Groups and geometries

Jürgen Bierbrauer

May 6, 1997

Contents

Chapter 1

Grouptheoretical prerequisites

The reader is assumed to be familiar with the following notions:

1. group
2. order of a finite group, order of an element
3. subgroup, normal subgroup, factor group
4. homomorphism, image, kernel, isomorphism
5. coset, index
6. Lagrange's theorem: the order of a subgroup of a finite group divides the order of the group.
7. isomorphism theorems like the following: if $\alpha : G_1 \longrightarrow G_2$ is a homomorphism, then $\alpha(G_1) \cong G_1/ker(\alpha)$, or: if N is a normal subgroup of G (we write $N \trianglelefteq G$) and A a subgroup of G (write $A \leq G$), then $NA/N \cong A/N \cap A$.
8. abelian groups, commutators, commutator subgroup
9. automorphism group
10. conjugation
11. inner automorphisms, center, centralizer, normalizer

12. permutation representation, orbit, transitivity, stabilizer G_x of a symbol x in group G.

13. orbit formula: the length of an orbit is the index of the stabilizer $|x^G| = [G : G_x]$.

14. simple group

15. p-group for a prime p.

16. Sylow's theorems: if G is a finite group and p a prime diciding its order, $|G| = p^n m$, where p does not divide m, then G does possess a subgroup P of order p^n (the **Sylow-p-subgroup**), all these subgroups are conjugate in G, their number (=the index of the normalizer $I\!N(P)$) is $\equiv 1(mod\ p)$. A p-subgroup $P \leq G$ is Sylow-p-subgroup if and only if p is not a divisor of $|I\!N_G(P)/P|$. Each p-subgroup of G is contained in a Sylow-p-subgroup.

17. direct product

18. cyclic group Z_n of order n.

19. calculations in Z_n :

    - if x generates Z_n and $(m, n) = 1$, then x^m generates Z_n (proved by Euclidean algorithm).
    - For arbitrary m the group generated by x^m has order $n/(n, m)$.
    - If $(n, m) = 1$, then the direct product $Z_n \times Z_m$ is the cyclic group Z_{nm}.
    - The **Euler ϕ function:** $\phi(n)$ is the number of generators of Z_n, equivalently the order of the automorphism group $Aut(Z_n)$. If $n = \prod_i p_i^{a_i}$ is the representation of n as a product of prime-powers, then $\phi(n) = \prod_i (p_i^{a_i} - p_i^{a_i - 1} = n \prod_{p|n}(1 - 1/p)$.
    - If $m|n$, then $x^{n/m}$ generates the unique subgroup of order m of Z_n.

20. elementary abelian group E_{p_n} (isomorphic to the additive group of a vector space).

21. on p-groups:

    - if $1 \neq N \lhd P$, then $N \cap \mathbb{Z}(P) \neq 1$, in particular the center of a nontrivial p-group is nontrivial.
    - If $Q < P$ are p-groups, then $\mathbb{N}_P(Q) > Q$ (in particular $Q \lhd P$ if $[P : Q] = p$).

22. A composition series of $G : G = G_0 \supset G_1 \supset \ldots \supset G_r = 1$, where all the $G_i \lhd G$ and G_i/G_{i+1} simple.

23. Jordan-Hölder theorem for composition series: the factors G_i/G_{i+1} are the same for all composition series, including multiplicities.

24. G is called a **solvable** group if all the factors in a composition series are cyclic groups (then necessarily of prime order).

Chapter 2

The classical simple groups

2.1 The alternating groups

Denote by S_n the **symmetric group** on n letters, consisting of the $n!$ permutations of an n-set Ω. Permutations are most conveniently written in the cycle notation. For example when $n = 6, \Omega = \{1, 2, 3, 4, 5, 6\}$ we write $\alpha = (1, 2, 4)(3, 6)$ to denote the permutation, which fixes 5 and maps $1 \longrightarrow 2 \longrightarrow 4 \longrightarrow 1, 3 \longrightarrow 6 \longrightarrow 3$. A cycle of length 1 is a **fixed point** and is usually not written out, a cycle of length 2 is a **transposition.** If we view Ω as basis of a vector space, then S_n is represented as a group of invertible linear mappings of the vector space $V = V(n, K)$ over an arbitrarily chosen field K. A transposition yields a linear mapping of determinant -1. Each permutation can be written as a product of transpositions. It suffices to prove this for a cