 13, 14, 15 en 23, 24, 25 met perspectiviteitscentrum 12, dan liggen de snijpunten 34, 35, 45 van de corresponderende zijden van deze driehoeken op een rechte (de perspectiviteitsas).
Dit is de *stelling van Desargues*. Het bewijs verloopt als volgt. Richt een of andere rechte op in het punt 12 (niet in het vlak) en kies daarop willekeurig twee punten 1 en 2. Bepaal nu de volgende punten: $3 := (1 \cup 13) \cap (2 \cup 23)$, $4 := (1 \cup 14) \cap (2 \cup 24)$ en $5 := (1 \cup 15) \cap (2 \cup 25)$.
De vijf punten 1, 2, 3, 4, 5 bepalen nu in het vlak een configuratie van Desargues, die precies gelijk is aan de oorspronkelijke figuur. Hieruit volgt dat 34, 45, 53 op een rechte liggen.

1.2 Opmerkingen

Bij de constructie hebben wij slechts gebruik gemaakt van de projectieve bewerkingen $\cap$ = snijden en $\cup$ = verbinden.
Bij het bewijs hebben wij gebruik gemaakt van het feit dat ons vlak zich in de ruimte bevindt. Een platlander zou dit bewijs niet kunnen geven. (Een gevolg hiervan is dat in een projectief vlak, dat gelegen is in een ruimte met meer dan twee dimensies de stelling van Desargues geldt; er zijn echter projectieve vlakken waarin deze stelling niet geldt, zoals we later zullen zien.)
Kiezen we het snijvlak “ongeschikt” dan ontstaan bijzondere gevallen van de stelling.
In het eerste geval komt de stelling van Desargues neer op de *pyramide eigenschap*: als $PR \parallel P'R'$ en $RQ \parallel R'Q'$, dan $PQ \parallel P'Q'$.
Neem het snijvlak door $12 \cap 345$. dan ligt het perspectiviteitscentrum (12) op de perspectiviteitsas (345). We noemen de perspectiviteit in dit geval een elatie (in het andere geval een homologie). In het geval $12 \parallel 345$ komen het centrum zowel als de as in oneindig te liggen en lopen dus alle overeenkomstige lijnen parallel; we hebben dan een translatie. De stelling van Desargues komt nu neer op de *prisma-eigenschap*: als $PP' \parallel QQ' \parallel RR'$ en $PR \parallel P'R'$, $RQ \parallel R'Q'$, dan $PQ \parallel P'Q'$.
De stelling van Desargues impliceert dus de prisma-eigenschap, omgekeerd echter niet: het is mogelijk dat in een projectief vlak de prisma-eigenschap geldt, maar de stelling van Desargues niet.
Als van twee driehoeken de verbindingslijnen der corresponderende hoekpunten door één punt gaan, dan liggen de snijpunten der corresponderende zijden op één lijn.
Als we de duale uitspraak bekijken (we vervangen punt door lijn en omgekeerd) dan krijgen we het omgekeerde van de stelling van Desargues:
Als van twee driehoeken de snijpunten der corresponderende zijden op een lijn liggen, dan gaan de verbindingslijnen der corresponderende hoekpunten door



Figuur 1.2: (i) snijvlak $\|$ 345 (ii) snijvlak $\|$ 12

één punt. (De operaties snijden en verbinden, $\cap$ en $\cup$ worden bij dualiseren ook verwisseld.)

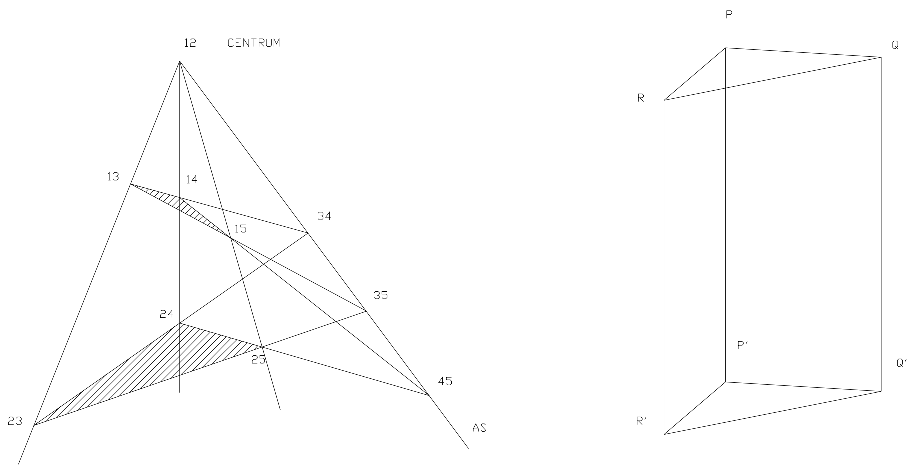
Opgave 1 Leg een verband tussen de configuratie van Desargues en de *Petersen-graaf*. Laat zien dat hieruit volgt dat de Petersen-graaf Sym(5) als groep van automorfismen heeft.

De zeshoeken van Pascal (1623-1662) *en Pappus* (250-300),
Beschouw zes punten 12, 23, 34, 45, 56, 61 op een kegelsnede (resp. op twee rechten in een vlak). Dan liggen de snijpunten 123/456, 234/561, 345/612 op een rechte.
Voor het bewijs construeren wij een ruimtelijke *zeshoek* 1, 2, 3, 4, 5, 6 *van Dandelin* (1794-1849), waarvan de zijden op een eenbladige hyperboloide liggen. Elke eenbladige hyperboloide bevat twee stelsels S en T van rechten. Twee rechten van hetzelfde stelsel kruisen; twee rechten van verschillende stelsels snijden (of zijn evenwijdig): Laat de hyperboloide gegeven zijn door de vergelijking

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} - \frac{z^2}{c^2} = 1.$$

laat de lijnen van stelsel S bepaald worden door

$$s_1 \left(\frac{x}{a} - \frac{z}{c} \right) = s_2 \left(1 - \frac{y}{b} \right),$$



Figuur 1.3: de prisma eigenschap

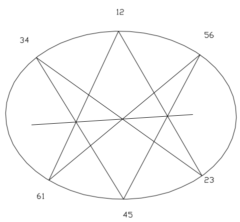
$$s_2\left(\frac{x}{a}+\frac{z}{c}\right) \quad = \quad s_1\left(1+\frac{y}{b}\right);$$

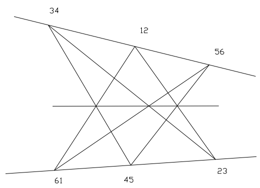
en de lijnen van het stelsel T door

$$\begin{aligned} t_1\left(\frac{x}{a}-\frac{z}{c}\right) &= t_2\left(1+\frac{y}{b}\right), \\ t_2\left(\frac{x}{a}+\frac{z}{c}\right) &= t_1\left(1-\frac{y}{b}\right); \end{aligned}$$

De zeshoek van Dandelin ontstaat nu als volgt. Beschouw een hyperboloide door de gegeven kegelsnede (resp. door de beide gegeven rechten). Neem de rechten van het stelsel S door de punten 23, 45, 61. Noem de verkregen snijpunten 2, 3, 4, 5, 6, 1.
Bekijken we vervolgens $P := 12 \cap 45$, $Q := 23 \cap 56$, $R := 34 \cap 61$, dan zien we dat $123 \cap 456 = PQ$, $234 \cap 561 = QR$, $345 \cap 612 = RP$.
De snijpunten van PQ, PR en QR met het vlak van de ellips liggen op een rechte omdat de lijnen PQ, PR en QR in één vlak liggen. Maar deze snijpunten zijn juist gelijk aan de drie snijpunten uit de stelling.

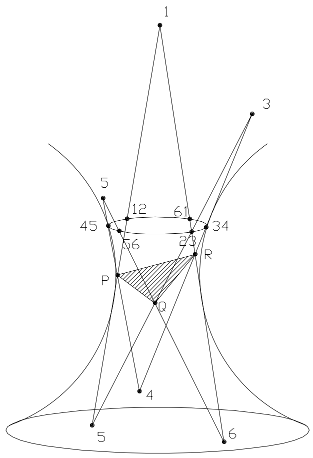
Opgave 2 Dualiseer de stelling van Pascal. (Bedenk dat dualisering van een kegelsnede (verzameling van punten) weer een kegelsnede (nu een verzameling van raaklijnen) oplevert.) Het resultaat van de dualisering is de stelling van Brianchon (1783–1864).



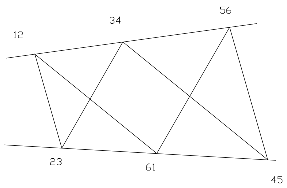


Figuur 1.4: de zeshoeken van Pascal en Pappus

De stelling van Pappus impliceert de stelling van Desargues, het omgekeerde geldt alleen in het eindige geval. (Zie [19].)
Een bijzonder geval van de stelling van Pappus ontstaat wanneer de corresponderende lijnen parallel lopen, de drie 'snijpunten' komen dan op de oneindige rechte te liggen.
$123 \parallel 456$, $234 \parallel 561$, $345 \parallel 612$.



Figuur 1.5: de zeshoek van Dandelin



Figuur 1.6: de configuratie van Pappus

Hoofdstuk 2

Projectieve meetkunde

2.1 Projectieve ruimten

Een projectieve ruimte is een paar $(\mathcal{P}, \mathcal{L})$ bestaande uit een verzameling $\mathcal{P}$ (de punten) en een collectie $\mathcal{L}$ (de lijnen) van deelverzamelingen van $\mathcal{P}$ zodat aan de volgende drie eigenschappen is voldaan.

PG 1. Elk tweetal (verschillende) punten ligt op één lijn.

PG 2. Elke lijn bevat tenminste 3 punten.

PG 3. Het axioma van Pasch: Als twee lijnen l en m elkaar snijden in een punt C, en A, D zijn twee van C verschillende punten van l, B, E twee van C verschillende punten van m, dan hebben de lijnen AB en DE een snijpunt.

Opmerking. Axioma's zijn binnen een wiskundige theorie op te vatten als 'spelregels', de bedoeling is natuurlijk wel dat het spel dat je gaat spelen iets met de werkelijkheid te maken heeft; het zijn echter geen van hogerhand vastgestelde 'eeuwige' waarheden.

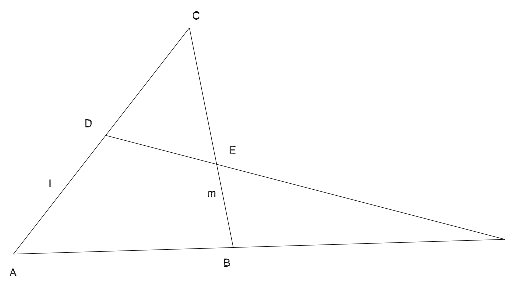
Een *deelruimte* van een projectieve ruimte $(\mathcal{P}, \mathcal{L})$ is een deelverzameling $\alpha \subset \mathcal{P}$ met de eigenschap:

$$\forall P \in \mathcal{P} : \forall Q \in \mathcal{P} : \forall R \in P \cup Q : ((P \in \alpha, Q \in \alpha) \Rightarrow R \in \alpha).$$

Met andere woorden, als een deelruimte twee punten bevat, dan bevat hij de hele lijn door die twee punten.
Met de bijbehorende lijnen is de deelruimte zelf weer een projectieve ruimte. Voorbeelden van deelruimten zijn:

$$\emptyset, \quad \{P\} \text{ voor } P \in \mathcal{P}, \quad \{P \mid P \in l\} \text{ voor } l \in \mathcal{L}.$$

Drie punten die niet op een lijn liggen bepalen een *vlak* (alle $X \in \mathcal{P}$ op $P_1 \cup S$, $S \in P_2 \cup P_3$ en de bijbehorende lijnen), 4 niet in een vlak liggende punten

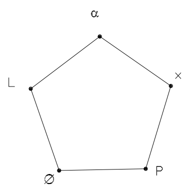


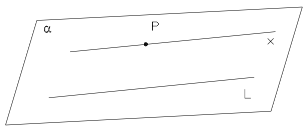
Figuur 2.1: de Pasch-configuratie

bepalen een 3-*ruimte* (alle $X \in \mathcal{P}$ op $P_4 \cup S$, $S \in P_1 \cup P_2 \cup P_3$), etcetera. Een *hypervlak* is een maximale echte deelruimte. Een *projectieve meetkunde* is de verzameling van alle deelruimten van een projectieve ruimte. Hieruit ontstaat een *affiene meetkunde* wanneer uit elke deelruimte de doorsnede met een gegeven hypervlak wordt weggelaten (onze "gewone" ruimte is een affiene ruimte, het vlak dat is "weggelaten" is het vlak in het oneindige).
Een verzameling van $d + 1$ elementen met al zijn deelverzamelingen is op te vatten als een "magere" projectieve meetkunde (vervang PG 2 door: elke lijn bevat tenminste twee punten). De lijnen zijn de paren elementen (de vlakken de drietallen, de hypervlakken de d-tallen etcetera). (Zie [28]). Ga na dat aan het axioma van Pasch voldaan wordt omdat de voorwaarden leeg zijn.
De deelruimten van een projectieve meetkunde vormen een *lattice* (rooster), waarin $\alpha \cap \beta$ de doorsnede en $\alpha \cup \beta$ de kleinste omvattende deelruimte van de deelruimten α en β is, en waarin de projectieve ruimte $\mathcal{P}$ zelf de grootste en $\emptyset$ de kleinste deelruimte is. Deze lattice is atomair (een punt heeft slechts $\emptyset$ als echt deel), gecomplementeerd ($\forall x\, \exists x' : (x \cup x' = \mathcal{P}, x \cap x' = \emptyset)$), en modulair, d.w.z. er bestaat geen Euclidische deellattice:
Omgekeerd is elke atomaire, gecomplementeerde, modulaire lattice een (eventueel magere) projectieve meetkunde. (zie [27], p. 139).
Een *vlag* is een stelsel deelruimten

$$\emptyset = \mathcal{D}_{-1} \subset \mathcal{D}_0 \subset \ldots \subset \mathcal{D}_{i-1} \subset \mathcal{D}_i \subset \ldots \subset \mathcal{P}$$

zodat, voor $i = 0, 1, 2, \ldots$, elke $\mathcal{D}_{i-1}$ een echte deelruimte is van $\mathcal{D}_i$, en geen echte deelruimten tussen $\mathcal{D}_{i-1}$ en $\mathcal{D}_i$ bestaan.
Wij beperken ons tot projectieve meetkunden $\mathcal{P}$ met eindige vlaggen; van een projectieve meetkunde heeft elke vlag dezelfde lengte $=: 1 + \dim \mathcal{P}$. Voor de





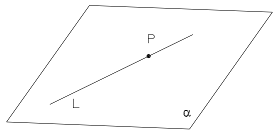
deelruimten $\mathcal{D}$ en $\mathcal{E}$ van $\mathcal{P}$ geldt:

$$\dim \mathcal{D} + \dim \mathcal{E} = \dim \mathcal{D} \cup \mathcal{E} + \dim \mathcal{D} \cap \mathcal{E}.$$

Voor het bewijs van de volgende stelling verwijzen we naar de redenering in 1.1
Als een projectieve ruimte dimensie groter dan 2 heeft, dan geldt de stelling van Desargues voor elk deelvlak.
We zullen echter projectieve vlakken ontmoeten waarvoor de stelling van Desargues niet geldt. Zulke projectieve vlakken kunnen dus niet als deelvlak worden ingebed in projectieve ruimten van dimensie meer dan 2. Projectieve ruimten waarin de stelling van Desargues geldt kunnen worden gecoördinatiseerd met behulp van een scheef lichaam, en met behulp van een lichaam wanneer de projectieve ruimte eindig is (d.w.z. een eindig aantal punten bevat). Deze aankondiging legaliseert de volgende paragraaf.

2.2 Projectieve ruimten over een lichaam

Zij $V(d+1, \mathbf{F})$ een vectorruimte van dimensie $d+1$ over een lichaam $\mathbf{F}$. De lineaire deelruimten van $V(d+1, \mathbf{F})$ vormen een projectieve meetkunde van dimensie d. Inderdaad, noem de 1-dimensionale lineaire deelruimten de *projectieve punten* en de 2-dimensionale lineaire deelruimten de *projectieve lijnen*. De projectieve punten en lijnen voldoen aan de axioma's (ga na!) PG 1, 2, 3. De aldus verkregen projectieve ruimte wordt genoteerd met $PG(d, \mathbf{F})$. Als $\mathbf{F}$ het eindige Galois lichaam $\mathbf{F}_q = GF(q)$, $q = p^k$, p priem is, dan schrijven we ook wel $PG(d, q)$. De magere projectieve meetkunde op $d+1$ punten zou dan worden genoteerd met $PG(d, 1)$ (dit wordt later nog toegelicht).



In $PG(d, \mathbf{F})$ geldt de stelling van Desargues, ook voor $d = 2$. Inderdaad, $PG(2, \mathbf{F})$ kan worden ingebed in $PG(3, \mathbf{F})$.
Zij H een lineaire deelruimte van $V(d+1, \mathbf{F})$. De *flat* door $p \in V$ en evenwijdig aan H is de verzameling $\{p+h \mid h \in H\}$. Selecteer in $V(d+1, \mathbf{F})$ een hypervlak H en een flat $A \parallel H$, $A \neq H$. De doorsneden van A met de lineaire deelruimten in $V(d+1, \mathbf{F})$ zijn flats. Omdat $A \cap H = \emptyset$ vormen deze flats een *affiene meetkunde*, aan te duiden met $AG(d, \mathbf{F})$.
Projectieve lijnen en punten (zoals α en π) corresponderen met affiene lijnen en punten in A (zoals a en P), behalve de lijnen en punten in H!
Voor een eindig lichaam $\mathbf{F}_q$ kunnen de aantallen deelruimten worden geteld. Wij bepalen eerst het aantal lineaire deelruimten van dimensie m van de vectorruimte $V(n, q)$, $m \leq n$. Het aantal verzamelingen van m lineair onafhankelijke vectoren in $V(n, q)$ is

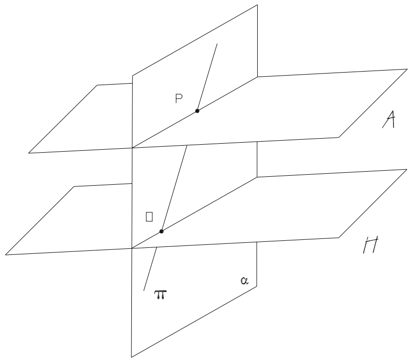
$$(q^n - 1)(q^n - q)(q^n - q^2) \dots (q^n - q^{n-1}).$$

Van deze verzamelingen bepalen echter steeds

$$(q^m - 1)(q^m - q) \dots (q^m - q^{m-1})$$

dezelfde lineaire deelruimte $V(m, q)$. Het quotient van deze uitdrukkingen is dus het aantal der $V(m, q)$ in $V(n, q)$. Dit quotient noteren wij met behulp van de q-analoga van de faculteit (!) en van de binomiaalcoefficient $\binom{n}{m}$:

$$n^{q}_{!} := (q-1)^{-n}(q^n - 1)(q^{n-1} - 1) \dots (q-1), \quad \begin{bmatrix} n \\ m \end{bmatrix}_q := \frac{n^{q}_{!}}{m^{q}_{!}\,(n-m)^{q}_{!}}.$$



Deze definities worden gelegaliseerd door de limieten:

$$\lim_{q\to 1} n\overset{q}{!} = n!, \quad \lim_{q\to 1} \begin{bmatrix} n \\ m \end{bmatrix}_q = \binom{n}{m}.$$

Stelling 2.1 *Het aantal lineaire deelruimten $V(m,q)$ in $V(n,q)$, $m \leq n$, bedraagt* $\begin{bmatrix} n \\ m \end{bmatrix}_q$.

Als er geen verwarring optreedt laten wij de index q weg.

Stelling 2.2 *Het aantal e-dimensionale deelruimten in $PG(d,q)$ bedraagt* $\begin{bmatrix} d+1 \\ e+1 \end{bmatrix}$. *(Als we $q = 1$ nemen krijgen we dus precies het aantal e-dimensionale deelruimten van een magere PG.) Het aantal e-dimensionale flats in $AG(d,q)$ bedraagt* $q^{d-e}\begin{bmatrix} d \\ e \end{bmatrix}$.

Het tweede deel van deze stelling is in te zien door eerst het aantal flats te nemen dat door de oorsprong gaat en vervolgens te bedenken dat een klasse evenwijdige e-flats uit q^{d-e} elementen bestaat.

Stelling 2.3 *De $V(1,q)$ en de $V(m,q)$ van een $V(n,q)$, $m \leq n$, vormen de punten en de blokken van een* $2 - \left(\begin{bmatrix} n \\ 1 \end{bmatrix}, \begin{bmatrix} m \\ 1 \end{bmatrix}, \begin{bmatrix} n-2 \\ m-2 \end{bmatrix}\right)$ *design. Dit design is symmetrisch dan en slechts dan $m = n - 1$.*

2.3 Spreads

Een t-spread in $PG(n,q)$ is een collectie van t-deelruimten zodat elk punt van $PG(n,q)$ ligt in één t-deelruimte. Een nodige (en ook voldoende) voorwaarde voor het bestaan van een t-spread is

$$\frac{q^{t+1}-1}{q-1} \mid \frac{q^{n+1}-1}{q-1}, \quad \text{dat is,} \quad t+1 \mid n+1.$$

Opgave 3 Vind een spread van 5 lijnen in $PG(3,2)$.

In het bijzonder bestaan in $PG(2d-1,q)$ spreads van q^d+1 deelruimten van dimensie $d-1$. Zo'n spread kan als volgt worden geconstrueerd. In termen van vectorruimten is het probleem: het vinden in $V(2d,q)$ van een stelsel van q^d+1 lineaire deelruimten van dimensie d, die (na weglating van 0) een partitie vormen van $V \setminus \{0\}$.
We kunnen $GF(q^{2d})$ beschouwen als een vectorruimte van dimensie 2 over $GF(q^d)$. De verzameling W der lineaire deelruimten van dimensie 1 vormt een partitie (laat 0 weg). Als $GF(q^{2d})$ wordt beschouwd als een vectorruimte van dimensie $2d$ over $GF(q)$, dan vormen de elementen van W disjuncte deelruimten van dimensie d over $GF(q)$ en de gevraagde spread is verkregen.
Elke $(d-1)$-spread in $PG(2d-1,q)$ is als volgt te beschrijven. Zij $U = U(d,q)$, en zij $V = U \times U$. Definieer, voor $i = 3,\ldots,q^d+1$:

$$W_1 = U \times \{0\}, W_2 = \{0\} \times U, W_i = \{(x, T_i(x)) \,|\, x \in U\},$$

waarin $T_i : U \to U$ een niet-singuliere lineaire transformatie is. Dan geldt het het volgende (bewijs dit!)

(i) $W_1,\ldots,W_{q^d+1}$ is een spread $\iff T_j^{-1}T_i$ heeft geen fixpunt voor $i \neq j$.

(ii) $W_1,\ldots,W_{q^d+1}$ is een spread $\iff T_i - T_j$ is niet singulier voor $i \neq j$.

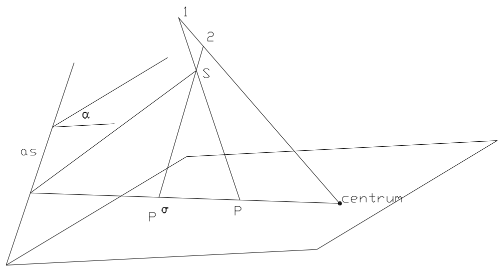
2.4 Collineaties

Een *collineatie* van de projectieve ruimte $(\mathcal{P},\mathcal{L})$ is een permutatie σ van $\mathcal{P}$ zodat $\mathcal{L}^\sigma = \mathcal{L}$. Een collineatie beeldt deelruimten af op deelruimten van dezelfde dimensie. De collineaties vormen een groep genaamd *Coll*.
Een collineatie σ heet een *centrale collineatie* als

$$\exists C \in \mathcal{P} : \forall l \in \mathcal{L} : ((C \in l) \Rightarrow (l^\sigma = l)).$$

Dan gaat elke deelruimte door C (het centrum) in zichzelf over. Voorts bestaat er een hypervlak (de as) waarvan elk punt in zichzelf overgaat. Inderdaad, als H en K hypervlakken, niet door C, zijn dan voldoet $(H \cap H^\sigma) \cup (K \cap K^\sigma)$.

Stelling 2.4 *Een collineatie heeft een centrum dan en slechts dan als hij een as heeft.*



Een centrale collineatie heet een *elatie* (*homologie*) wanneer centrum en as incident (niet incident) zijn. De elaties genereren een groep. Duidelijk is dat

$$\langle \text{elaties} \rangle \leq \langle \text{centr. collin.} \rangle \leq \text{Coll}.$$

Wanneer de projectieve ruimte ligt in een projectieve ruimte van een hogere dimensie (dit kan alleen misgaan als de dimensie twee is), dan is elke centrale collineatie σ als volgt te construeren.
Neem de punten 1 en 2 op een lijn door het centrum en neem het hypervlak α door de as. Bij elke $P \in \mathcal{P}$ construeert met P^σ volgens

$$(P \cup 1) \cap \alpha = S, \quad (2 \cup S) \cap \mathcal{P} = P^\sigma.$$

Voorts: $C^\sigma := C$. Elk punt van de as is vast onder σ.

Opgave 4 Toon aan dat σ een collineatie is. Herken de constructie van Desargues van 1.1.

Beschouw nu weer de vectorruimte $V = V(n, \mathbf{F})$ en de daarbij behorende projectieve ruimte $PG(n-1, \mathbf{F})$.
Zij $- \in \text{Aut}\mathbf{F}$. Een $-$ *semilineaire afbeelding* van V is een afbeelding $\sigma : V \to V$ zodat

$$(x+y)^\sigma = x^\sigma + y^\sigma, \quad (\lambda x)^\sigma = \bar{\lambda} x^\sigma,$$

voor alle $x, y \in V$, $\lambda \in \mathbf{F}$. Zij $\Gamma L(V)$ de groep van de niet singuliere semilineaire afbeeldingen van V, dat is, de groep van alle transformaties

$$(x_1, x_2, \ldots, x_n)^\sigma = (\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n)A, \quad \det A \neq 0.$$

De *algemene lineaire groep* $GL(V)$ is de groep van de niet singuliere lineaire afbeeldingen van V:

$$(x_1, x_2, \ldots, x_n)^\sigma = (x_1, x_2, \ldots, x_n)A, \quad \det A \neq 0.$$

De *speciale lineaire groep* $SL(V)$ is de groep van alle

$$(x_1, x_2, \ldots, x_n)^\sigma = (x_1, x_2, \ldots, x_n)A, \quad \det A = 1.$$

De lineaire afbeelding $\tau : V \to V$ gegeven door

$$x^\tau = x + \phi(x)c, \quad c \in V, \quad \phi \in V^*,$$

heet een *dilatatie* als $\phi(c) \notin \{0, -1\}$, en een *transvectie* als $\phi(c) = 0$.
$SL(V)$ wordt voortgebracht door de transvecties; $GL(V)$ wordt voortgebracht door de dilataties en de transvecties. Inderdaad, ten opzichte van een geschikte basis is de matrix van een transvectie $I + aE_{ij}, i \neq j$, en is de matrix van een dilatatie $I + \phi(c)E_{ii}$.
In $PG(n-1, \mathbf{F})$ induceert elke niet-singuliere semilineaire afbeelding een collineatie, induceert elke dilatatie een homologie, en induceert elke transvectie een elatie. Voor de groepen geldt:

$$\begin{array}{ccccc} \langle\text{elaties}\rangle & \leq & \langle\text{centr. collin.}\rangle & \leq & \text{Coll } PV \\ || & & || & & || \\ PSL(V) & \leq & PGL(V) & \leq & P\Gamma L(V) \end{array}$$

Voor bijzonderheden verwijzen wij naar [12], hoofdstuk 2 "The general linear group", en naar [6]. In deze referenties worden ook de ordes van de groepen bepaald, in het geval $\mathbf{F} = \mathbf{F}_q$, $q = p^e$, p priem (Ga na!)

$$\begin{aligned} q^{\frac{1}{2}n(n-1)}(q-1)^n n\overset{\mathrm{q}}{!} = |GL(n,q)| &= (q-1)|PGL(n,q)|, \\ \frac{1}{e}|\Gamma L(n,q)| = |GL(n,q)| &= (q-1)|SL(n,q)|, \\ \frac{1}{e}|P\Gamma L(n,q)| = |PGL(n,q)| &= |PSL(n,q)| \times \text{ggd}(n, q-1). \end{aligned}$$

Hoofdstuk 3

Projectieve en affiene vlakken

3.1 Het projectieve vlak

Een *projectief vlak* is een projectieve meetkunde $(\mathcal{P}, \mathcal{L})$ zodat

PG 1' Elk tweetal verschillende punten ligt op één lijn.

PG 2' Elk tweetal verschillende lijnen heeft één punt gemeen.

PG 3' Er zijn 4 punten, waarvan geen drie op een lijn liggen.

Een projectief vlak is een projectieve ruimte van dimensie 2. Een eindig projectief vlak is een 2-$(n^2+n+1, n+1, 1)$ design en wordt genoteerd met $PG(2,n)$. De parameter n heet de *orde* van $PG(2,n)$.

Stelling 3.1 (Bruck-Ryser) *Nodig voor het bestaan van een $PG(2,n)$ is dat*

$$(n \equiv 1 \textit{ of } 2 \pmod 4) \Rightarrow (n = u^2 + v^2;\ u, v \in \mathbf{Z}).$$

Voor het bewijs van deze belangrijke stelling, zie [14], 87-89. $PG(2,n)$ bestaat voor $n = 2, 3, 4, 5, 7, 8, 9, 11, 13$, niet voor $n = 6$, 14 terwijl het bestaan van $PG(2,10)$ en $PG(2,12)$ niet bekend is. (*Inmiddels is aangetoond [17] dat $PG(2,10)$ niet bestaat.*)
Voor een collineatie $\sigma \in$ Coll $\equiv \Gamma$ van het projectieve vlak $(\mathcal{P}, \mathcal{L})$ is Fix $\sigma := \{P \in \mathcal{P} \mid P^\sigma = P\}$.

Opgave 5 Wanneer voor een collineatie σ Fix σ vier punten bevat waarvan geen drie collineair zijn, vormt Fix σ een subvlak (is σ de identiteit).

Een centrale collineatie σ is gedefinieerd door

$$\exists c \in \mathcal{P} : \forall l \in \mathcal{L} : ((C \in l) \Rightarrow (l^\sigma = l)).$$

Dan geldt ook

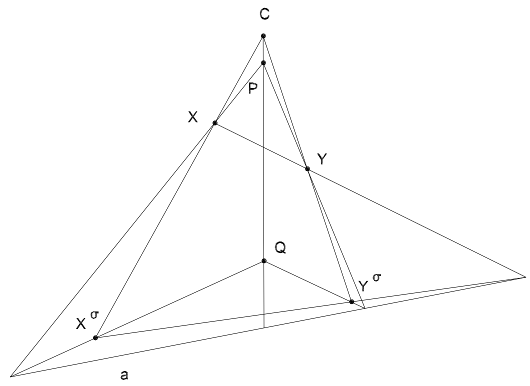
$$\exists a \in \mathcal{L} : \forall P \in \mathcal{P} : ((P \in a) \Rightarrow (P^\sigma = P)).$$

Voor centrum $C \in \mathcal{P}$ en as $a \in \mathcal{L}$ definieren wij

$$\Gamma(C, a) := \{\sigma \in \Gamma \mid \sigma \text{ heeft centrum } C \text{ en as } a\}.$$

Voor gegeven c, a, P, Q bestaat er ten hoogste één $\sigma \in \Gamma(C, a)$ zodat $P^\sigma = Q$. Een projectief vlak heet (C, a)-*transitief* als $\Gamma(C, a)$ transitief is op de niet vaste punten van een lijn $\neq a$ door C (hij is dan ook transitief op de lijnen $\neq a$ door C).

Stelling 3.2 *Een projectief vlak is (C, a)-transitief dan en slechts dan als de (C, a)-stelling van Desargues geldt.*



Figuur 3.1:

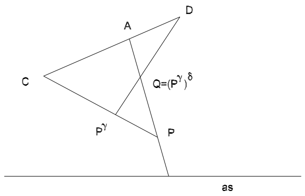
Inderdaad, bij gegeven C, a, P, Q definieer de $1--1$ afbeelding σ zoals aangegeven is in de tekening. Dan is σ een collineatie dan en slechts dan als voor alle X en Y geldt:

$$(X \cup Y) \cap a = (X^\sigma \cup Y^\sigma) \cap a.$$

Dit komt neer op de stelling van Desargues voor centrum C en as a.

Stelling 3.3 *Als een projectief vlak (C, a)-transitief en (D, a)-transitief is met $C \neq D$, dan is het ook (A, a)-transitief voor elke $A \in C \cup D$.*

Inderdaad, construeer $\delta_\gamma \in \Gamma(A, a)$ bij $\gamma \in \Gamma(C, a)$ en $\delta \in \Gamma(D, a)$ zoals hierboven aangegeven.



Figuur 3.2:

Een projectief vlak heet een *translatievlak* t.o.v. de as a, wanneer het (C, a)-transitief is voor elke $C \in a$.
Een projectief vlak heet een *Moufang vlak* wanneer het translatievlak is t.o.v. elke lijn.
Opmerking. Lenz en Barlotti klassificeerden alle mogelijkheden voor (C, a)-transitiviteiten van een projectief vlak, zie [6], p. 126.

3.2 Baer deelvlakken, Singer cykels

Zij $\pi = (\mathcal{P}, \mathcal{L})$ een projectief vlak van de orde n, en zij $\pi' = (\mathcal{P}', \mathcal{L}')$ een projectief vlak van de orde m, waarbij $\mathcal{P}' \subset \mathcal{P}$ en $\mathcal{L}' \subset \mathcal{L}$ (*** dit is niet helemaal consequent ***). Dan heet π' een deelvlak van π. Zij π' een *echt* deelvlak van π.

Stelling 3.4 *Als elk punt van $\mathcal{P}$ ligt op een lijn van $\mathcal{L}'$ dan geldt: $m^2 = n$; als dit niet zo is dan: $m^2 + m \leq n$.*

Bewijs. Als $P \in \mathcal{P}$ op geen enkele lijn van $\mathcal{L}'$ ligt, dan bevat elk der $n+1$ lijnen uit $\mathcal{L}$ door P ten hoogste één punt uit $\mathcal{P}'$. Anderzijds is elke $P' \in \mathcal{P}'$ verbonden met P door een lijn uit $\mathcal{L}$. Hieruit volgt dat $m^2 + m + 1 \leq n + 1$. Neem nu aan dat elke $P \in \mathcal{P}$ ligt op een $l' \in \mathcal{L}'$. dan wordt $\mathcal{P} \setminus \mathcal{P}'$ door de lijnen uit $\mathcal{L}'$ verdeeld in disjuncte klassen van elk $n - m$ punten:

$$n^2 + n + 1 - (m^2 + m + 1) = (n - m)(m^2 + m + 1), \quad (n - m)(n - m^2) = 0.$$

In het eerste geval, dus als $m^2 = n$, heet π' een Baer deelvlak.

Wij lichten dit toe met de Baer deelvlakken $PG(2, \mathbf{F}_3)$ van $PG(2, \mathbf{F}_9)$. Merk eerst op dat

$$GF(9) = \{a + b\varepsilon \mid \varepsilon^2 = -1;\, a, b \in GF(3)\}$$

wordt gegenereerd door $\omega := 1 - \varepsilon$ (en niet door ε).
$PG(2, \mathbf{F}_9)$ bevat 13 reële en 78 complexe punten. Wij vragen ons af of deze 91 punten kunnen worden gepartitioneerd in 7 disjuncte Baer deelvlakken van de orde 3, zie [24] pp. 67–88, i.h.b. p. 78.
Beschouw $PG(2, \mathbf{F}_q)$ met de bijbehorende vectorruimte $V = V(3, \mathbf{F}_q)$. Een niet-singuliere lineaire afbeelding $S : V \to V$ induceert een collineatie van $PG(2, \mathbf{F}_q)$. Een *Singer cykel* van $PG(2, \mathbf{F}_q)$ is een rij vectoren

$$x,\, Sx,\, S^2x,\, \ldots,\, S^{q^2+q}x$$

die alle punten van $PG(2, \mathbf{F}_q)$ voorstelt. Criterium is dat de *Singer matrix* S geen eigenwaarde in $\mathbf{F}_q$ heeft. Voor $PG(2, \mathbf{F}_3)$ en voor $PG(2, \mathbf{F}_9)$ voldoen

$$S = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \quad \text{en} \quad \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & \omega^2 \\ 0 & 1 & 0 \end{bmatrix}.$$

De boven gevraagde partite van $PG(2, \mathbf{F}_9)$ in 7 Baer deelvlakken wordt verkregen door de 13 machten van S toe te passen op de 7 vectoren $(1, 0, 0)$, $(\omega, 1, 0)$, $(-\omega, 1, 0)$, $(\omega^2, 1, 0)$, $(-\omega^2, 1, 0)$, $(\omega^3, 1, 0)$, $(-\omega^3, 1, 0)$.
Samen met $(0, 1, 0)$, $(1, 1, 0)$ en $(-1, 1, 0)$ vormen deze vectoren in het vlak $z = 0$ in $V(3, \mathbf{F}_9)$ een $PG(1, \mathbf{F}_9)$.

3.3 Transversal designs, etc.

Zij $S = \{0, 1, \ldots, n-1\}$ een verzameling van n symbolen. Een *k-vector* is een element van $S^k = S \times S \times \cdots \times S$. Noem de coördinaat posities de *plaatsen*
Een *transversal design* $T(k, n)$ op S is een verzameling van n^2 stuks k-vectoren zodat voor elk paar plaatsen elk geordend paar symbolen uit S precies één keer voorkomt. De $k \times n^2$ matrix die de k-vectoren als kolommen heeft is een *orthogonal array* $OA(k, n)$ van sterkte 2. Elk tweetal rijen heeft op overeenkomstige plaatsen precies alle geordende paren uit S (is orthogonaal).
Normaliseer de beide eerste rijen tot

$$\begin{matrix} 000 & \ldots & 0 & 11 & \ldots & 1 & \ldots & (n-1) & (n-1) & .. & (n-1) \\ 012 & .. & (n-1) & 01 & .. & (n-1) & .. & 0 & 1 & \ldots & (n-1) \end{matrix}.$$

Dan leveren de overige $k-2$ rijen, gearrangeerd in $n \times n$-matrices, een stelsel van $k-2$ *orthogonale latijnse vierkanten* van de orde n, zeg $k-2$ MOLS(n) (Mutually Orthogonal Latin Squares). Anders gezegd, selecteer voor de k-vector twee plaatsen (zeg rij en kolom). Voor een andere plaats m bepaalt elke rij $a \in S$ en kolom $b \in S$ een symbool $A^m_{a,b} \in S$. De matrix

$$A^m = \left[A^m_{a,b}\right]_{a,b \in S}$$

is een latijs vierkant. De $k-2$ aldus verkregen matrices $A^1, \ldots, A^{k-2}$ vormen $(k-2)$ MOLS.

Opgave 6 Bewijs dit!

Opgave 7 Bij een gegeven $T(k,n)$ wordt een graaf gedefinieerd als volgt. De knopen zijn de k-vectoren, en twee knopen zijn verbonden als de corresponderende k-vectoren op één plaats overeenstemmen. Deze graaf is sterk regulier. Bewijs dit.

De duale structuur van een transversaal design $TD(k,n)$ is een (k,n)-*net* N, dat als volgt wordt gedefinieerd. De *punten* van N zijn de k-vectoren van $TD(k,n)$. Een *lijn* van N is een verzameling van k-vectoren die op één plaats een constant symbool hebben. Een punt *ligt op* een lijn wanneer de corresponderende k-vector op de corresponderende plaats het corresponderende symbool heeft. Er zijn n^2 punten, elke lijn heeft n punten, door elk punt gaan k lijnen, er zijn nk lijnen. Voorts gelden (als $k > 2$) voor de verzameling $\mathcal{P}$ der punten en $\mathcal{L}$ der lijnen de volgende eigenschappen.

N1. Er is ten hoogste één lijn door twee verschillende punten.

N2. $\forall P \in \mathcal{P} : \forall P \notin l \in \mathcal{L} : \exists! m \in \mathcal{L} : (P \in m,\ l \cap m = \emptyset)$.

N3. Er zijn 3 punten niet op een lijn, zodat elk tweetal op een lijn ligt.

Omgekeerd, zij $(\mathcal{P}, \mathcal{L})$ een eindige incidentie structuur die voldoet aan N1, N2, N3. Noem $l, m \in \mathcal{L}$ *evenwijdig* wanneer l en m samenvallen of gerelateerd zijn volgens N2. Evenwijdigheid is een equivalentie relatie (bewijs!), die $\mathcal{L}$ verdeelt in (zeg k) klassen van een constant aantal (zeg n) onderling evenwijdige lijnen. Er zijn n^2 punten, nk lijnen, n punten per lijn, en van elk der k klassen één lijn per punt (bewijs!). Geef de n verschillende lijnen van elke klasse aan door verschillende symbolen uit $\{0, 1, \ldots, n-1\}$. Dan wordt elk punt aangegeven door een k-vector. De n^2 punten vormen de k-vectoren van een transversal design. Inderdaad, voor elk paar klassen komt elk geordend paar symbolen precies één keer voor.

Stelling 3.5 *De volgende objecten zijn equivalent:* $T(k,n)$*,* $OA(k,n)$*,* $(k-2)$ *MOLS(n),* (k,n)*-net.*

3.4 Het affiene vlak

Een *affien vlak* is een incidentie structuur zodat

AG 1. Elk tweetal verschillende punten ligt op één lijn.

AG 2. Voor elk punt-lijn paar (P,l) met $P \notin l$ is er één lijn door P en disjunct met l (zeg $||l$).

AG 3. Er zijn 3 punten die niet op een lijn liggen.

Zij l een lijn van het projectieve vlak $\mathcal{P}$. Zij $\mathcal{P}^l$ de incidentie structuur die ontstaat door uit $\mathcal{P}$ de lijn l met al zijn punten weg te laten. Dan is $\mathcal{P}^l$ een affien vlak.

Stelling 3.6 *Bij een affien vlak $\mathcal{A}$ behoort een op isomorfie na eenduidig projectief vlak $\mathcal{P}$ met de eigenschap dat $\mathcal{A} = \mathcal{P}^l$ voor zekere l van $\mathcal{P}$.*

Inderdaad, zij $\mathcal{A}$ een affien vlak. Voeg toe als punten de klassen van de equivalentie relatie $(l = m) \vee (l \parallel m)$. Voeg toe als lijn de verzameling v der klassen. Met geschikte incidentie ontstaat dan een projectief vlak $\mathcal{P}$ met $\mathcal{P}^v = \mathcal{A}$. De lijn v heet de *oneigenlijke lijn* voor $\mathcal{A}$, en de punten van v heten de *oneigenlijke punten* voor $\mathcal{A}$.

Stelling 3.7 *De affiene vlakken $\mathcal{P}^l$ en $\mathcal{P}^m$ zijn isomorf dan en slechts dan als $\exists \sigma \in Coll(\mathcal{P}) \,:\, (l^\sigma = m)$.*

Als Coll($\mathcal{P}$) niet transitief is op de lijnen van $\mathcal{P}$ dan behoren dus bij $\mathcal{P}$ niet-isomorfe affiene vlakken.
Een *eindig affien vlak* heeft de orde n, wanneer het bijbehorende projectieve vlak de orde n heeft, en wordt genoteerd met $AG(2, n)$. Het vlak heeft n^2 punten, $n^2 + n$ lijnen, n punten per lijn, $n + 1$ lijnen per punt, en $n + 1$ parallelklassen van elk n lijnen.

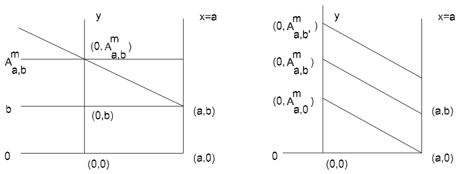
Stelling 3.8 *De volgende objecten zijn equivalent: $AG(2, n)$, $T(n+1, n)$, $OA(n+1, n)$, $(n-1)$ MOLS(n).*

We geven nogmaals het verband tussen $AG(2, n)$ en $T(n + 1, n)$. Zij gegeven een transversal design $T(n+1, n)$ op S. Een punt is een $(n+1)$-vector. Een lijn is een verzameling van $(n+1)$-vectoren die op één plaats een constant symbool hebben. Dan vormen de punten en de lijnen een $AG(2, n)$ (bewijs!).
Omgekeerd, ga uit van het affiene vlak $AG(2, n)$. Noem de punten van l_∞ de plaasen. Selecteer twee oneigenlijke punten $Y = (x-$ coördinaat) en $X =$ $(y-$coördinaat). Voorzie de lijnen door Y en de lijnen door X van verschillende symbolen uit $S = \{0, 1, \ldots, n-1\}$. Dan heeft elk punt van $AG(2, n)$ twee coördinaatsymbolen. Als B het snijpunt is van de lijn met symbool 0 door Y en de lijn met symbool b door X, dan krijgt elke lijn door B het symbool b (behalve BY die als het symbool 0 heeft). Nu zijn alle lijnen voorzien van symbolen. Voeg aan elk punt P toe de $(n+1)$-vector waarvan elke plaats wordt gevuld met het symbool van de lijn door P naar die plaats op l_∞. De aldus gedefinieerde $(n+1)$-vectoren vormen een transversal design $T(n+1, n)$ over S (bewijs!).
De n^2 kolommen van de bijbehorende $OA(n + 1, n)$ komen overeen met de n^2 punten van $AG(2, n)$, gearrangeerd volgens de n punten van de n lijnen door Y.

Zonder de algemeenheid te schaden kunnen wij $OA(n+1,n)$ de volgende vorm geven (in de eerste kolom staan de plaatsen):

$$\begin{array}{c|c|cc|c|ccc|c|ccc|}
Y & 0\,0\ldots\ 0 & 1\,1 & 1 & . & aa & a & a & . & n-1 & \ldots & n-1\\
X & 0\,1\ldots n-1 & 0\,1 & n-1 & . & 01 & b & n-1 & . & 0 & \ldots & n-1\\
1 & 0\,1\ldots n-1 & 1 & & . & a & & & . & n-1 & & \\
. & \ldots\ldots & & & . & & & & . & & & \\
m & 0\,1\ldots n-1 & m & & . & A^m_{a,0} & A^m_{a,b} & & . & & & \\
. & \ldots\ldots & & & . & & & & . & & & \\
n-1 & 0\,1\ldots n-1 & n-1 & & . & & & & . & & &
\end{array}$$

De lijn door Y met symbool a en de lijn door X met symbool b bepalen een punt met coördinaten (a,b) waarvan de verbindingslijn naar de plaats m het symbool $A^m_{a,b}$ krijgt.



Figuur 3.3:

De lijnen door de punten van $x = a$ naar de plaats m snijden de Y-as volgens de ordinaten $A^m_{a,y}$. Deze symbolen vormen de a-de rij van

$$A^m = \left[A^m_{a,b}\right]_{a,b\in S}.$$

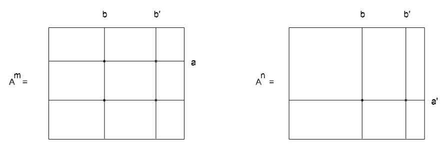
De matrices $A^1, \ldots, A^{n-1}$ vormen een $(n-1)$ MOLS(n). De m-de rij van het $OA(n+1,n)$ is de concatenatie van de rijen van A^m.

Opmerking. $A^m_{a,b}$ definieert een ternaire relatie A op S, zie [14]

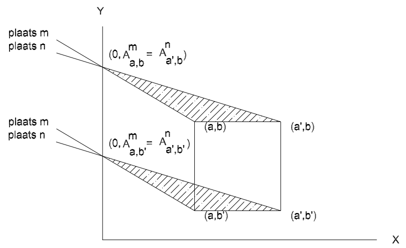
Een affien vlak $AG(2,n)$ heet *lineair* wanneer, voor alle $m = 1, 2, \ldots, n-1$ de matrices A^m dezelfde verzameling van rijen hebben.

Stelling 3.9 $AG(2,n)$ *is lineair dan en slechts dan als de prisma eigenschap van Desargues geldt t.o.v.* (Y, l_∞).

Bewijs. Beschouw de Latijnse vierkanten A^m en A^n. Wij willen aantonen dat er bij elke rij a van A^m een rij a' van A^n bestaat, die overeenstemt op de kolommen b en b'.



Een blik op de onderstaande figuur geeft het verband met de prisma eigenschap



Figuur 3.4:

Voorbeeld. Constructie van $AG(2, \mathbf{F}_4)$ met behulp van 3 MOLS(4). Zowel $AG(2, \mathbf{F}_4)$ als het bijbehorende $PG(2, 4)$ zijn uniek.

Y	0	0	0	0	1	1	1	1	2	2	2	2	3	3	3	3
X	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3
1	0	1	2	3	1	0	3	2	2	3	0	1	3	2	1	0
2	0	1	2	3	2	3	0	1	3	2	1	0	1	0	3	2
3	0	1	2	3	3	2	1	0	1	0	3	2	2	3	0	1

De rijen 1,2,3 van het OA zijn de concatenaties van de drie orthogonale Latijnse vierkanten van de orde 4. In dit voorbeeld komen de Latijnse vierkanten ook voor als deelmatrices van de OA. Is dit toeval?
Neem aan dat het omgekeerde van de prisma-eigenschap van Desargues geldt t.o.v. (X, l_∞). Dan vormen de deelmatrices $B^1, \dots, B^{n-1}$ van het OA een stelsel van $(n-1)$ MOLS(n):

$$\begin{array}{ccc|ccc|ccc|c|ccc|}
0 & \dots & 0 & 1 & \dots & 1 & 2 & \dots & 2 & & n-1 & \dots & n-1 \\ \cline{4-9} \cline{11-13}
0 & \dots & n-1 & & & & & & & & & & \\
 & & & & B^1 & & & B^2 & & \dots & & B^{n-1} & \\
0 & \dots & n-1 & & & & & & & & & &
\end{array}$$

Inderdaad, de matrices B^i zijn latijse vierkanten (Bewijs!). Voorts zijn B^i en B^j orthogonaal. Immers, stel van niet, dus stel dat de volgende situatie optreedt:

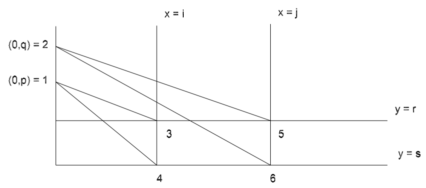
$$\begin{array}{|ccccc|c|ccccc|c|ccccc|c}
0 & \dots & 0\,0 & \dots & 0 & & \mathrm{i} & \dots & \mathrm{i\,i} & \dots & \mathrm{i} & & \mathrm{j} & \dots & \mathrm{j\,j} & \dots & \mathrm{j} & \\ \hline
0 & \dots & \mathrm{p\,q} & \dots & n-1 & & 0 & \dots & \mathrm{r\,s} & \dots & n-1 & & 0 & \dots & \mathrm{r\,s} & \dots & n-1 & \\
 & & & & & & & & & & & & & & & & & \\
 & & \mathrm{p\,q} & & & \dots & & & \mathrm{p} & & & \dots & & & \mathrm{q} & & & \dots \\
 & & \mathrm{p\,q} & & & & & & \mathrm{\ \ p} & & & & & & \mathrm{\ \ q} & & & \\
 & & & & & & & & & & & & & & & & & \\ \hline
 & & 1\,2 & & & & & & 3\,4 & & & & & & 5\,6 & & &
\end{array}$$

De kolommen 1,2,3,4,5,6 corresponderen met zes punten in het affiene vlak waarvoor geldt

$$12 \parallel 34 \parallel 56,\ 13 \parallel 25,\ 14 \parallel 26 \ \text{ en } \ 35 \parallel 46.$$

Dit is strijdig met de omgekeerde prismaeigenschap, die zegt dat

$$12 \parallel 35 \parallel 46.$$

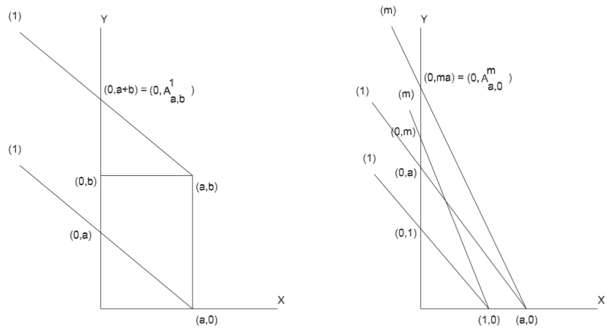


Figuur 3.5:

Stelling 3.10 *$B_i = [A^m_{ib}]_{m,b\in S}$, $i = 1, \ldots, n-1$ vormen $(n-1)$ MOLS(n) als het omgekeerde van de prisma-eigenschap van Desargues geldt t.o.v. (X, l_∞).*

3.5 Optellen en vermenigvuldigen van coördinaten.

Voor elk punt van $AG(2,n)$ hebben wij coördinaten t.o.v. de oneigenlijke punten Y en X geintroduceerd, waarbij $a, b \in S = \{0, 1, \ldots, n-1\}$. Voor de symbolen uit S definieren wij de *optelling* en de *vermenigvuldiging* als volgt (zie [14], chapter 5).



Figuur 3.6:

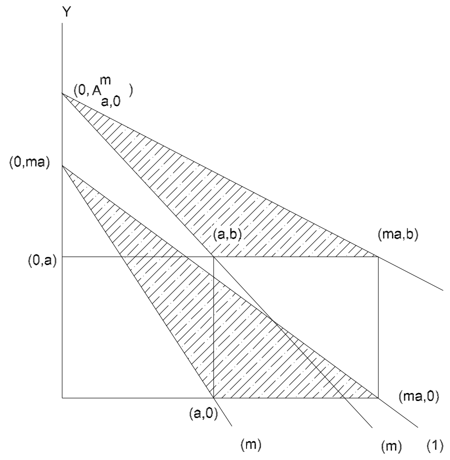
Voor de aldus gedefinieerde bewerkingen geldt (ga na!)

$$\begin{array}{lll} 0+a=a=a+0, & \exists!\, x\in S\ (a+x=c), & \exists!\, x\in S\ (x+b=c), \\ 1\,a=a=a\,1 & \exists!\, x\in S\ (m\,x=c), & \exists!\, x\in S\ (x\,a=c). \end{array}$$

Dit maakt zowel $(S,+)$ als $(S,.)$ tot een *loop*.

OPMERKING. Dit maakt S met de ternaire relatie $A^m_{a,b}$ tot een ternaire ring, zie [**?**] p. 113.

De geldigheid van andere algebraische eigenschappen in $(S,+,.)$ hangt samen met de geldigheid van bepaalde meetkundige eigenschappen, en van transitiviteits-eigenschappen van de collineatie groep. Wij geven enige voorbeelden. Voor uitputtende behandeling zie [14] en [4].
Beschouw de lijn door (a,b) en het oneigenlijke punt (m); deze lijn snijdt de Y-as in $(0, A^m_{a,b})$. Zojuist hebben wij het punt $(0, ma)$ gedefinieerd met behulp van de lijn door $(a,0)$ en (m).



Figuur 3.7:

Stelling 3.11 *Als $AG(2,n)$ lineair is, dan geldt*

$$\forall m, a, b \in S : \ (A^m_{a,b} = ma + b).$$

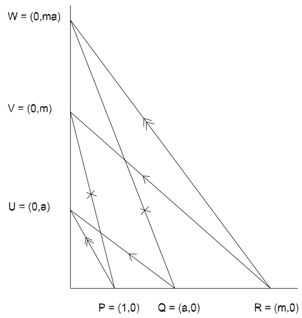
BEWIJS. De lineariteit van $AG(2,n)$ is gelijkwaardig met het gelden van de prisma-eigenschap t.o.v. (Y, l_∞). De verbindingslijnen van de corresponderende hoekpunten van de gearceerde driehoeken zijn evenwijdig aan de Y-as. Eén paar zijden is evenwijdig aan (m), één paar is evenwijdig aan de X-as. Dan moet ook het derde paar evenwijdig zijn, en moet de lijn door (ma, b) door (1) gaan. Wegens de definitie van optelling volgt hieruit het gestelde. □

$AG(2,n)$ is een *translatievlak* dan en slechts dan als de prisma-eigenschap geldt voor alle oneigenlijke centra. Voor een translatievlak geldt behalve de lineariteit ook dat $(S,+)$ een Abelse groep is, en dat ook voor $(S,+,.)$ de links-distributieve wet geldt:

$$a(b+c) = ab + ac.$$

Dit maakt $(S,+,.)$ tot een *quasifield* (= Veblen-Wedderburn system). Als ook de pyramide-eigenschap onbeperkt geldt, dan geldt ook de andere distributieve wet en is $(S,+,.)$ een *division-ring* (= semi-field).
De volledige geldigheid van stelling van Desargues maakt ook de vermenigvuldigin associatief, en $(S,+,.)$ is een *scheef-lichaam.* Eindige scheve lichamen hebben een commutatieve vermenigvuldiging (Stelling van Wedderburn). De

volledige geldigheid van Desargues voor $AG(2,n)$ maakt dus $(S,+,.)$ tot een eindig lichaam. Volgens de stelling van Artin-Zorn wordt $(S,+,.)$ reeds tot een eindig lichaam door het bestaan van alle mogelijke elaties voor $AG(2,n)$. Voor bijzonderheden zij verwezen naar [14]
Tenslotte tonen wij aan dat de commutativiteit van de vermenigvuldiging in $(S,+,.)$ volgt uit de geldigheid van het bijzondere geval van de stelling van Pappus dat op blz. * werd besproken. Inderdaat, uit $PV \parallel QW$, $QU \parallel RV$ volgt dat $PU \parallel RW$, dus $(0,ma) = W = (0,am)$ en $am = ma$:



Figuur 3.8:

3.6 Niet-Desarguese vlakken.

Er bestaan drie voorbeelden van projectieve vlakken $PG(2,9)$ waarin de stelling van Desargues niet altijd geldt, zie [24]. Zij zijn gebaseerd op het *nearfield* van de orde 9. Zij

$$Q = \{0, \pm 1, \pm\alpha, \pm\beta, \pm\gamma \,:\, \alpha+\beta+\gamma = 0,\ \alpha-\beta = \beta-\gamma = \gamma-\alpha = 1\}$$

een vectorruimte van dimensie 2 over $GF(3)$. Definieer vermenigvuldiging zoals bij de quaternionen:

$$\alpha^2 = \beta^2 = \gamma^2 = -1,\ \beta\gamma = -\gamma\beta = \alpha,\ \gamma\alpha = -\alpha\gamma,\ \alpha\beta = -\beta\alpha = \gamma,$$

zodat $\alpha\beta\gamma = -1$. Dit maakt $(Q,+,.)$ tot een nearfield (alle lichaamseigenschappen gelden, behalve de commutativiteit en de links-distributiviteit, wèl de rechts-distributiviteit):

$$\begin{aligned}(\beta+1)\beta &= \alpha\beta = \alpha(\alpha-1)\\ \beta^2+\beta = -1+\beta &= \gamma = 1+\alpha = -\alpha^2+\alpha.\end{aligned}$$

Noem $\mathbf{R} := \{0, \pm 1\}$ reëel en $\mathbf{I} = \{\pm\alpha, \pm\beta, \pm\gamma\}$ imaginair. Dit nearfield heeft Aut= $Sym(3)$ met 6 elementen tegen 2 voor $GF(9)$.

OPMERKING. In termen van een primitief element ω kunnen we in $Q = \{0, \omega^0, \omega^2, \omega^4, \omega^6, \omega^1, \omega^3, \omega^5, \omega^7\}$ de vermenigvuldiging definieren door $\omega^i\omega^j = \omega^{i+j}$ voor j even, $\omega^i\omega^j = \omega^{i+3j}$ voor j oneven.

Met behulp van het nearfield Q definieren wij een affien vlak door

$$\begin{aligned} \mathcal{P} &= \{(x,y) \mid x, y \in Q\}, & |\mathcal{P}| &= 81, \\ \mathcal{L} &= \{y = xm + n \text{ en } x = a \mid m, n, a \in Q\}, & |\mathcal{L}| &= 90. \end{aligned}$$

Er is voldaan aan de axioma's van een affien vlak. Inderdaad, zij $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$. Als $x_1 = x_2$, $y_1 \neq y_2$ dan voldoet slechts $x = x_1$. Als $x_1 \neq x_2$ dan moet

$$\begin{gathered} y_1 = x_1 m + n, \quad y_2 = x_2 m + n, \quad y_1 - y_2 = (x_1 - x_2)m, \\ m = (x_1 - x_2)^{-1}(y_1 - y_2), \quad n - y_2 - x_2 m. \end{gathered}$$

Voor $A = (a, b)$, $l = \{(x, y) \mid y = xm + n\}$ voldoet de lijn $y = xm + (b - am)$ aan het axioma van Euclides.
De collineaties van het aldus gedefinieerde affiene vlak zijn

$$\begin{aligned} &(x,y) \mapsto (x+\rho, y+\sigma);\ (x,y) \mapsto (x\rho, y\sigma)\ \rho, \sigma \neq 0; \\ &(x,y) \mapsto (y,x);\ (x,y) \mapsto (x+y, x-y); \\ &(x,y) \mapsto (Sx, Sy),\ S \in \mathrm{Aut}(Q), \quad \text{voor } \rho, \sigma \in Q. \end{aligned}$$

Het bestaan van de eerste groep van collineaties maakt het vlak een translatievlak.

OPMERKING. De afbeeldingen $(x, y) \mapsto (\rho x, \sigma y)$ behoeven geen collineaties te zijn. Bij voorbeeld $(x, y) \mapsto (\alpha x, \alpha y)$ beeldt de op $y = x + 1$ liggende punten $(0, 1)$, $(1, -1)$, (α, γ) af op de niet-collineaire $(0, \alpha)$, $(\alpha, -\alpha)$, $(-1, -\beta)$.

Opgave 8 Geef een voorbeeld waaruit volgt dat dit projectieve vlak niet-Desargues is.

Ook het duale vlak is een projectief vlak (niet-isomorf) waarin Desargues niet algemeen geldt.
Er is nog een derde vlak waarin Desargues niet geldt; het is zelfduaal; het is een Hughes-vlak, de punten zijn alle (x, y), $x, y \in Q$. De Rechten zijn reëel of imaginair, $12 + 78 = 90$ stuks:

$$\begin{array}{ll} y = ax + b, & y - b = p(x - a) \quad , \\ x = c & y = ax + q,\ x = r \ ; \\ a, b, c \in \mathbf{R}. & p, q, r \in \mathbf{I}. \end{array}$$

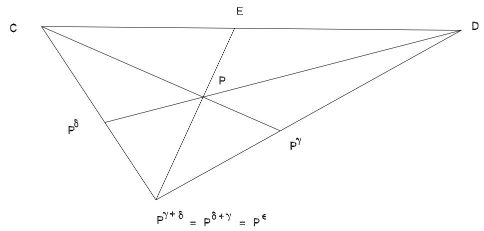
Dit Hughes-vlak is geen translatievlak, zie [24].

Opmerking. Bij deze 4 projectieve vlakken behoren $7 = 1 + 2 + 2 + 2$ affiene vlakken van de orde 9. Zie [15].

3.7 Eindige affiene translatievlakken.

Een *translatie* van $AG(2, n)$ is een elatie met l_∞ als as. $AG(2, n)$ bezit ten hoogste n^2 translaties. Inderdaad, l_∞ bevat $n + 1$ mogelijke centra voor translaties; voor elk centrum bestaan (afgezien van de identiteit) ten hoogste $n - 1$ translaties. Wij gebruiken de additieve schrijfwijze voor de groepen $\Gamma_{C_i} := \Gamma_{C_i,l_\infty}$ der translaties met centrum C_i en as l_∞. Wij nemen aan dat er tenminste twee centra C_1, $C_2 \in l_\infty$ zijn waarvoor $\Gamma_{C_i} \neq \{0\}$.

Stelling 3.12 *$T := \bigcup_{C \in l_\infty} \Gamma_C$ is een elementair Abelse groep (een directe some van cyclische groepen $\mathbf{Z}_p$, voor eenzelfde priemgetal p).*



Figuur 3.9:

Bewijs. Voor $\gamma \in \Gamma_C$, $\delta_i n \Gamma_D$ geldt $\gamma + \delta \in \Gamma_E$, dus T is een groep. Voor $C \neq D$ vormen P, P^γ, P^δ, $P^{\gamma+\delta}$ een parallellogram, dus $\gamma + \delta = \delta + \gamma$. Ook voor γ, $\gamma' \in \Gamma_C$ volgt de commutativiteit. Er bestaat een $\gamma \in \Gamma_C$ van priem orde, zeg p. Dan heeft ook $0 \neq \delta \in \Gamma_d$ de orde p. Inderdaad,

$$p\delta \in \Gamma_D,\ \gamma \neq 0 = p\gamma,\ p\delta = p\delta + p\gamma = p(\delta + \gamma) \in \Gamma_E,$$

en $\Gamma_D \cap \Gamma_E = \{0\}$. Alle elementen $\neq 0$ hebben dus de orde p en T is elementair Abels. □

GEVOLG. $|\Gamma_C|$ is deelbaar op n, voor elke $C \in l_\infty$; $|T|$ is deelbaar op n^2.

Voor de rest van deze paragraaf nemen wij aan dat $AG(2,n)$ een *translatievlak* is. Dan geldt

$$|T| = n^2 \quad \text{en} \quad |\Gamma_C = n| \quad \text{voor elke } C \in l_\infty.$$

Als gevolg van de stelling is de *translatie groep* T commutatief en $n = p^k$, p priem.
Zij $(\Phi, +, .)$ de *ring der endomorfismen* van T, dat is

$$\Phi := \left\{ \phi : T \to T \,|\, \forall \alpha, \beta \in T : ((\alpha + \beta)^\phi = \alpha^\phi + \beta^\phi) \right\},$$

waarin $\phi + \psi$, $\phi.\psi$ worden gedefinieerd door

$$\forall \alpha \in T : (\alpha^{\phi.\psi} := (\alpha^\phi)^\psi, \, \alpha^{\phi+\psi} = \alpha^\phi + \alpha^\psi).$$

De *kern* K van $T = \bigcup_{C \in l_\infty} \Gamma_C$ is de verzameling der endomorfismen $\phi : T \to T$ waarvoor

$$(\Gamma_C)^\phi \subset \Gamma_C, \quad \text{voor elke } C \in l_\infty.$$

Stelling 3.13 $(K, +, .)$ *is een lichaam.*

BEWIJS. De endomorfismen identiteit en $0 : T \to \{0\}$ behoren tot K. Zij $\phi, \psi \in K$ dan $\phi\psi \in K$ en $\phi \pm \psi \in K$ wegens

$$(\Gamma_C)^{\phi\psi} \subset \Gamma_C^\phi \subset \Gamma_c, \, \gamma^{\phi \pm \psi} = \gamma^\phi + \gamma^{\pm\psi} \in \Gamma_C^\phi + \Gamma_C^\psi \subset \Gamma_C + \Gamma_C = \Gamma_C$$

voor $\gamma \in \Gamma_C$. Blijft nog aan te tonen dat elke $\phi \in K^*$ een inverse heeft en dus dat elke $\phi \in K^*$ één-éénduidig op is. Inderdaad, zij $\gamma^\phi = \delta^\phi$ met $\gamma \neq \delta \in T$ dus $\gamma - \delta =: \alpha \neq 0 = \alpha^\phi$. Zij $\alpha \in \Gamma_A$, kies $\beta \in \Gamma_B \in T \setminus \Gamma_A$, dan $\alpha + \beta \neq \Gamma_A \cup \Gamma_B$ maar (zeg) $\alpha + \beta \in \Gamma_C$, $A \neq c \neq B$. Nu geven $\beta^\phi = \alpha^\phi + \beta^\phi = (\alpha + \beta)^\phi \in \Gamma_C$ en $\Gamma_B \cup \Gamma_C = \{0\}$ dat $\beta^\phi = 0$. Maar dan is $\tau^\phi = 0$ voor elke $\tau \in T$, dus $\phi = 0$, een tegenspraak. Dit bewijst dat $\phi \in K^*$ één-éénduidig is. Bewijs zelf dat ϕ een afbeelding op is. $\square$

Een *vectorruimte* over een lichaam K is een Abelse groep T en een afbeelding $K \times T \to T$ zodat voor alle $\phi, \psi \in K$; $\alpha, \beta \in T$ geldt:

$$\phi(\alpha + \beta) = \phi\alpha + \phi\beta, \; (\phi + \psi)\alpha = \phi\alpha + \psi\alpha, \; (\phi\psi)\alpha = \phi(\psi\alpha), \; 1\,\alpha = \alpha.$$

Stelling 3.14 *De groep T der translaties van een translatievlak is een vectorruimte over de kern K. De ondergroepen Γ_C, $C \in l_\infty$, zijn lineaire deelruimten. In de corresponderende projectieve ruimte vormen de corresponderende deelruimten een spread.*

VOORBEELD. Zij gegeven een spread van lijnen in $PG(3,q)$. Beschouw $PG(4,q) = AG(4,q) \cup PG(3,q)$. Noem "punten" de q^4 putnen van $AG(4,q)$. Noem "lijnen" de vlakken in $PG(4, q)$ die $PG(3, q)$ snijden in een lijn van de spread. De "punten" en "lijnen" vormen een affien translatievlak van de orde q^2. Inderdaad, er is voldaan aan de axioma's (ga na!).

Opgave 9 Zij gegeven een spread van deelruimten $PG(r-1, q)$ in $PG(2r-1, q)$. Beschouw

$$PG(2r, q) = AG(2r, q) \cup PG(2r-1, q).$$

Definieer een $AG(2, q^r)$.

Stelling 3.15 (André 1954) . *Er is een 1-1 correspondentie tussen de translatievlakken van de orde q^{t+1} met kern $\mathbf{F}_q$, en de t-spreads in $PG(2t+1, q)$.*

Voor verder theorie en constructie zij verwezen naar [23], [**?**] §11, en [6] chapter V.

Hoofdstuk 4

Polaire meetkunde

4.1 Polariteiten

Zij $\mathcal{P}$ een projectieve meetkunde, dat is, de verzameling van alle deelruimten van een projectieve ruimte. Een *correlatie* δ van $\mathcal{P}$ is een permutatie van $\mathcal{P}$ die de inclusie inverteert:

$$\forall S, T \in \mathcal{P} \,:\, ((S \subset T) \Rightarrow (T^\delta \subset S^\delta)).$$

Een *polariteit* π is een correlatie van de orde 2, dus π^2 =id. Dan geldt ook

$$\forall S, T \in \mathcal{P} \,:\, ((S \subset R^\pi) \Rightarrow (T \subset S^\pi)).$$

Een voorbeeld van een polariteit in een projectief vlak is de klassieke verwantschap pool $\longleftrightarrow$ poollijn ten opzichte van een kegelsnede.
Voor een correlatie δ heet $S \subset \mathcal{P}$ *totaal isotroop* als $S \cap s^\delta = S$, *niet-isotroop* als $S \cap S^\delta = \emptyset$, *isotroop* als S een isotroop punt bevat (d.w.z. een punt p met $p \in p^\delta$).

Stelling 4.1 *Een polariteit van een eindig projectief vlak heeft tenminste één isotroop punt.*

Bewijs (Ryser). Zij π een polariteit van $PG(2,n)$; nummer de punten en de lijnen van $PG(2,n)$ zó dat $l_i = P_i^\pi$, voor $i = 1, \ldots, n^2+n+1$. Dan is de punt-lijn incidentie matrix N symmetrisch, en

$$N^2 = N\,N^t = nI + J.$$

Daarom heeft N de eigenwaarden $(n+1)^1$, $(\sqrt{n})^a$, $(-\sqrt{n})^b$. Stel

$$\text{Spoor } N = n + 1 + (a-b)\sqrt{n} = 0,$$

dan zou $\sqrt{n}$ geheel en deelbaar op $n+1$ moeten zijn. Dit is onmogelijk voor $n > 1$. Dus Spoor $N \neq 0$, diag N bevat tenminste één 1, er is dus tenminste één punt $p \in p^\pi$.

Zij $\mathcal{P}(V)$ de projectieve meetkunde die behoort bij een vectorruimte V over een lichaam $\mathbf{F}$. Een voorbeeld van een correlatie van $\mathcal{P}(V)$ wordt gegeven door

$$\delta : S \mapsto S^\delta := \{x \mid f(x, S) = 0\}, \quad S \in \mathcal{P},$$

waarin $f : V \times V \to \mathbf{F}$ een niet ontaarde bilineaire vorm op V is (zie [12] hoofdstuk 3, "Pairings and bilinear forms"). De afbeelding δ is eveneens een correlatie wanneer f een niet-ontaarde sesquilineaire vorm is (zie [12] hoofdstuk 5, "The unitary group"). Omgekeerd is elke correlatie van $\mathcal{P}(V)$ afkomstig van een niet-ontaarde sesquilineaire vorm op V.
Zij $- \in \mathrm{Aut}\mathbf{F}$. Een *sesquilineaire vorm* $f : V \times V \to \mathbf{F}$ wordt gedefinieerd door

$$\begin{aligned} f(x + x', y + y') &= f(x, y) + f(x, y') + f(x', y) + f(x', y'), \\ f(\alpha x, \beta y) &= \alpha\bar{\beta} f(x, y), \end{aligned}$$

voor alle $x, x', y, y' \in V$ en $\alpha, \beta \in \mathbf{F}$. Wanneer $-$ de identiteit is, dan is f een *bilineaire vorm*. Een sesquilineaire vorm is *niet-ontaard* wanneer

$$(\forall y \in V : (f(x, y) = 0)) \Rightarrow (x = 0),$$

m.a.w. wanneer $v^\delta = \{0\}$. Een sesquilineaire vorm f heet *reflexief* wanneer

$$\forall x, y \in v : ((f(x, y) = 0) \Rightarrow (f(y, x) = 0)).$$

De polariteiten van $\mathcal{P}(V)$ zijn precies de polariteiten die afkomstig zijn van de reflexieve niet-ontaarde sesquilineaire vormen op V. Deze zijn de volgende (voor het bewijs zie [12], 3.13 en 5.2, of [7], 5.3 en 5.8.).

I. (alternerend): $- = \mathrm{id}$, $\quad \forall x \in V : f(x, x) = 0),$

II. (symmetrisch): $- = \mathrm{id}$, $\quad \forall x, y \in V : f(x, y) = f(y, x), \exists z \in V : (f(z, z) \neq 0),$

III. (Hermiets): $- \neq \mathrm{id}$, $\quad \forall x, y \in V : (f(x, y) = f(\bar{y}, x)).$

In het geval I volgt dat

$$\forall x, y \in V : (f(x, y) + f(y, x) = 0),$$

dus dat de vorm scheef is voor char $\mathbf{F} \neq 2$, en symmetrisch voor char $\mathbf{F} = 2$.
De polariteiten van $\mathcal{P}(V)$, die behoren bij de gevallen I,II,III worden genoemd symplectische, orthogonale en unitaire polariteiten respectievelijk. Een *symplectische, orthogonale, unitaire* projectieve meetkunde is een $\mathcal{P}(V)$, waarbij V is voorzien van een symplectische, orthogonale of unitaire polariteit.

4.2 Symplectische Meetkunde

Een symplectische ruimte (V, f) is een vectorruimte $V(d, \mathbf{F})$ voorzien van een niet-ontaarde alternerende bilineaire vorm f. Noteer $f = (\ ,\ )$. Kies $c_1 \in V$, en kies $c_2 \in V$ zó dat $(c_1, c_2) = 1$. Kies $c_3 \in V$ zodat $c_3 \perp \langle c_1, c_2 \rangle$, en herhaal dit proces. In termen van de tweedimensionale deelruimten $V_i = \langle c_{2i-1}, c_{2i} \rangle$ (de *hyperbolische vlakken* schrijven wij

$$V = V_1 \perp V_2 \perp \ldots \perp V_{d/2}.$$

Na verandring van volgorde heeft de basis (de *symplectische basis*) de matrix (de *Gram matrix*)

$$[(c_i, c_j)] = \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix}$$

Blijkbaar is d even, en heeft V totaal isotrope deelruimten van dimensie $d/2$.

Opmerking. Wanneer (,) ontaard is dan is er een niet triviaal *radicaal*

$$\operatorname{Rad} V := \{y \in V \mid \forall x \in V \,:\, ((x, y) = 0)\},$$

$V = \operatorname{Rad} V \perp V_1 \perp \cdots \perp V_m = U_1 \perp \cdots \perp U_r \perp V_1 \perp \cdots \perp V_m$, waarin $U_i = \langle a_i \rangle$, $V_i = \langle c_{2i-1}, c_{2i} \rangle$, a_i isotroop, c_{2i-1} en c_{2i} een hyperbolisch paar als boven.

Opmerking. Al is een vorm f niet-ontaard op V, zijn restrictie tot een deelruimte U van V kan best ontaard zijn.

Een *isometrie* van (V, f) in (V', f') is een lineaire afbeelding $\rho : V \to V'$ zodat

$$\forall x, y \in V \,:\, (f'(\rho x, \rho y) = f(x, y)).$$

Stelling 4.2 (Witt) *Zij $\rho : V \to V'$ een isometrie* op *van twee symplectische ruimten (V, f) en (V', f'). Zij $\sigma : U \to V'$ een isometrie van een deelruimte $U < V$ in V'. Dan kan σ worden uitgebreid tot een isometrie $\tilde{\sigma} : V \to V'$.*

Voor het bewijs zie [12], 3.28, 3.30, 3.31, 3.32. Een gevolg van de stelling van Witt is dat alle maximale totaal isotrope deelruimten van V dezelfde dimensie hebben. Deze dimensie heet de *index* van V.
De *symplectische groep* $Sp(V)$ is de groep van alle isometrieen van V op zichzelf. In termen van matrices bestaat $Sp(V)$ uit alle A met

$$A \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix} A^t = \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix}.$$

Dan $\det A = \pm 1$, in feite $\det A = 1$ (zie [12], 4.4).
De orde van $Sp(d, \mathbf{F}_q)$ kan worden bepaald door het aantal geordende symplectische bases te tellen. Voor c_1 zijn $q^d - 1$ mogelijkheden. Als $(c_1, c_2) = 1 = (c_1, c_2')$, dan $(c_1, c_2 - c_2') = 0$, dus voor c_2 zijn q^{d-1} mogelijkheden. Daarom geldt

$$\begin{aligned} |Sp(d, \mathbf{F}_q)| &= q^{d-1}(q^d - 1)q^{d-3}(q^{d-2} - 1) \cdots q(q^2 - 1) = \\ &= q^{(d/2)^2} \prod_{i=1}^{d/2} (q^{2i} - 1). \end{aligned}$$

Voor de structuur van $Sp(d, \mathbf{F}_q)$ zie [12] hoofdstuk 4, "The symplectic group". Op de bij $V(d, \mathbf{F})$ behorende projectieve ruimte $PG(d-1, \mathbf{F})$ induceert de symplectische vorm (,) een zogenaamde *nulpolariteit*. Elk projectief punt ligt in zijn poolhypervlak. Elke projectieve rechte heeft een pooldeelruimte van dimensie $d-3$ (de doorsnede van de poolhypervlakken van twee van zijn punten); de projectieve rechte ligt in zijn pooldeelruimte wanneer het corresponderende vlak in $V(d, \mathbf{F})$ totaal isotroop is.
In $PG(3, \mathbf{F})$ is de standaard vorm

$$(x, y) = x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3.$$

Elk projectief punt $\langle p\rangle$ ligt in zijn poolvlak

$$\langle p\rangle^\perp = \{\langle x\rangle \in PG(2, \mathbf{F}) \,|\, (x, p) = 0\}.$$

In $PG(3, \mathbf{F})$ zijn de maximale totaal isotrope deelruimten projectieve rechten, namelijk de projectieve rechten door $\langle p\rangle$ in het projectieve vlak $\langle p\rangle^\perp$, voor elke $\langle p\rangle \in PG(3, \mathbf{F})$; in $PG(3, q)$ zijn er $q^3 + q^2 + q = 1$ totaal isotrope rechten. Men spreekt van een *lineair complex* van rechten. $PG(2m-1, q)$ bevat totaal isotrope deelruimten van dimensie $m-1$.
De *projectieve symplectische* groep $PSp(V)$ is de actie van $Sp(V)$ op de projectieve ruimte $\mathcal{P}(V)$. Op de verzameling $\mathcal{P}$ der punten van $\mathcal{P}(V)$ werkt $PSp(V)$ transitief. Inderdaad, de standaardvorm $\begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix}$ voor de symplectische vorm kan worden bereikt uitgaande van een willekeurige vector c. Voorts werkt $PSp(V)$ transitief op de paren projectieve punten $\langle c\rangle$, $\langle d\rangle$ met $(c, d) = 0$, en ook op de paren met $(c, d) \neq 0$. Inderdaad in beide gevallen kan de standaardvorm bereikt worden uitgaande van $\langle c\rangle$ and $\langle d\rangle$.
Op $\mathcal{P} \times \mathcal{P}$ heeft $PSp(V)$ dus drie banan:

$$\mathcal{P} \times \mathcal{P} = \mathrm{Diag} \cup \{(P, Q) \in \mathcal{P}^2 \,|\, P \perp Q\} \cup \{(P, Q) \,|\, P \not\perp Q\}.$$

De niet-triviale relaties definieren een paar van complementaire grafen, genaamd *rang 3 grafen*. Deze grafen zijn sterk regulier.

Opgave 10 Definieer de graaf Γ als volgt. De punten van Γ zijn de projectieve punten van $PG(2m-1, q)$. Twee punten $\langle p\rangle$ en $\langle q\rangle$ zijn verbonden wanneer zij symplectisch polair zijn, dus als $(p, q) = 0$. Bewijs dat Γ sterk regulier is en bepaal de parameters.

4.3 Orthogonale meetkunde, char $\mathbf{F} \neq 2$.

Een *kwadratische vorm* op $V(d, \mathbf{F})$ is een afbeelding $Q : V \to \mathbf{F}$ zodat

Q1: $Q(\alpha x) = \alpha^2 Q(x),\ \alpha \in \mathbf{F},\ x \in V$;

Q2: $Q(x + y) - Q(x) - Q(y)$ is een bilineaire vorm op V

Noem de bilineaire vorm (x, y) dan geldt

$$(x,y) = (y,x),\ (x,x) = 2Q(x),\ x, y \in V.$$

Neem aan dat char $\mathbf{F} \neq 2$, dan kunnen de kwadratische en de symmetrische bilineaire vorm uit elkaar worden afgeleid. We hebben dan een *orthogonale meetkunde*.

OPMERKING. Voor char $\mathbf{F} = 2$ is de bilineaire vorm alternerend, en behoort bij elke bilineaire vorm een semi-lineaire familie van kwadratische vormen; wij komen hierop terug in **??**.

Zij (V, Q) een vectorruimte voorzien van een kwadratische vorm die niet ontaard is (i.e. waarvan de bilineaire vorm niet ontaard is.) Wij leiden twee standaardgedaanten af voor Q.
Kies $c_1 \in V$, $Q(c_1) \neq 0$. Dan is $\langle c_1 \rangle^\perp$ niet ontaard, dus bevat een vector c_2 met $Q(c_2) \neq 0$. Herhaal dit proces, en vind een orthogonale basis van niet-isotrope vectoren. Ten opzichte van deze basis geldt

$$Q(x) = \sum_{i=1}^{d} \lambda_i x_i^2,\ (x,y) = 2\sum_{i=1}^{d} \lambda_i x_i y_i,\ \lambda_i = Q(c_i).$$

In termen van symmetrische matrices komt dit neer op diagonaliseren. Het hangt af van $\mathbf{F}$ hoe $Q(x)$ verder te reduceren. Over $\mathbf{R}$ kan de volgende vorm worden bereikt, waarin $2p - d$ de *signatuur* van Q heet:

$$Q(x) = \sum_{i=1}^{p} x_i^2 - \sum_{i=p+1}^{d} x_i^2.$$

Over $\mathbf{C}$ kan een som van d kwadraten worden bereikt.
Hoewel V niet-ontaard is, kunnen totaal isotrope deelruimten U voorkomen. Een vector c, en dus ook $\langle c \rangle$, is ofwel totaal isotroop ofwel niet-isotroop. Voor een 2-dimensionale deelruimte U zijn de mogelijkheden: niet-isotroop, totaal isotroop, isotroop en ontaard, isotroop en niet-ontaard. In het laatste geval, noem *hyperbolisch*, kan een basis worden gevonden met matrix $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. Inderdaad, zij $U = \langle c, a \rangle$. Neem c isotroop, dan $(c, a) \neq 0$. Kies $d = \lambda a + \mu c$ zodat

$$\lambda = 1/(c,a),\ \mu = -(a,a)/2(a,c)^2,$$

dan voldoen c en d.
Zij (V, Q) een niet-ontaarde orthogonale ruimte. Kies een isotrope vector en vorm een hyperbolisch vlak H_1 en vorm een hyperbolisch vlak H_2 loodrecht op H_1. Pas dit proces toe totdat er geen isotrope punten meer zijn. De corresponderende basis heeft de Gram matrix

$$\begin{bmatrix} O & I & O \\ I & O & O \\ O & O & G \end{bmatrix}$$

Wanneer r de dimensie is van een maximale totaal isotrope deelruimte, dan geldt

$$V = H_1 \perp H_2 \perp \ldots \perp H_r \perp W,$$

waarin H_i hyperbolische vlakken zijn en W een niet-isotrope deelruimte is (zie [12], 3.30 en 3.34).
Ook voor orthogonale ruimten geldt de stelling van Witt ([12], 3.32) en zijn de dimensies van de maximale totaal isotrope deelruimten dezelfde.
Wanneer $\mathbf{F} = GF(q)$, q oneven, dan kunnen wij méér zeggen. Zij γ een niet-kwadraat in $\mathbf{F}$. Een niet-ontaard vlak U in V is ofwel niet-isotroop (zet $\varepsilon = -$), ofwel hyperbolisch (zet $\varepsilon = +$). In beide gevallen is het aantal niet-isotrope vectoren $(q-\varepsilon)(q-1)$. De gram matrices van geschikte bases van U zijn

$$\begin{bmatrix} 1 & 0 \\ 0 & -\gamma \end{bmatrix}, \quad \text{resp.} \quad \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

corresponderend met de kwadratische vormen

$$Q(x) = x_1^2 - \gamma x_2^2, \quad \text{resp.} \quad Q(x) = x_1^2 - x_2^2.$$

Nu weten wij, wegens stelling **, dat elke V van dimensie > 2 een isotrope vector $\neq 0$ bevat. Als gevolg hiervan bestaan slechts de volgende gevallen voor niet-ontaarde orthogonale meetkunden $(V(d, \mathbf{F}), Q)$:

d oneven: $V = H_1 \perp \ldots \perp H_{(d-1)/2} \perp \langle a \rangle, Q(a) = 1$ of γ,

d even, $\varepsilon = +$: $V = H_1 \perp \ldots \perp H_{d/2}$,

d even, $\varepsilon = -$: $V = H_1 \perp \ldots \perp H_{(d-2)/2} \perp W$, waarin W een niet-isotroop vlak is.

De kwadratische vormen kunnen dus in de volgende standaardvorm worden gebracht:

d oneven: $Q(x) = 2(x_1x_2 + \cdots + x_{d-2}x_{d-1}) + x_d^2(1 \text{ of } \gamma)$

d even, $\varepsilon = +$: $Q(x) = 2(x_1x_2 + \cdots + x_{d-1}x_d)$,

d even, $\varepsilon = -$: $Q(x) = 2(x_1x_2 + \cdots + x_{d-3}x_{d-2}) + x_{d-1}^2 - \gamma x_d^2$.

De *index* van V, dat is de maximale dimensie van totaal isotrope deelruimte van V, is respectievelijk

$$\frac{1}{2}(d-1), \quad \frac{1}{2}d, \quad \frac{1}{2}(d-2).$$

Zij $\phi(d)$ het aantal isotrope vectoren $\neq 0$ in $(V(d), Q)$.

Stelling 4.3 *$\phi(d) = (q^{d/2} - \varepsilon)(q^{(d/2)-1} + \varepsilon)$ voor d even,
$\phi(d) = q^{d-1} - 1$ voor d oneven.*

Bewijs. Elk der bovenstaande gevallen is van de vorm

$$V(d) = H_1 \perp V(d-2) = \langle a, b\rangle \perp V(d-2),$$

met hyperbolische $\langle a, b\rangle$ en $V(d-2)$ van hetzelfde type als $V(d)$. De gevraagde $\phi(d)$ is het aantal vectoren $\alpha a + \beta b + v \neq 0$ zodat $\alpha, \beta \in \mathbf{F}$, $v \in V(d-2)$, $0 = Q(\alpha a + \beta b + v) = \alpha\beta + Q(v)$.
Als $\beta = 0$, $v = 0$, dan is er één zo'n vector voor elke $\alpha \neq 0$. Als $\beta = 0$, $v \neq 0$, dan zijn er $\phi(d-2)$ zulke vectoren voor elke α. Voor elke $\beta \neq 0$ zijn er q^{d-2} zulke vectoren, omdat voor elke $v \in V(d-2)$ een unieke α bestaat zodat $\alpha\beta + Q(v) = 0$. Dus

$$\begin{aligned} \phi(d) &= q - 1 + q\phi(d-2) + (q-1)q^{d-2}, \\ \phi(d) &- q^{d-1} + 1 = q(\phi(d-2) - q^{d-3} + 1). \end{aligned}$$

□

De beginwaarden $\phi(1) = 0$ en $\phi(2) = (q-1)(1+\varepsilon)$ leiden tot het gestelde.
Een niet-ontaarde *kwadriek* in $PG(d-1, q)$ wordt gedefinieerd door

$$\{\langle x\rangle \in \mathcal{P} \mid Q(x) = 0\}.$$

Als de dimensie van $PG(d-1, q)$ *even* is, dan is er één type kwadriek; deze bevat maximale projectieve deelruimten van dimensie $(d-3)/2$. Als de dimensie van $PG(d-1, q)$ *oneven* is, dan zijn er twee typen kwadrieken: de *hyperbolische* kwadrieken, van index $d/2$, die maximale projectieve deelruimten van dimensie $(d-2)/2$ bevatten, en de *elliptische* kwadrieken, van index $(d-2)/2$, die maximale projectieve deelruimten van dimensie $(d-4)/2$ bevatten.

Voorbeeld. $PG(3, q)$ heeft hyperboloiden met rechten, en ellipsoiden zonder rechten. $PG(5, q)$ heeft hyperbolische kwadrieken met vlakken, en elliptische kwadrieken met slechts rechten. $PG(4, q)$ en de Desarguese $PG(2, q)$ hebben één type kwadriek, met resp. zonder projectieve rechten.

Als gevolg van de bovenstaande stelling hebben kwadrieken in $PG(d-1, q)$ de volgende aantallen punten:

$d-1$	hyp., $\varepsilon = +$	ell., $\varepsilon = -$	kwadriek
2			$q+1$
3	$(q+1)^2$	q^2+1	
4			q^3+q^2+q+1
5	$(q^2+1)(q^2+q+1)$	$(q^3+1)(q+1)$	
even			$(q^d-1)/(q-1)$
oneven	$\dfrac{(q^{d/2}-\varepsilon)(q^{(d/2)-1}+\varepsilon)}{q-1}$		

Beschouw in $PG(d-1, q)$ een kwadriek Q, een punt $\langle a\rangle$ en zijn poolvlak ten opzichte van Q:

$$\langle a\rangle^{\perp} = \{\langle x\rangle\} \mid (x, a) = 0\}.$$

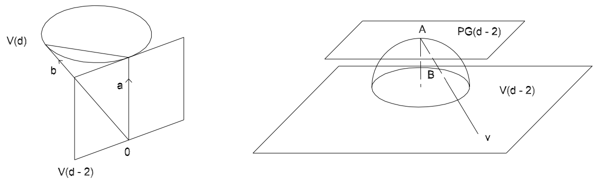
Wanneer $\langle a \rangle \notin Q$, dan is zijn poolvlak een $PG(d-2,q)$ die Q snijdt in een niet-ontaarde kwadriek van een dimensie lager. Het hangt af van de pariteit van d welke gevallen zich voordoen.
Het poolvlak van $\langle a \rangle \in Q$ heet het *raakvlak* in $\langle a \rangle$ aan Q. Wij geven een projectieve interpretatie van de formule

$$\frac{\phi(d)}{q-1} = 1 + q^{d-2} + q\frac{\phi(d-2)}{q-1}.$$

Het linkerlid is het aantal punten van Q. De 1 slaat op $\langle a \rangle \in Q$. De kwadriek Q bevat q^{d-2} punten die *niet* in het raakvlak liggen. Dat kan men ook als volgt inzien. In $V(d,q)$ vormen de vlakken door a (resp. in $PG(d-1,q)$ vormen de lijnen door $\langle a \rangle$) een

$$PG(d-2,q) = PG(d-3,q) \cup AG(d-2,q),$$

en q^{d-2} is het aantal punten van $AG(d-2,q)$.



Figuur 4.1:

Het raakvlak in $\langle a \rangle \in Q$ snijdt de kwadriek Q in een kegel met top $\langle a \rangle$. Voor elke α hebben wij in $V(d-2)$ een kegel van isotrope vectoren, wegens

$$Q(\alpha a + v) = Q(v), \quad v \in V(d-2).$$

De restrictie van de kwadratische vorm $Q(x)$ tot $V(d-2)$ geeft in de bijbehorende $PG(d-3,q$ een kwadriek die $\phi(d-2)/(q-1)$ punten bevat.
De *orthogonale groep* $\mathcal{O}(V)$ is de groep der isometrieen van (V,Q) op zichzelf, dat is,

$$\mathcal{O}(V) = \{\sigma \in GL(V) \mid \forall x \in V\ :\ (Q(x^\sigma) = Q(x))\}.$$

In termen van matrices bestaat $\mathcal{O}(V)$ uit alle A met $AEA^t = E$, waarin E de matrix van de Q behorende bilineare vorm is.

De *projectieve orthogonale* groep $P\mathcal{O}(V)$ is de actie van $\mathcal{O}(V)$ op de projectieve ruimte $\mathcal{P}(V)$. Op de punten van de bij de kwadratische vorm Q behorende kwadriek Ω werkt $P\mathcal{O}(V)$ transitief. Inderdaad, de standaardvorm

$$\begin{bmatrix} O & I & O \\ I & O & O \\ O & O & G \end{bmatrix}$$

voor de bilineaire vorm kan worden bereikt uitgaande van een willekeurige isotrope vector c. Voorts werkt $P\mathcal{O}(V)$ transitief op de paren isotrope projectieve punten $\langle c\rangle$, $\langle d\rangle$ met $(c,d)=0$, en ook op de paren met $(c,d)\neq 0$. Daarom werkt $P\mathcal{O}(V)$ op Ω als een rang 3 groep; $P\mathcal{O}(V)$ definieert op de punten van Ω een paar van complementaire rang 3 grafen. Deze grafen zijn sterk regulier.
Voor deze en verdere bijzonderheden betreffende de structuur en de orde van $\mathcal{O}(V)$ en $P\mathcal{O}(V)$ verwijzen wij naar [2] chapter 5, [6] 1.4 en [12] chapter 6: "orthogonal groups, char $\mathbf{F}\neq 2$".

Opgave 11 De graaf Γ wordt als volgt gedefinieerd. De punten van Γ zijn de punten van de kwadriek Ω in $PG(d-1,q)$. Twee punten $\langle p\rangle$ en $\langle q\rangle$ zijn verbonden wanneer hun verbindingslijn op de kwadriek ligt. Bewijs dat Γ sterk regulier is, en bepaal de parameters (er zijn 3 gevallen!).

4.4 Unitaire meetkunde.

Eerst enige opmerkingen over het "complexe" vlak $GF(q^2)$. Zij ξ een primitief element, dan

$$GF(q^2)=\{0,\xi,\xi^2,\ldots,\xi^{q^2-1}=1\}.$$

De *conjugatie* $-$, gedefinieerd door

$$\forall z\in GF(q^2)\ :\ (\bar z := z^q)$$

is een van de identiteit verschillend automorfisme van $GF(q^2)$ (ga na!). De zelfgeconjugeerde elementen $z=\bar z$ zijn

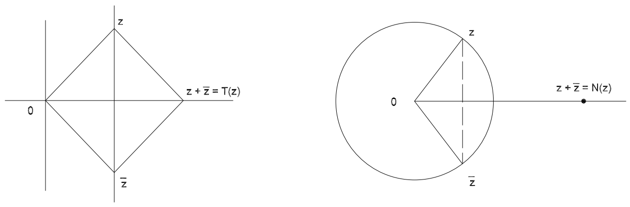
$$\{0,\xi^{q+1},\xi^{2(q+1)},\ldots,\xi^{(q-1)(q+1)}\};$$

deze elementen vormen een deellichaam $GF(q)$. Definieer twee functies $T=$ trace en $N=$ norm door

$$T(z):=z+\bar z,\quad N(z):=z\,\bar z.$$

De trace is een $(q,1)$ afbeelding van $GF(q^2)$ op $GF(q)$. De norm is een $(q+1,1)$ afbeelding van $GF(q^2)\setminus\{0\}$ op $GF(q)\setminus\{0\}$ (ga na!). Een gevolg hiervan is dat bij elke $r\in GF(q)\setminus\{0\}$ er $q+1$ elementen $z\in GF(q^2)$ bestaan zodat $z\,\bar z=r$. Als $T(z)=0$ voor $z\in GF(q^2)\setminus\{0\}$, dan is

$$z^{q-1}=-1,\quad z^{(q^2-1)/2}=(-1)^{(q+1)/2},$$



Figuur 4.2:

dus z is een kwadraat voor $q = -1 \pmod 4$ en een niet-kwadraat voor $q = 1 \pmod 4$.

Opgave 12 Toon aan dat de vergelijking

$$z\bar{z} + \bar{\alpha}z + \alpha\bar{z} = 0, \quad \alpha \in GF(q^2)$$

q oplossingen $z \neq 0$ heeft.

Opgave 13 Toon aan dat de vergelijking

$$\bar{\alpha}z + \alpha\bar{z} + \beta\bar{\beta} = 0, \quad \alpha, \beta \in GF(q^2)$$

q oplossingen z heeft.

Een *unitaire ruimte* is een vectorruimte $V(d, \mathbf{F})$ voorzien van een niet-ontaarde Hermite-vorm, dat is, een niet-ontaarde sesquilineaire vorm (x, y) met

$$- \neq \text{id}, \quad \forall x, y \in V \;:\; ((y, x) = \overline{(x, y)}).$$

Zij $\mathbf{F}_0$ het deellichaam der zelfgeconjugeerde elementen van $\mathbf{F}$, dan geldt

$$\forall x \in V \;:\; ((x, x) \in \mathbf{F}_0).$$

Ten opzichte van een orthogonale basis geldt

$$(x, y) = \lambda_1 x_1 \bar{y}_1 + \ldots + \lambda_d x_d \bar{y}_d, \quad 0 \neq \lambda_i \in \mathbf{F}_0.$$

Voor eindige $\mathbf{F}_{q^2}$ kunnen wij bereiken

$$(x, y) = x_1 \bar{y}_1 + \ldots + x_d \bar{y}_d,$$

omdat bij elke $\lambda \in \mathbf{F}_q$ bestaan $\zeta \in \mathbf{F}_{q^2}$ zodat $\zeta\bar{\zeta} = \lambda$. De laatste eigenschap heeft ook ten gevolge dat elke $V(d, \mathbf{F}_{q^2})$ van dimensie ≥ 2 isotroop is. Inderdaad, voor $x \in v$, $y \in V$ met $(x,x) = (y,y) = 1$, $(x,y) = 0$ geldt

$$(x + \zeta y, x + \zeta y) = 1 + \zeta\bar{\zeta},$$

hetgeen nul is voor geschikte $\zeta \in GF(q^2)$. Dit voert tot de volgende standaard vormen, in termen van hyperbolische vlakken H_i en niet-isotrope p:

d even: $\quad V = H_1 \perp \ldots \perp H_{d/2}$,
d oneven: $\quad V = H_1 \perp \ldots \perp H_{(d-1)/2} \perp \langle p \rangle$.

Zij $\phi(d)$ het aantal isotrope vectoren $\neq 0$ in de unitaire ruimte $V(d)$ over $GF(q^2)$.

Stelling 4.4 $\phi(d) = (q^d - (-1)^d)(q^{d-1} - (-1)^{d-1})$.

BEWIJS. Schrijf, met hyperbolische $\langle a, b \rangle$,

$$V(d) = H_1 \perp V(d-2) = \langle a, b \rangle \perp V(d-2).$$

De gevraagde $\phi(d)$ is het aantal vectoren $\alpha a + \beta b + v \neq 0$, zodat $\alpha, \beta \in \mathbf{F}_{q^2}$, $v \in V(d-2)$,

$$0 = (\alpha a + \beta b + v, \alpha a + \beta b + v) = \alpha\bar{\beta} + \beta\bar{\alpha} + (v,v).$$

Als $\beta = 0$, $v = 0$, dan is er één zo'n vector voor elke $\alpha \neq 0$. Als $\beta = 0$, $v \neq 0$, dan zijn er $\phi(d-2)$ zulke vectoren voor elke α. Voor elke $\beta \neq 0$, zijn er q^{2d-3} zulke vectoren; inderdaad, voor elke $v \in V(d-2)$ zijn er precies q waarden α in $\mathbf{F}_{q^2}$ zodat $\alpha\bar{\beta} + \beta\bar{\alpha} + (v,v) = 0$. Dus

$$\phi(d) = q^2 - 1 + q^2\phi(d-2) + (q^2-1)q^{2d-4}q,$$
$$\phi(d) - q^{2d-1} + 1 = q^2(\phi(d-2) - q^{2d-5} + 1).$$

De beginwaarden $\phi(1) = \phi(0) = 0$ leiden tot het gestelde. □

Een *Hermite oppervlak* in $PG(d-1, q^2)$ wordt gedefinieerd door

$$\Omega_{d-1} := \left\{ \langle x \rangle \in PG(d-1, q^2) \,|\, (x,x) = 0 \right\}.$$

Ten opzichte van een orthonormale basis in $V(d, q^2)$ is de vergelijking van Ω_{d-1}

$$x_1^{q+1} + x_2^{q+1} + \cdots + x_d^{q+1} = 0.$$

Opgave 14 Bepaal de projectieve punten van de Hermite-kromme

$$\Omega_2 := x_1^3 + x_2^3 + x_3^3 = 0$$

in $PG(2, 4)$.

Op grond van de bovenstaande stelling bedraagt het aantal projectieve punten van Ω_{d-1}

$$|\Omega_{d-1}| = \frac{(q^d - (-1)^d)(q^{d-1} - (-1)^{d-1})}{q^2 - 1}.$$

In $PG(3, q^2)$ heeft het Hermite oppervlak $(q^2+1)(q^3+1)$ punten. In $PG(2, q^2)$ heeft de Hermite kromme q^3+1 punten. In $PG(1, q^2)$ heeft de Hermite verzameling $q+1$ punten.
Beschouw een punt $\langle p \rangle \in \Omega_{d-1} \subset PG(d-1, q^2)$, het *raakvlak* in $\langle p \rangle$ aan Ω_{d-1} is het poolvlak

$$\langle p \rangle^{\perp} = \left\{ \langle x \rangle \in PG(d-1, q^2) \,|\, (x, p) = 0 \right\}.$$

De lijnen door $\langle p \rangle$ in het raakvlak vormen de punten van een projectieve ruimte $PG(d-3, q^2)$, waarop $(\ ,\ )$ een Hermite vorm induceert. Inderdaad, voor $\langle x \rangle$, $\langle x' \rangle \in \langle p \rangle^{\perp}$ voldoen $y = x - \lambda p$ en $y' = x' - \mu p$ aan

$$(y, y') = (x - \lambda p, x' - \mu p) = (x, x').$$

Als $\langle x \rangle \in \Omega_{d-1} \cap \langle p \rangle^{\perp}$, dan ook $\langle x - \lambda p \rangle \in \Omega_{d-1} \cap \langle p \rangle^{\perp}$ voor elke $\lambda \in GF(q^2)$.

Lemma *Elke lijn van $PG(d-1, q^2)$ door $\langle p \rangle \in \Omega_{d-1}$, die niet ligt in $\langle p \rangle^{\perp}$, bevat nog precies q andere punten van Ω_{d-1}.*

BEWIJS. Geef de lijn aan door $\langle p + \lambda a \rangle$ met $(p, a) \neq 0$, dan geldt voor de snijpunten van de lijn met Ω_{d-1}

$$0 = (p + \lambda a, p + \lambda a) = \lambda \bar{\lambda}(a, a) + \lambda(a, p) + \bar{\lambda}(p, a).$$

In het complexe λ-vlak is dit een cirkel. Er zijn q oplossingen $\lambda \neq 0$, die q snijpunten $\neq \langle p \rangle$ opleveren. □

Wij geven een projectieve interpretatie van de formule

$$\frac{\phi(d)}{q^2 - 1} = 1 + q^2 \frac{\phi(d-2)}{q^2 - 1} + q \cdot q^{2(d-2)}.$$

De punten van Ω_{d-1} worden geteld door één punt $\langle p \rangle \in \Omega_{d-1}$, de punten $\neq \langle p \rangle$ van $\Omega_{d-1} \cap \langle p \rangle^{\perp}$ (in het raakvlak) en de punten van Ω_{d-1} niet in het raakvlak. Elk punt van Ω_{d-3}, in de boven beschreven $PG(d-3, q^2)$ levert q^2 punten van Ω_{d-1}. Elke projectieve lijn door $\langle p \rangle$ en niet in $\langle p \rangle^{\perp}$ levert q punten van Ω_{d-1}; het aantal van zulke lijnen bedraagt

$$\frac{(q^2)^{d-1} - 1}{q^2 - 1} - \frac{(q^2)^{d-2} - 1}{q^2 - 1} = q^{2d-4}.$$

Hiermee is een projectieve interpretatie van de formule verkregen.

Opgave 15 In $PG(3, 4)$ is het Hermite oppervlak een kubisch oppervlak. Toon aan dat het oppervlak 45 punten bevat, 3 lijnen per punt, 5 punten per lijn, en 27 lijnen.

Opgave 16 Toon aan dat in $PG(2, q^2)$ de punten van Ω_2 en de snijlijnen van Ω_2 (in de zin van het lemma) een $2-(q^3+1, q+1, 1)$ design vormen. Dit design heet een *unital*.

De *unitaire groep* $U(V)$ is de groep der isometrieen ten opzichte van de Hermite vorm:

$$U(V) := \{\sigma \in GL(V) \,|\, \forall x, y \in V \,:\, ((x^\sigma, y^\sigma) = (x, y))\}\,.$$

Voor de structuur van de unitaire groep, zie [12], Chapter 5, "The unitary group". Weer geldt de stelling van Witt ([12], 5.32).
De *projectieve unitaire groep* $PU(d, q^2)$ is de actie van de unitaire groep op de punten van $PG(d-1, q^2)$. Deze actie is natuurlijk niet transitief omdat een niet-isotroop punt niet in een isotroop punt kan worden overgevoerd. $PU(d, q^2)$ werkt wel transitief op de punten van het Hermite-oppervlak Ω_{d-1}, op de paren loodrechte punten van Ω_{d-1} en op de paren niet-loodrechte punten van Ω_{d-1}. Dit volgt uit de boven afgeleide standaardvorm voor Ω_{d-1}. Dit betekent dat $PU(d, q^2)$ als een rang 3 groep werkt op de punten van Ω_{d-1}.

Opgave 17 Bepaal de parameters van de hierdoor gedefinieerde sterk reguliere graaf.

Op de punten van $PG(d-1, q^2) \setminus \Omega_{d-1}$ werkt $PU(d, q^2)$ eveneens transitief. Het aantal van deze punten is

$$u_{d-1} := |PG(d-1, q^2)| - |\Omega_{d-1}| = \frac{q^{d-1}(q^d + (-1)^{d-1})}{q+1}.$$

Noem twee punten $\langle c\rangle \neq \langle d\rangle\Omega_{d-1}$ verbonden als $(c, d) = 0$. dan ontstaat er een transitieve graaf met de parameters

$$n = u_{d-1}, \quad k = u_{d-2}, \quad \lambda = u_{d-3},$$

maar de μ hoeft niet constant te zijn. Voor $q = 2$ geldt echter $\mu = 4u_{d-4}$ en is de graaf sterk regulier.

VOORBEELD. Op de punten van $PG(3, 4) \setminus \Omega_3$ definieeert loodrechtheid een sterk reguliere graaf met $(n, k, \lambda, \mu) = (40, 12, 2, 4)$.

4.5 Orthogonale meetkunde, char $\mathbf{F} = 2$.

Een lichaam $\mathbf{F}$ met char $\mathbf{F} = p$ heet *perfect* wanneer $\mathbf{F}^p \simeq \mathbf{F}$. Een eindig lichaam met karakteristiek 2 is perfect wegens

$$(\alpha + \beta)^2 = \alpha^2 + \beta^2, \quad (\alpha\beta)^2 = \alpha^2\beta^2, \quad -1 = 1.$$

Wij onderzoeken de meetkunde van $V(d, \mathbf{F})$ en $PG(d-1, \mathbf{F})$ met eindige $\mathbf{F}$ en char $\mathbf{F} = 2$, eerst met een symmetrische bilineaire vorm (II blz. *), daarna met de kwadratische vormen behorend bij een alternerende bilineaire vorm (I blz. *).

Zij f een niet-ontaarde symmetrische bilineaire vorm voor V. Dan bezit V een basis die orthonormaal is t.o.v. f. Inderdaad, volgens de definitie en perfectie is er een e_1 zodat $f(e_1, e_1) = 1$. Stel dat de restrictie van f tot $\langle e_1 \rangle^\perp$ alternerend is, dan zijn er $e_2, e_3 \in V$ zodat

$$[f(e_i, e_j)] = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

Dan vormen $e_1+e_2+e_3$, e_1+e_2, e_1+e_3 een orthonormale basis voor $\langle e_1, e_2, e_3 \rangle$. Gebruik verder inductie. Ten opzichte van de orthonormale basis geldt

$$f(x, y) = x_1y_1 + x_2y_2 + \cdots + x_dy_d.$$

De isotrope punten voldoen aan

$$0 = f(x, x) = x_1^2 + x_2^2 + \cdots + x_d^2 = (x_1 + x + 2 + \cdots + x_d)^2,$$

dus zijn de punten van een hypervlak.
We wenden ons tot de meer interessante verfijning van de symplectische meetkunde, genaamd de *orthogonale meetkunde char* $\mathbf{F} = 2$, die ontstaat door beschouwing van kwadratische vormen. Deze worden gedefinieerd door

$$Q(\lambda x + \mu y) = \lambda^2 Q(x) + \lambda\mu(x, y) + \mu^2 Q(y),$$

waarin (x, y) een alternerende bilineaire vorm is.
Zij $V(2m, \mathbf{F})$ een niet-ontaarde symplectische ruimte met alternerende bilineaire vorm (,). Hierbij behoort een semi-lineaire familie van kwadratische vormen. Inderdaad als $Q(x)$ een kwadratische vorm is bij (,), dan ook $Q(x)+L(x)$, met $L(x)$ semi-lineair t.o.v. het Frobenius-automorfisme $\lambda \mapsto \lambda^2$. Ontbind $V(2m, \mathbf{F})$ volgens (,) in hyperbolische vlakken

$$V = H_1 \perp H_2 \perp \ldots \perp H_m.$$

Voor $z = z_1 + z_2 + \ldots + z_m$ met $z_i \in H_i$ geldt

$$Q(z) = Q(z_1) + Q(z_2) + \ldots + Q(z_m)$$

Wij onderzoeken eerst het gedrag van Q op een hyperbolisch vlak H. Zij u, v een symplectische basis voor H, dus zij

$$\begin{bmatrix} (u,u) & (u,v) \\ (v,u) & (v,v) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Zij $Q(u) = \alpha$, $Q(v) = \beta$, dan geldt

$$Q(\xi_1 u + \xi_2 v) = \alpha\xi_2^2 + \xi_1\xi_2 + \beta\xi_2^2.$$

Als $\alpha = 0$ dan kan $\beta = 0$ worden gemaakt door v te vervangen door $v' = v + \beta u$, omdat

$$(u, v') = 1, \quad Q(v') = Q(v) + \beta + 0 = \beta + \beta = 0.$$

Als $\alpha\beta \neq 0$ dan kan $\alpha = 1$ worden gemaakt door

$$u' = u/\sqrt{\alpha}, \quad v' = v\sqrt{\alpha}.$$

Er blijft dus

$$\begin{array}{ll} Q(\xi_1 u + \xi_2 v) = \xi_1\xi_2, & \text{noem } \textit{type A} \\ Q(\xi_1 u + \xi_2 v) = \xi_1^2 + \xi_1\xi_2 + \beta\xi_2^2, & \text{noem } \textit{type B} \end{array}$$

Beschouw nu $V(4, \mathbf{F}) = B \perp B$, dat is $V = \langle u_1, v_1, u_2, v_2\rangle$ met $(u_1, v_1) = (u_2, v_2) = 1$, overige $(\, , \,) = 0$,

$$Q(u_1) = Q(u_2) = 1, \quad Q(v_1) = \beta_1, \quad , Q(v_2) = \beta_2.$$

Neem als nieuwe basis $\langle u_1 + u_2, v_2\rangle$ en $\langle u_1, v_1 + v_2\rangle$, dan

$$Q(u_1 + u_2) = 0, \; Q(v_2) = \beta_2, \; Q(u_1) = 1, \; Q(v_1 + v_2) = \beta_1 + \beta_2,$$

en wij kunnen bereiken

$$V(4, \mathbf{F}) = A \perp (B \text{ of } A).$$

Door iteratie vinden wij

$$\begin{array}{rcl} V(2m, \mathbf{F}) & = & A \perp A \perp \ldots \perp A \quad \text{of} \\ V(2m, \mathbf{F}) & = & B \perp A \perp \ldots \perp A. \end{array}$$

De bijbehorende kwadratische vormen zijn

$$\begin{array}{rcl} Q^+(x) & := & \xi_1\xi_2 + \xi_3\xi_4 + \ldots \xi_{2m-1}\xi_{2m}, \\ Q^\beta(x) & := & \xi^2 + \xi_1\xi_2 + \beta\xi_2^2 + \xi_3\xi_4 + \ldots + \xi_{2m-1}\xi_{2m}. \end{array}$$

Opmerking. β modulo $\{k^2 + k \,|\, k \in \mathbf{F}\}$ is de *Arf invariant* van Q, zie [16], 1.12. In het geval $\mathbf{F} = \mathbf{F}_2$ is $\beta \in \{0, 1\}$.

Stelling 4.5 *$V(2m, \mathbf{F}_2$ heeft twee soorten kwadratische vormen namelijk*

$$\begin{array}{rcl} Q^+(x) & := & \xi_1\xi_2 + \xi_3\xi_4 + \ldots \xi_{2m-1}\xi_{2m}, \\ Q^-(x) & := & \xi^2 + \xi_1\xi_2 + \xi_2^2 + \xi_3\xi_4 + \ldots + \xi_{2m-1}\xi_{2m}. \end{array}$$

$Q^\varepsilon(x)$ heeft $2^{2m-1} + \varepsilon.2^{m-1}$ nulpunten, $\varepsilon \in \{+, -\}$.

Bewijs. De gedaante van $Q^\varepsilon(x)$ volgt uit het bovenstaande. Voor het tellen van het aantal nulpunten van $Q^+(x)$ en dat van $Q^-(x)$ merken wij eerst op dat deze aantallen de som 2^{2m} hebben. Inderdaad,

$$Q^-(x + e) = 1 + Q^+(x), \quad \text{voor } \; e = (1, 1, 0, \ldots, 0),$$

en voor alle $x \in V(2m, \mathbf{F}_2)$. Nu bestaat $A \perp A \perp \ldots \perp A$ uit de vectoren $x + y$ met $x \in X$, $y \in Y$, waarin X en Y m-dimensionale deelruimten van $V(2m, \mathbf{F}_2)$ zijn waarop Q^+ nul is. Het aantal vectoren $x + y$ met $Q^+(x + y) = (x, y) = 0$ bedraagt $2^m + (2^m - 1)2^{m-1}$, namelijk 2^m voor $x = 0$, en 2^{m-1} voor elke $x \neq 0$.

□

De verzameling $V(2m, \mathbf{F}_2) \setminus \{0\}$ kan worden beschouwd als de verzameling $\mathcal{P}$ der projectieve punten van $PG(2m-1, \mathbf{F}_2)$. In $\mathcal{P}$ definieren wij de *kwadrieken*

$$\Omega^\varepsilon := \{x \in \mathcal{P} \,|\, Q^\varepsilon(x) = 0\}, \quad \varepsilon \in \{+, -\}.$$

Volgens de stelling geldt (vgl. $\phi(d)$ uit 4.3)

$$|\Omega^\varepsilon| = 2^{2m-1} + \varepsilon.2^{m-1} - 1 = (2^m - \varepsilon)(2^{m-1} + \varepsilon).$$

De *symplectische groep* $Sp(2m, \mathbf{F}_2)$ is de groep der isometrieen t.o.v. $(\ ,\ )$ van V op zichzelf. De *orthogonale groep* $O^\varepsilon(2m, \mathbf{F}_2)$ is de groep der isometrieen t.o.v. Q^ε van V op zichzelf. $Sp(2m, \mathbf{F}_2)$ werkt op $\mathcal{P}$ als een rang 3 groep: transitief op de punten, op de paren punten met $(x, y) = 0$ en op de paren punten met $(x, y) = 1$. $O^\varepsilon(2m, \mathbf{F}_2)$ werkt als een rang 3 groep op Ω^ε, en ook op $\mathcal{P} \setminus \Omega^\varepsilon$. Dit levert 5 series van sterk reguliere grafen, genaamd $S(2m, 2)$ op $\mathcal{P}$, $O^\varepsilon(2m, 2)$ op Ω^ε, en $N^\varepsilon(2m, 2)$ op $\mathcal{P} \setminus \Omega^\varepsilon$, waarin steeds x en y verbonden zijn wanneer $(x, y) = 0$. De parameters zijn als volgt (ga dit na!):

$$\begin{array}{rll}
S(2m,2): & n = 2^{2m} - 1, & k = 2^{2m-1} - 2, \\
& \lambda = 2^{2m-2} - 3 & \mu = 2^{2m-2} - 1; \\
O^\varepsilon(2m,2): & n = 2^{2m-1} + \varepsilon 2^{m-1} - 1, & k = 2^{2m-2} + \varepsilon 2^{m-1} - 2, \\
& \lambda = 2^{2m-3} + \varepsilon 2^{m-1} - 3\ , & \mu = 2^{2m-3} + \varepsilon 2^{m-2} - 1; \\
N^\varepsilon(2m,2): & n = 2^{2m-1} - \varepsilon 2^{m-1} & k = 2^{2m-2} - 1, \\
& \lambda = 2^{2m-3} - 2, & \mu = 2^{2m-3} + \varepsilon 2^{m-2}.
\end{array}$$

De grafen $S(2m, 2)$ op $\mathcal{P}$ en $O^\varepsilon(2m, 2)$ op Ω^ε hebben de volgende eigenschap.
Triangle property: bij elk paar verbonden punten u en v behoort een punt $f(u, v)$, verbonden met beide, zodat elk overig punt van de graaf verbonden is met één of drie van u, v, $f(u, v)$.
Inderdaad, $u + v$ voldoet als $f(u, v)$ omdat

$$\begin{aligned}
&(u + v, u) = (u + v, v) = (u, v) = 0, \\
&(u, x) + (v, x) + (u + v, x) = 0,
\end{aligned}$$

en (voor het geval $O^\varepsilon(2m, 2)$)

$$Q(u + v) = Q(u) + Q(v) + (u, v) = 0 + 0 + 0 = 0.$$

De grafen $S(2m, 2)$ op $\mathcal{P}$ en $N^\varepsilon(2m, 2)$ op $\mathcal{P} \setminus \Omega^\varepsilon$ hebben de volgende eigenschap.

Cotriangle property: bij elk niet-verbonden paar punten u en v behoort een punt $g(u, v)$, niet verbonden met beide, zodat elk overig punt van de graaf verbonden is met één of drie van u, v, $g(u, v)$.

Inderdaad, $u + v$ voldoet als $g(u, v)$ omdat

$$(u + v, u) = (u + v, v) = (u, v) = 1,$$
$$(u, x) + (v, x) + (u + v, x) = 0,$$

en (voor het geval $N^\varepsilon(2m, 2)$)

$$Q(u + v) = Q(u) + Q(v) + (u, v) = 1 + 1 + 1 = 1.$$

Opmerking. In essentie worden $S(2m, 2)$ en $O^\varepsilon(2m, 2)$ gekarakteriseerd door de triangle property. In essentie worden $S(2m, 2)$ en $N^\varepsilon(2m, 2)$ gekarakteriseerd door de cotriangle property (ook het complement van de triangulaire graaf $T(m)$ voldoet). Zie hierover [25, 26].

In het voorgaande hebben wij verondersteld dat $V(d, \mathbf{F})$ een niet-ontaarde symplectische ruimte is, dus dat $V^\perp = \{0\}$. Dit kan alleen als d even is. Wanneer V ontaard is, dan geldt $V \cap V^\perp \neq \{0\}$. De definitie van een kwadratische vorm

$$Q(\lambda x + \mu y) = \lambda^2 Q(x) + \mu^2 Q(y) + \lambda\mu(x, y)$$

geldt ook voor ontaarde alternerende bilineaire vormen (,). We noemen (V, Q) *niet-singulier* als

$$\forall 0 \neq x \in V^\perp : (Q(x) \neq 0),$$

en *singulier* als $Q(x) = 0$ op een deelruimte $\neq \{0\}$ van $V \cup V^\perp$. Een singuliere V is isotroop, maar niet omgekeerd (ga na).

Voorbeeld. In $V(2, \mathbf{F}_2)$ is de standaardvorm $x_1y_2 + x_2y_1$. Equivalent hiermee is

$$\begin{aligned} (x, y) &= x_1y_2 + x_2y_1 + x_1y_3 + x_3y_1 + x_2y_3 + x_3y_2, \\ V^\perp &= \{x \in V \mid \forall y \in V : ((x, y) = 0)\} = \langle(1, 1, 1)\rangle. \end{aligned}$$

De 8 bijbehorende kwadratische vormen zijn

$$Q(x) = \sum_{i=1}^{3} \varepsilon_i x_i + x_1x_2 + x_1x_3 + x_2x_3, \quad \varepsilon_i \in \{0, 1\}.$$

Deze zijn niet-singulier als $\sum \varepsilon_i = 0$, en singulier als $\sum \varepsilon_i = 1$.

Voorbeeld. In $(V, \mathbf{F}_2)$ is de standaardvorm

$$x_1y_2 + x_2y_1 + x_3y_4 + x_4y_3.$$

Equivalent hiermee is

$$(x, y) = \sum_{i \neq j} x_i y_j.$$

De 16 bijbehorende kwadratische vormen

$$Q(x) = \sum \varepsilon_i x_i + \sum_{i<j} x_i x_j, \quad \varepsilon_i \in \{0,1\},$$

zijn alle niet-singulier.

Opgave 18 In $V(4, \mathbf{F}_2)$ zijn zowel $\sum_{i<j} x_i x_j$ als $\sum_{i\leq j} x_i x_j$ van het type $Q^-(x)$. Welke $Q(x)$ zijn van het type $Q^+(x)$?

Opgave 19 In $V(6, \mathbf{F}_2)$ is $\sum_{i\leq j} x_i x_j$ van het type $Q^+(x)$ en $\sum_{i<j} x_i x_j$ van type $Q^-(x)$. Hoe zit dat in $V(2m, \mathbf{F}_2)$?

Zij $B(x,y)$ een niet-ontaarde alternerende bilineare vorm op $V(2m, \mathbf{F}_2)$, en zij $Q^\varepsilon(x)$ een daarbij behorende kwadratische vorm. Beschouw de $2^{2m} \times 2^{2m}$ matrices

$$B := [B(x,y)]_{x,y\in V}\,, \quad Q^\varepsilon := [Q^\varepsilon(x+y)]_{x,y\in V}\,.$$

Opgave 20 Bewijs dat $[B\ J{-}B]$ een (2^{2m+1}, 2^{2m}, 2^{2m-1})-code is. Interpreteer 0, 1 als elementen van $\mathbf{Z}$ en bewijs dat $2B - J$ een Hadamard matrix is.

Opgave 21 Bewijs dat Q^ε per rij $2^{2m-1} - \varepsilon 2^{m-1}$ enen heeft. Maak een Hadamard matrix van Q^ε.

Zij $\mathcal{B}$ de vectorruimte van alle (ook de ontaarde, ook nul) alternerende bilineaire vormen $B(x,y) = x^t By$ op $V(2m, \mathbf{F}_2)$, met

$$(B_1 + B_2)(x,y) := B_1(x,y) + B_2(x,y).$$

Zij $\mathcal{Q}$ de vectorruimte van alle mogelijke kwadratische vormen $Q(x)$ op $V(2m, \mathbf{F}_2)$, met

$$(Q_1 + Q_2)(x) := Q_1(x) + Q_2(x).$$

Opgave 22 Bewijs dat $\dim \mathcal{B} = m(2m-1)$, $\dim \mathcal{Q} = m(2m+1)$. Wat is het verband tussen $\mathcal{B}$ en $\mathcal{Q}$?

4.6 Polaire ruimten

De voorgaande paragrafen zijn gewijd aan de zogenaamde *klassieke meetkunden*, hun isotrope punten en hun totaal isotrope deelruimten. In elk der gevallen draagt de verzameling der isotrope punten drie soorten structuur.

I. Orde-structuur: de totaal isotrope deelruimten, partieel geordend door inclusie.

II. Lijn-structuur: de punten en de lijnen zijn de isotrope punten en de totaal isotrope lijnen.

III. Graaf-structuur: de knopen zijn de isotrope punten; twee punten zijn verbonden als de corresponderende isotrope punten op een totaal isotrope lijn liggen.

Deze structuren zijn gelijkwaardig. De doorsned van de totaal isotrope deelruimten door twee punten (volgens I) geeft de lijn door die punten (volgens II). Twee punten op een lijn (volgens II) zijn verbonden (volgens III). De maximale klieken (volgens III) zijn de maximale totaal isotrope deelruimten (volgens I), en elke totaal isotrope deelruimte is de doorsned van twee maximale totaal isotrope deelruimten. Deze laatste uitspraak volgt uit de standaard Gram matrix

$$\begin{bmatrix} O & O & I & O & O \\ O & O & O & I & O \\ \pm I & O & O & O & O \\ O & \pm I & O & O & O \\ O & O & O & O & G \end{bmatrix}$$

In de polaire meetkunde stelt men axioma's op voor deze structuren, teneinde de klassieke meetkunden te karakteriseren. Soms levert dit extra mogelijkheden, ook wanneer men zich beperkt tot eindige structuren. Het verst in deze richting gaan Buekenhout en Shult [5] met de volgende definitie voor een structuur van de soort II.
Een *prepolaire ruimte* is een incidentie structuur $(\mathcal{P}, \mathcal{L})$ van punten en lijnen (met tenminste 2 punten) zodat elke $P \in \mathcal{P}$ en $l \in \mathcal{L}$ met $P \notin l$ voldoen aan de eigenschap: P is verbonden met één of alle punten van l.

VOORBEELD. De isotrope punten $\mathcal{P}$ en de totaal isotrope lijnen $\mathcal{L}$ van een klassieke meetkunde vormen een prepolaire ruimte. Inderdaad, voor gegeven $P \notin l$ geldt ofwel $P \notin l^\perp$, dus $Q := P^\perp \cap l$ is het enige punt van l verbonden met P door een lijn uit $\mathcal{L}$, ofwel $P \in l^\perp$ dus
$inP^\perp$ en alle punten van l zijn verbonden met P door lijnen uit $\mathcal{L}$.

VOORBEELD. Een cockktail party graaf Γ is het complement van een 1-factor:

De knopen en de verbindingen van Γ vormen een prepolaire ruimte, die "mager" is, in de zin dat elke lijn twee punten heeft. De maximale klieken in Γ komen overeen met de maximale totaal isotrope deelruimten.

VOORBEELD. Een gegeneraliseerde vierhoek is een prepolaire ruimte, omdat daarin elk punt P verbonden is met één punt van elke lijn $l \not\ni P$.

Een prepolaire ruimte heet *niet-ontaard* als er geen punt bestaat dat met alle andere punten van $\mathcal{P}$ verbonden is door lijnen van $\mathcal{L}$. Buekenhout en Shult [5]

bewijzen dat in een niet-ontaarde prepolaire ruimte door elk tweetal punten ten hoogste één lijn gaat.
Een *lineaire deelruimte* van een prepolaire ruimte is een deelverzameling van paarsgewijs verbonden punten die met twee punten alle punten van een lijn bevat. De *rang* van een prepolaire ruimte is de lengte van een maximale vlag van lineaire deelruimten. Voor een niet-ontaarde prepolaire ruimte met lijnen van tenminste drie punten tonen Buekenhout en Shult de structuur I van een polaire ruimte in de zin van Tits aan.
Een *polaire ruimte van rang* n is een verzameling S (van punten) en een collectie van deelverzamelingen (genaamd lineaire deelruimten) die voldoen aan

(i) een lineaire deelruimte met de daarin bevatte lineaire deelruimten vormt een projectieve ruimte van dimensie d, met $-1 \leq d \leq n-1$,

(ii) de doorsnede van twee lineaire deelruimten is een lineaire deelruimte,

(iii) voor een gegeven lineaire deelruimte D van dimensie $n-1$ en een punt $P \in S \setminus d$ is er een unieke lineaire deelruimte E zodat $P \in E$, $\dim D \cap E = n-2$, en E bevat elk punt van D dat collineair is met P,

(iv) er bestaan disjuncte lineaire deelruimten van dimensie $n-1$.

Tits [**?**] en Veldkamp hebben de polaire ruimten van rang ≥ 3 geklassificeerdd. In het eindige geval zijn de juist de in dit hoofdstuk behandelde klassieke polaire ruimten. De polaire ruimten van rang 2 zijn de gegeneraliseerde vierhoeken (voor de klassieke gegeneraliseerde vierhoeken, zie [6], pag 301).
Ook voor de grafenstructuur III is er een karakterisering,

Stelling 4.6 (Buekenhout-Shult) . *Zij Γ een eindige graaf met de volgende eigenschap. Elke verbinding ligt in een kliek Δ van afmeting ≥ 3 zodat elke knoop buiten Δ is verbonden met één of alle knopen van Δ. dan geldt een van de volgende mogelijkheden:*

(i) Γ bevat een knoop verbonden met alle andere knopen,

(ii) Γ is de lege graaf,

(iii) $\Gamma = \Gamma(\pi)$, waarin π een polariteit of een niet-ontaarde kwadratische vorm is op een projectieve ruimte $\mathcal{P}$; de knopen van $\Gamma(\pi)$ zijn de isotrope of de singuliere punten van $\mathcal{P}$, die verbonden zijn als zij loodrecht zijn,

(iv) De klieken Δ van Γ zijn maximale klieken; de knopen en de klieken van Γ vormen een gegeneralizeerde vierhoek.

Hoofdstuk 5

Kwadratische verzamelingen

5.1 Ovalen

Een *ovaal* in een projectief vlak $PG(2,n)$ is een verzameling van $n+1$ punten waarvan geen drie collineair zijn. Een *secant*, *tangent*, *passant*, van een ovaal is een lijn die respectievelijk 2, 1, 0 snijpunten met de ovaal heeft.

Opgave 23 Door elk punt van een ovaal gaat één tangent. Een ovaal heeft $n+1$ tangenten, $n(n+1)/2$ secanten en $n(n-1)/2$ passanten. Bewijs dit.

Stelling 5.1 (Qvist) *In $PG(2,n)$, n even, gaan alle tangenten aan een ovaal door één punt.*

Bewijs. Zij $n = 2m$. Omdat de ovaal een oneven aantal punten heeft, gaat er door elk punt van elke secant tenminste één tangent. Omdat de ovaal in totaal $2m+1$ tangenten heeft, gaat er door elk punt van elke secant precies één tangent. Het snijpunt van twee tangenten kan dus slechts door tangenten worden verbonden met de punten van een ovaal. Daarom ligt dit snijpunt op alle tangenten. Dit snijpunt heet de *nucleus* van de ovaal. $\square$

Als gevolg van deze stelling laat elke ovaal in $PG(2,2m)$ zich uitbreiden tot een verzameling K van $2m+2$ punten waarvan geen drie punten collineair zijn. Elk punt $\notin K$ ligt op $m+1$ secanten en m passanten van K. Elke secant bevat $2m-1$ punten $\notin K$.

Opgave 24 De graaf Γ wordt gedefinieerd op de punten van $\mathcal{P} \setminus K$, en twee punten zijn verbonden wanneer hun verbindingslijn een secant van K is. bewijs dat Γ een sterk reguliere graaf is en bepaal de parameters. Construeer een symmetrische Hadamard matrix met een constante diagonaal, door de graaf Γ uit te breiden met een geisoleerd punt.

Opgave 25 Bewijs dat in $PG(2, 2m+1)$ geen drietal tangenten aan een ovaal door één punt gaat.

Vervolgens beschouwen wij een Desargues vlak $PG(2,q)$, $q = p^r$, $p \neq 2$ priem, afkomstig van de vectorruimte $V(3, \mathbf{F}_q)$. Een *kegelsnede* is de verzameling

$$\{\langle x \rangle \in PG(2,q) \,|\, Q(x) = 0\}$$

waarin $Q(x)$ een niet-singuliere kwadratische vorm op V is. Een kegelsnede is een ovaal. Wij willen omgekeerd bewijzen dat elke ovaal een kegelsnede is (vermoeden van Kustaanheimo, bewezen door Segre).

Lemma *In $PG(2,q)$ liggen de driehoek gevormd door 3 punten van de ovaal en de driehoek gevormd door de tangenten in deze punten perspectivisch.*

Bewijs. Neem $\langle e_1 \rangle$, $\langle e_2 \rangle$, $\langle e_3 \rangle$, $\langle p \rangle$ op de ovaal K. Geef de lijnen $\langle e_i, p \rangle$ $i = 1, 2, 3$ de vergelijking

$$x_2 = \lambda_1 x_3; \quad x_3 = \lambda_2 x_1; \quad x_1 \lambda_3 x_2,$$

met $\lambda_1 \lambda_2 \lambda_3 = 1$. Laat de tangenten in $\langle e_1 \rangle$, $\langle e_2 \rangle$, $\langle e_3 \rangle$ tot vergelijking hebben

$$t_1 \, : \, x_2 = \alpha_1 x_3 \, ; \, t_2 \, : \, x_3 = \alpha_2 x_1 \, ; \, t_3 \, : \, x_1 = \alpha_3 x_2.$$

Neem $i \in \{1, 2, 3\}$. Wanneer $\langle p \rangle$ alle punten ongelijk $\langle e_i \rangle$, $i = 1, 2, 3$ van K doorloopt, dan doorloopt λ_i alle waarden van $\mathbf{F}_q$ behalve 0 en α_i, dus

$$\alpha_i \prod \lambda_i = -1.$$

Vermenigvuldig, voor $i = 1, 2, 3$, dan volgt $\alpha_1 \alpha_2 \alpha_3 = -1$. Hier uit volgt dat de verbindingslijnen van $\langle e_i \rangle$ en $t_j \cap t_k$ (met $\{i, j, k\} = \{1, 2, 3\}$) door één punt U gaan (ga na!). Wanneer wij $U = \langle e_1 + e_2 + e + 3 \rangle$ nemen dan geldt $\alpha_1 = \alpha_2 = \alpha_3 = -1$. $\square$

Stelling 5.2 *In een Desargues vlak van oneven orde is elke ovaal een kegelsnede.*

Bewijs. Neem $\langle e_1 \rangle$, $\langle e_2 \rangle$, $\langle e_3 \rangle$, $\langle e_1 + e_2 + e_3 \rangle$ als in het lemma. Dan heeft niet alleen de ovaal K, maar ook de kegelsnede

$$C = \{\langle x \rangle \in PG(2,q) \,|\, x_1 x_2 + x_2 x_3 + x_3 x_1 = 0\}$$

in zijn punten $\langle e_i \rangle$ de tangent t_i met $\alpha_i = -1$. We gaan bewijzen dat $(\langle p \rangle \in K) \Rightarrow (\langle p \rangle \in C)$. Laat $P = \langle (p_1, p_2, p_3) \rangle$ en $t \, : \, b_1 x_1 + b_2 x_2 + b_3 x_3 = 0$ een punt en de bijbehorende tangent aan K zijn. Pas het lemma toe op de driehoek $\langle e_i \rangle$, $\langle e_j \rangle$, $\langle p \rangle$ dan volgt $b_2(p_1 + p_2) = b_3(p_1 + p_3)$ en cyclisch. De eis dat P op t ligt voert dan tot het gestelde. $\square$

Opgave 26 Vul de details in, bij het bovenstaande bewijs.

OPMERKING. De zojuist bewezen stelling van Segre geldt niet in een Desargues vlak van even orde ≥ 8. Inderdaad, beschouw de kegelsnede C in $PG(2, 2^k)$ en vervang één van zijn punten door zijn nucleus. De verkregen ovaal heeft meer dan 7 punten gemeen met de oorspronkelijke kegelsnede. Daarom is deze ovaal geen kegelsnede (twee kegelsneden hebben immers ten hoogste 4 punten gemeen).

5.2 De kwadriek van Klein

Wij gaan de lijnen van $PG(3, \mathbf{F})$ beschrijven met behulp van zes Plücker coördinaten. Beschouw twee vectoren a en b in $V(d, \mathbf{F})$. Wij gebruiken $a \wedge b$ als bilineair alternerend symbool voor het paar a, b, dat is,

$$a \wedge a = 0,\ a \wedge b = -b \wedge a,\ a \wedge (b + c) = a \wedge b + a \wedge c,\ a \wedge (\lambda b) = \lambda(a \wedge b).$$

Op een constante na bepaalt $a \wedge b$ de deelruimte $\langle a, b\rangle$, omdat

$$(\lambda a + \mu b) \wedge (\rho a + \sigma b) = (\lambda\sigma - \mu\rho)(a \wedge b).$$

Ten opzichte van de basis $e_1, e_2, \ldots, e_d$ van $V(d, \mathbf{F})$ geldt

$$a \wedge b = \left(\sum_i \alpha_i e_i\right) \wedge \left(\sum_i \beta_i e_i\right) = \sum_{i<j} (\alpha_i\beta_j - \alpha_j\beta_i) e_i \wedge e_j.$$

De Plücker coördinaten van $a \wedge b$ zijn de $d(d - 1)/2$ coördinaten

$$p_{ij} := \alpha_i\beta_j - \alpha_j\beta_i\,; \quad i < j\,;\ i, j = 1, \ldots, d.$$

Stelling 5.3 *In $V(4, \mathbf{F})$ geldt voor de zes coördinaten van $a \wedge b$,*

$$p_{12}p_{34} + p_{23}p_{14} + p_{31}p_{24} = 0.$$

BEWIJS. Wegens $p_{ij} = -p_{ji}$ geldt het volgende:

$$\begin{bmatrix} 0 & p_{12} & p_{13} & p_{14} \\ p_{21} & 0 & p_{23} & p_{24} \\ p_{31} & p_{32} & 0 & p_{34} \\ p_{41} & p_{42} & p_{43} & 0 \end{bmatrix} \begin{bmatrix} 0 & p_{43} & p_{24} & p_{32} \\ p_{34} & 0 & p_{41} & p_{13} \\ p_{42} & p_{14} & 0 & p_{21} \\ p_{23} & p_{31} & p_{12} & 0 \end{bmatrix} = I_4.$$

De linker matrix heeft rang 2, omdat

$$\text{rang } [\alpha_i\beta_j - \alpha_j\beta_i] \leq \text{rang } [\alpha_i\beta_j] + \text{rang } [\alpha_j\beta_i] = 1 + 1.$$

Daarom is rechts de determinant, dus de factor nul. □

De uitdrukking $p_{12}p_{34} + p_{23}p_{14} + p_{31}p_{24} = 0$ is de vergelijking van een hyperbolische kwadriek Ω^+ in $PG(5, \mathbf{F})$, met coördinaten $(p_{23}, p_{31}, p_{12}, p_{14}, p_{24}, p_{34})$. Dit is de *Klein kwadriek*.

Stelling 5.4 *Er is een bijectie tussen de rechten van $PG(3, \mathbf{F})$ en de punten van de Klein kwadriek Ω^+.*

BEWIJS. Een rechte in $PG(3, \mathbf{F})$ correspondeert met een vlak in $V(4, \mathbf{F})$, dus met een $a \wedge b$, dus met zes coördinaten die voldoen aan de vergelijking van de kwadriek. Omgekeerd behoort er precies één rechte in $PG(3, \mathbf{F})$ bij gegeven p_{ij}, niet alle nul, die voldoet aan de vergelijking van Ω^+. Inderdaad, de projectieve punten $(0, p_{12}, p_{13}, p_{14})$, $(p_{21}, 0, p_{23}, p_{24})$, $(p_{31}, p_{32}, 0, p_{34})$ en $(p_{41}, p_{42}, p_{43}, 0)$ zijn collineair, en de $a \wedge b$ van elk tweetal heeft Plücker coördinaten evenredig met p_{ij}. □

Stelling 5.5 *Twee lijnen in $PG(3, \mathbf{F})$ met Plücker coördinaten p_{ij} en q_{ij} snijden elkaar dan en slechts dan als*

$$B(p_{ij}, q_{ij}) := p_{12}q_{34} + p_{34}q_{12} + p_{23}q_{14} + p_{14}q_{23} + p_{31}q_{24} + p_{24}q_{31} = 0.$$

BEWIJS. Stel de lijnen zijn gegeven door $a \wedge b$ en $c \wedge d$. De lijnen snijden elkaar dan en slechts dan als

$$0 = \begin{vmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \beta_1 & \beta_2 & \beta_3 & \beta_4 \\ \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 \\ \delta_1 & \delta_2 & \delta_3 & \delta_4 \end{vmatrix}.$$

Ontwikkel de determinant naar de onderdeterminanten van de beide eerste rijen, dan verkrijgt met $B(p_{ij}, q_{ij})$. □

In $V(6, \mathbf{F})$ is de vorm $B(p_{ij}, q_{ij})$ een symplectische vorm. In termen van $PG(5, \mathbf{F})$ zegt de stelling dat twee lijnen in $PG(3, \mathbf{F})$ snijden wanneer de corresponderende punten op de Klein kwadriek verbonden zijn door een op Ω^+ liggende lijn. Dus als $\langle p \rangle \in \Omega^+$ en $\langle q \rangle \in \Omega^+$, dan

$$\langle p, q \rangle \in \Omega^+ \Leftrightarrow B(p, q) = 0.$$

De correspondentie tussen de lijnen van $PG(3, \mathbf{F})$ en de punten van $\Omega^+ \subset PG(5, \mathbf{F})$ kan in beide richtingen worden gebruikt.

VOORBEELD. Op de Klein kwadriek Ω^+ liggen twee soorten projectieve vlakken, namelijk die corresponderend met de lijnen in een vlak, en die corresponderend met de lijnen door een punt in $PG(3, \mathbf{F})$.

Opgave 27 Hoe gedragen zich deze twee soorten vlakken onderling en wederzijds?

Een *lineair complex* van lijnen in $PG(3, \mathbf{F})$ is een stelse lijnen dat in $PG(5, \mathbf{F})$ corresponeert met de doorsnede van de Klein kwadriek Ω^+ en een hypervlak. Een lineair complex wordt bepaald door de pool van zijn hypervlak ten opzichte van Ω^+. Omdat $PO^+(6, \mathbf{F})$ transitief is op de punten van Ω^+, en ook

op de punten $\notin \Omega^+$, hebben wij de volgende standaardvormen voor de lineaire complexen:
De pool $(0, 0, 0, 0, 0, 1)$ geeft het *speciale lineaire complex*, $p_{12} = 0$.
De pool $(0, 0, 1, 0, 0, 1)$ geeft het *algemene lineaire complex*, $p_{12} + p_{34} = 0$.

Stelling 5.6 *Een speciaal lineair complex bestaat uit alle lijnen in $PG(3, \mathbf{F})$ die een gegeven lijn snijden.*

Bewijs. Het hypervlak van een speciaal lineair complex raakt aan de Klein kwadriek. Het speciale complex bestaat dus uit alle lijnen die de met het raakpunt corresponderende lijn snijden. □

Stelling 5.7 *Een algemeen lineair complex bestaat uit alle lijnen van $PG(3, \mathbf{F})$ die totaal isotroop zijn ten opzichte van een symplectische vorm.*

Bewijs. Zonder de algemeenheid te schaden geven wij het complex de standaardvorm

$$0 = p_{12} + p_{34} = x_1 y_2 - x_2 y_1 + x_3 y_4 - x_4 y_3 =: b(x, y)$$

voor projectieve lijnen $\langle x, y \rangle$. Interpreteer nu $b(x, y)$ als een symplectische vorm voor $PG(3, \mathbf{F})$. □

Opgave 28 Bewijs dat in $PG(3, \mathbf{F}_q)$door elk punt $q+1$ lijnen van een algemeen lineair complex gaan en dat die lijnen in een vlak liggen.

Opgave 29 Waarmee corresponderen de regelscharen van een hyperboloide in $PG(3, \mathbf{F})$?

5.3 The twisted polarity

We specializeren nu tot $\mathbf{F} = GF(q)$, $q = 2^h$, en beschouwen wederom

$$V(4, \mathbf{F}_q) = V = \langle e_1, e_2, e_3, e_4 \rangle,$$
$$V \wedge V = \langle e_2 \wedge e_3, e_3 \wedge e_1, e_1 \wedge e_2, e_1 \wedge e_4, e_2 \wedge e_4, e_3 \wedge e_4 \rangle.$$

V is voorzien van de symplectische vorm

$$[b(e_i, e_j)] = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \oplus \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

en $V \wedge V$ is voorzien van de boven gedefinieerde vorm $B(\, , \,)$, die op de basisvectoren werkt volgens

$$B(e_h \wedge e_i, e_j \wedge e_k) = \begin{cases} 1 & \text{als } \{h, i, j, k\} = \{1, 2, 3, 4\}, \\ 0 & \text{anders.} \end{cases}$$

Het lineaire complex $p_{12}+p_{34} = 0$ wordt in V voorgesteld door de totaal isotrope vlakken ten opzichte van $b(x, y)$, en in $V \wedge V$ door de 5-dimensionale deelruimte W

$$W := \langle e_1 \wedge e_2 + e_3 \wedge e_4,\ e_1 \wedge e_3,\ e_2 \wedge e_4,\ e_1 \wedge e_4,\ e_2 \wedge e_3\rangle.$$

Ten opzichte van $B(,)$ heeft W het radicaal

$$\text{rad } W = \langle e_1 \wedge e_2 + e_3 \wedge e_4\rangle,$$

en $W = (\text{rad } W) \perp V'$, met

$$V' = \langle e_1 \wedge e_3, e_2 \wedge e_4, e_1 \wedge e_4, e_2 \wedge e_3\rangle.$$

Definieer de lineaire afbeelding (projectie) $\pi : W \to V$ door

$$\begin{array}{lll} \pi(\text{rad } W) = 0, & \pi(e_1 \wedge e_3) = e_1, & \pi(e_2 \wedge e_4) = e_2, \\ & \pi(e_1 \wedge e_4) = e_3, & \pi(e_2 \wedge e_3) = e_3. \end{array}$$

Dan induceert π een isometrie tussen V' met $B(,)$ en V met $b(,)$. Projectief gezien induceert π een bijectie tussen de totaal isotrope lijnen en de punten van de symplectische $PG(3, q)$.
De lijnen door een punt P in $PG(3, q)$ corresponderen met de punten van een projectief vlak op de Klein kwadriek. De totaal isotrope lijnen door P in $PG(3, q)$ corresponderen met de punten van een projectieve lijn op Ω^+, die onder π wordt geprojecteerd op een totaal isotrope lijn van de symplectische $PG(3, q)$.
Zij $\mathcal{L}$ de verzameling van de totaal isotrope lijnen van de symplectische $PG(3, q)$, en zij $\mathcal{P}$ de verzameling van de punten van $PG(3, q)$. Dan induceert π dus niet alleen een afbeelding $\pi_{\mathcal{L}} : \mathcal{L} \to \mathcal{P}$, maar ook een afbeelding $\pi_{\mathcal{P}} : \mathcal{P} \to \mathcal{L}$, en er geldt

$$(P \in l) \Longleftrightarrow (\pi_{\mathcal{L}}(l) \in \pi_{\mathcal{P}}(P)).$$

Wij onderzoeken of $\pi_{\mathcal{L}}\pi_{\mathcal{P}} : \mathcal{P} \to \mathcal{L} \to \mathcal{P}$ aanleiding kan geven tot een “polariteit” tussen $\mathcal{P}$ en $\mathcal{L}$. Daartoe berekenen wij eerst $\pi_{\mathcal{L}}\pi_{\mathcal{P}}$.
Zij $x = \sum x_i e_i$, $y = \sum y_i e_i$, $z = \sum z_i e_i$ met $b(x, y) = b(x, z) = 0$. Wij berekenen

$$\begin{array}{rcl} \pi_{\mathcal{L}}\pi_{\mathcal{P}}(\langle x\rangle) & = & \pi_{\mathcal{L}}(\pi_{\mathcal{L}}(x \wedge y) \wedge \pi_{\mathcal{L}}(x \wedge z)). \\ \pi(x \wedge y) \wedge \pi(x \wedge z) & = & b(y, z)[(x_1x_2 + x_3x_4)(e_1 \wedge e_2 + e_3 \wedge e_4) + \\ & & +x_1^2 e_1 \wedge e_3 + x_2^2 e_2 \wedge e_4 + x_3^2 e_1 \wedge e_4 + x_4^2 e_2 \wedge e_3]. \\ \pi(\pi(x \wedge y) \wedge \pi(x \wedge y)) & = & b(x, y)\left[x_1^2 e_1 + x_2^2 e_2 + x_3^2 e_3 + x_4^2 e_4\right]. \end{array}$$

Hieruit volgt

$$\pi_{\mathcal{L}}\pi_{\mathcal{P}}\langle(x_1, x_2, x_3, x_4)\rangle = \langle(x_1^2, x_2^2, x_3^2, x_4^2)\rangle,$$

met andere woorden, $\pi_{\mathcal{L}}\pi_{\mathcal{P}} : \mathcal{P} \to \mathcal{L} \to \mathcal{P}$ is een semilineaire afbeelding ten opzichte van het *Frobenius automorfisme* $\phi : \alpha \mapsto \alpha^2$ van $GF(2^h)$. Dit bewijst:

Lemma *Voor $\pi_{\mathcal{L}}\pi_{\mathcal{P}} : \mathcal{P} \to \mathcal{L} \to \mathcal{P}$ geldt $\pi_{\mathcal{L}}\pi_{\mathcal{P}} = \phi$.*

Lemma *$GF(2^h)$ bezit een (uniek) automorfisme σ met $\sigma^2 = \phi$ dan en slechts dan als h oneven is.*

Bewijs. voor $h = 2m+1$ voldoet $\alpha^\sigma = \alpha^{2^{m+1}}$ omdat

$$(\alpha^\sigma)^\sigma = \left(\alpha^{2^{2m+1}}\right)^2 = \alpha^2.$$

Voor even h is $GF(4)$ een deellichaam, waarin het kwadraat van elke $\sigma \in \text{Aut } GF(2^h)$ de identiteit induceert. □

Stelling 5.8 *Er bestaat een (unieke) "polariteit" ρ tussen $\mathcal{P}$ en $\mathcal{L}$, d.w.z. afbeeldingen $\rho_\mathcal{P} : \mathcal{P} \to \mathcal{L}$ en $\rho_\mathcal{L} : \mathcal{L} \to \mathcal{P}$ met $\rho_\mathcal{P}\rho_\mathcal{L} = 1_\mathcal{L}$, $\rho_\mathcal{L}\rho_\mathcal{P} = 1_\mathcal{P}$, in een symplectische $PG(3,q)$, $q = 2^h$, dan en slechts dan als h oneven is.*

Bewijs. Zij h oneven. Voor $\pi_\mathcal{L}\pi_\mathcal{P} : \mathcal{P} \to \mathcal{L} \to \mathcal{P}$ geldt $\pi_\mathcal{L}\pi_\mathcal{P} = \phi$ en $\phi = \sigma^2$, $\sigma \in$ Aut $GF(2^h)$. Definieer $\rho_\mathcal{P} := \sigma^{-1}\pi_\rho$, $\rho_\mathcal{L} := \sigma^{-1}\pi_\mathcal{L}$ dan is, omdat $\pi\sigma = \sigma\pi$,

$$\rho_\mathcal{L}\rho_\mathcal{P} = \sigma^{-1}\pi_\mathcal{L}\sigma^{-1}\pi_\mathcal{P} = \sigma^{-2}\pi_\mathcal{L}\pi_\mathcal{P} = \sigma^{-2}\sigma^2 = 1.$$

Dit bewijst dat $\rho_\mathcal{L}$ en $\rho_\mathcal{P}$ elkaars inverse zijn. Noem $\rho_\mathcal{P} = \rho$, dan geldt voorts

$$(P_1 \in \rho(P_2)) \Longleftrightarrow (P_2 \in \rho(P_1)).$$

Als h even is, dan bestaat er geen σ, en ook geen polariteit. □

Deze $\rho : \mathcal{P} \leftrightarrow \mathcal{L}$ heet de *twisted polarity* van Tits, vgl. D.E. Taylor's appendix "The geometry of the Klein quadric" in [12]; zie ook [6] en de volgende paragraaf.

5.4 Ovoiden

Een *ovoide* is een verzameling van q^2+1 punten in $PG(3, \mathbf{F}_q)$ waarvan geen drietal op een lijn ligt. Een voorbeeld van een ovoide is een elliptische kwadriek. Analoog aan de stelling van Segre geldt (Barlotti):

Stelling 5.9 *In $PG(3, \mathbf{F}_q)$, q oneven, is elke ovoide een elliptische kwadriek.*

Wij beperken ons verder tot $PG(3, \mathbf{F}_q)$, $q = 2^h$. Zij M een *maximale verzameling* van $q^2 + m$ punten waarvan geen drietal op een lijn ligt. $PG(3,2)$ heeft maximale M van 8 punten, namelijk de punten buiten een vlak. Voor $q = 2^h$, $h > 1$ geldt echter het volgende.

Stelling 5.10 *In $PG(3, \mathbf{F}_q)$, $q = 2^h$, $h > 1$ is een maximale verzameling een ovoide (dus $m = 1$).*

Bewijs. Zij $P \in M$, M een maximale verzameling. Wij bewijzen eerst dat er een tangent door P bestaat. Stel dat elke lijn door P secant is, dan heeft M

q^2+q+2 punten, $\binom{q^2+q+2}{2}$ secanten en geen tangenten. Maar het totaal aantal lijnen van $PG(3, \mathbf{F}_q)$ is

$$(q^2+1)(q^2+q+1) > \binom{q^2+q+2}{2}$$

dus er is een passant, zeg l. De vlakken door l snijden M in 0 of $q+2$ punten, dus $q+2$ is een deler van

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

en $q=2$, tegenspraak.
Zij t een tangent door P aan M. Van de $q+1$ vlakken door t heeft tenminste één, zeg π, met M de $q+1$ punten van een ovaal gemeen. Inderdaad, $q+2$ punten kan niet, omdat er dan geen tangenten zijn, en als alle vlakken $\leq q$ punten van M zouden hebben, dan zou M

$$\leq 1+(q+1)(q-1) = q^2 < q^2+m$$

hebben. Zij N de nucleus van de ovaal in π. Elke lijn door N in π snijdt de ovaal dus in één punt. Voorts gaat door N tenminste één secant $s \notin \pi$, anders zou M niet maximaal zijn. Elk vlak door s snijdt M in tenhoogste $q+1$ punten (niet in $q+2$ punten omdat er een tangent in π is). Maar dan levert

$$m+q^2 \leq 2+(q+1)(q-1)$$

dat $m=1$. Voorts heeft elk vlak door de secant s precies $q+1$ punten van M.
□

Stelling 5.11 *Zij $\mathcal{O}$ een ovoide in $PG(3,q)$, $q=2^h$, $h>1$. Elk vlak snijdt $\mathcal{O}$ in 1 of $q+1$ punten. Er zijn q^2+1 raakvlakken en q^3+q snijvlakken.*

BEWIJS. Net als in de vorige stelling nemen wij $P \in \mathcal{O}$, een tangent $t \ni P$, een vlak $\pi \ni t$ met $|\pi \cap \mathcal{O}| = q+1$, de nucleus N van $\pi \cap \theta$, en een secant $s \ni N$. Wij weten dat elk vlak door s de ovoide $\mathcal{O}$ in $q+1$ punten snijdt. Zij $Q \in \mathcal{O} \setminus \pi$. Dan is NQ een secant van $\mathcal{O}$. Inderdaad, de doorsnede van $\mathcal{O}$ met het vlak σ door s en NQ is een ovaal, waarvoor $\sigma \cup \pi$ een tangent, en s een secant is, dus waarvoor N niet de nucleus is. Elk vlak door t heeft dus ofwel slechts P, ofwel $q+1$ punten met $\mathcal{O}$ gemeen. Er zijn dus q snijvlakken en precies één raakvlak door t. Dit geldt voor elk punt $P \in \mathcal{O}$, en de bewering volgt. □

Stelling 5.12 *Zij $\mathcal{O}$ een ovoide in $PG(3,q)$, $q=2^h$, $h>1$. Door $P \notin \mathcal{O}$ gaan $q+1$ tangenten; deze liggen in een vlak.*

BEWIJS. $\mathcal{O}$ is maximaal, dus er is een secant s door P. In elk van de $q+1$ vlakken door s heeft P precies één tangent. Twee tangenten door P bepalen een vlak en dus een ovaal, waarvan P de nucleus is. Buiten de tangenten aan deze ovaal heeft P dus geen andere tangenten. $\square$

Ten opzichte van een ovoide $\mathcal{O}$ in $PG(3,q)$, $q = 2^h$, bestaat de volgende correlatie. Een raakvlak correspondeert met zijn raakpunt. Een snijvlak correspondeert met de nucleus van zijn snijovaal; dan correspondeert een punt $P \notin \mathcal{O}$ met het vlak van zijn tangenten aan $\mathcal{O}$.

Stelling 5.13 *De zojuist beschreven correlatie is een symplectische polariteit.*

Bewijs. Als P en π corresponderen, dan geldt $P \in \pi$ en de tangenten in π zijn de lijnen door P. Als ook P' en π' corresponderen, dan geldt

$$(P \in \pi') \Longleftrightarrow (P \cup P' = \pi \cup \pi') \Longleftrightarrow (P' \in \pi),$$

dus de correlatie is een polariteit van het symplectische type. $\square$

De totaal isotrope lijnen ten opzichte van de gevonden symplectische polariteit zijn de tangenten aan de ovoide. Er zijn $(q+1)(q^2+1)$ tangenten, en evenveel punten in $PG(3,q)$. Door een punt gaan $q+1$ tangenten, en elke tangent bevat $q+1$ punten. Noem $\mathcal{P}$ de verzameling der punten, en $\mathcal{L}$ de verzameling der tangenten. In **??** hebben wij aangetoond dat voor h oneven (en slechts dan) er een (unieke) twisted polarity $\rho : \mathcal{P} \to \mathcal{L}$ met $\rho^2 = 1$ bestaat, geconstrueerd met behulp van het unieke automorfisme σ van $GF(2^h)$ dat voldoet aan $\sigma^2 = \phi$. De verzameling van q^2+1 punten die op hun ρ-beeld liggen is een ovoide. Deze ovoide heet de *Tits-ovoide*. De tangenten die hun ρ-beeld bevatten vormen een spread van $PG(3,q)$. Dit heeft een aantal gevolgen.

Gevolg. In verband met de in **??** genoemde stelling van André geeft de spread bestaande uit de q^2+1 tangenten aan de Tits-ovoide aanleiding tot de constructie van een eindig translatievlak van de order 2^{4r+2}, voor elke $r \geq 1$, zie [**?**] §12.

Gevolg. Voor $q \geq 8$ zijn de Tits-ovoiden geen kwadrieken. Inderdaad, het volgende is niet bijzonder moeilijk aan te tonen (zie [12], appendix §8. of [21] §1.). In $PG(3,q)$ worden affiene coordinaten ingevoerd: $x = x_3/x_1$, $y = x_4/x_1$, $z = x_2/x_1$. Dan bestaat de Tits-ovoide uit het oneigenlijke punt van de z-as en de q^2 punten

$$\left\{(x,y,z) \,|\, z = xy + x^{2+\sigma} + y^\sigma\right\}.$$

Reeds voor $q = 8$ levert dit een ovoide op die geen kwadriek is.

Gevolg. De groep der automorfismen van de Tits-ovoide is de *Suzuki groep* $Sz(q)$ van de orde $(q^2+1)q^2(q-1)$. Deze groep werkt 2-transitief op de Tits-ovoide. Voor de structuur van $Sz(q)$, zie [12] appendix, [21] en [29].

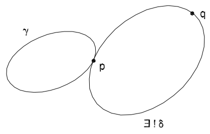
5.5 Möbius meetkunde

Een *Möbius vlak* $(\mathcal{P}, \mathcal{L})$ is een verzameling $\mathcal{P}$ van punten, en een collectie Γ van deelverzamelingen (zeg cirkels), zodat geldt:

(i) elk drietal punten ligt op één cirkel,

(ii) er zijn vier punten niet op een cirkel,

(iii) $\forall p, q \in \mathcal{P} : \forall \gamma \in \Gamma, p \in \gamma, q \notin \gamma \exists! \delta \in \Gamma : (p \in \delta,\ q \in \delta,\ \gamma \cup \delta = \{p\})$.



Figuur 5.1:

Voorbeeld. De punten en de cirkels van een sfeer in $\mathbf{R}^3$ voldoen aan de axioma's. Stereografische projectie vanuit $N \in$ sfeer geeft de punten, lijnen en cirkels van het Euclidische vlak. Wanneer slechts de cirkels door N worden beschouwd, dan geeft stereografische projectie de punten en lijnen van het Euclidische vlak, en wordt (iii) het axioma van Euclides.

Voorbeeld. Zij $\mathcal{P}$ de verzameling van de punten van een ovoide in $PG(3, \mathbf{F})$. Zij Γ de collectie van de snijvlakken van de ovoide (dus niet de raakvlakken). Dan vormt $(\mathcal{P}, \Gamma)$ een Möbiusvlak. Zij $P \in \mathcal{P}$ een vast punt van de ovoide, met raakvlak π. De lijnen $\notin \pi$ door P, en de vlakken $\neq \pi$ door P vormen een Desargues affien vlak.

Voorbeeld. Beschouw het "complexe" vlak $GF(q^2) \cup \{\infty\}$ met conjugatie $-$ en zelfgeconjugeerde $GF(q)$. De elementen van het complexe vlak en de cirkels

$$\left\{ z \in GF(q^2) \,|\, rz\bar{z} + \bar{s}z + s\bar{z} + t = 0;\ r, s, t \in GF(q) \right\}$$

vormen een Möbiusvlak. De Möbius transformaties

$$z \mapsto \frac{az+b}{cz+d}, \quad ad-bc=1,$$

voeren cirkels in cirkels over.

Opgave 30 De punten en de blokken van een 3-$(n^2+1, n+1, 1)$ design vormen een Möbius vlak.

Wij keren terug tot de definitie van een Möbius vlak $(\mathcal{P}, \mathcal{L})$.

Stelling 5.14 *Zij Λ het deel van Γ dat bestaat uit alle cirkels door een vast punt $N \in P$. Dan is $(\mathcal{P} \setminus \{N\}, \Lambda)$ een affien vlak.*

Opgave 31 Bewijs deze stelling.

Wij weten dat een affien vlak niet Desargues hoeft te zijn. Dat is wel zo wanneer het Möbius vlak *kwadrikaal* (afkomstig van een elliptische kwadriek in $PG(3, \mathbf{F})$) of *ovoidaal* (afkomstig van een ovoide in $PG(3, \mathbf{F})$) is. In de Möbius meetkunde tracht met ovoidale en kwadrikale Möbius vlakken te karakteriseren door meetkundige eigenschappen van de cirkels.

Stelling 5.15 *Möbius vlak is kwadrikaal dan en slechts dan als de stelling van Miquel geldt.*

Voor dit resultaat van van der Waerden en Smid (1935) zie [6] Ch. 6, en ook [20]

Stelling 5.16 *Een Möbius vlak is ovoidaal dan en slechts dan als de bundelstelling geldt.*

Voor de bundelstelling zie [6]. Van der Waerden en Smid (1935) bewezen $\Rightarrow$, en J. Kahn [1] bewees de andere kant. Omdat een elliptische kwadriek een ovoide is, en omdat er ovoiden bestaan die geen kwadriek zijn (zie **??**), impliceert de stelling van Miquel de bundel stelling, maar niet omgekeerd (vergelijk het gedrag van de stellingen van Pappus en Desargues). Voor verdere resultaten zie [6] Ch. 6.
Analoog aan de Möbius meetkunde worden de meetkunden van *Minkowski* en *Laguerre* gedefinieerd. Wij volstaan met een eenvoudig model, en verwijzen verder naar [8] Kapitel 12.

VOORBEELD. Zij Ω een hyperbolische kwadriek of een kwadratische kegel in $PG(3, q)$. Zij Σ de verzameling der vlakken in $PG(3, q)$, die met Ω tenminste twee punten, maar geen rechte gemeen hebben. Dan is (Ω, Σ) een Minkowski meetkunde als Ω een hyperboloide is, en een Laguerre meetkunde als Ω een kegel is. Stereografische projectie vanuit een punt $N \in \Omega$ levert een $(q-1, q)$-net, respectievelijk een (q, q)-net (zie **??** en ga na).

Bibliografie

[1] Moet nog gebeuren

[2] E. Artin, Geometric Algebra (1957)

[3] R. Baer, Linear algebra and projective geometry (1957)

[4] L.M. Blumenthal, A modern view of geometry (1961)

[5] F. Buekenhout, E. Shult, On the foundations of polar spaces, Geom. Ded. **3** (1974), 155-170.

[6] P. Dembowski, Finite geometries (1968)

[7] K.W. Gruenberg–A.J. Weir, Linear geometry (1967)

[8] H. Halder–W. Heise, Einführung in die Kombinatorik (1976)

[9] M. Hall, The theory of groups (1959)

[10] M. Hall, Combinatorial theory (1967)

[11] R. Hartshorne, Foundations of projective geometry (1967)

[12] D.G. Higman, Classical groups, TH-report 78-WSK-04 (1978)

[13] J.W.P. Hirschfeld, Projective geometries over finite fields (1979)

[14] D.R. Hughes–F.C. Piper, Projective planes (1973)

[15] R. Kamber, Untersuchungen über affine Ebenen der Ordnung 9, Thesis ETH Zürich (1976)

[16] I. Kaplansky, Linear algebra and geometry (1974)

[17] artikel van Lam

[18] S. Lang, Algebra (1969)

[19] J.H. van Lint, Combinatorial theory seminar THE (1974)

[20] J.H. van Lint, Möbius vlakken, M.C. vakantiecursus (1978)

[21] H. Lüneburg, Die Suzukigruppen und ihre Geometrien (1965)

[22] H. Lüneburg, Transitive erweiterungen endlicher permutationsgruppen (1969)

[23] T.G. Ostrom, Finite translation planes, Springer lecture notes 158 (1970)

[24] T.G. Room–P.B. Kirkpatrick, Miniquaternion geometry (1971)

[25] J.J. Seidel, On two-graphs, and Shult's characterization of symplectic and orthogonal geometries over $GF(2)$, TH-Report 73-WSK-02 (1973)

[26] E.E. Shult, Groups, polar spaces and related structures, Nijenrode conference, M.C. Tract **57** (1974) 130–161.

[27] O. Tamaschke, Projectieve Geometrie I, II (1971)

[28] J. Tits, Buildings of spherical type and finite BN-pairs (1974)

[29] J. Tits, Ovoides et groupes de Suzuki, Archiv. Math. **13** (1962), 187–198.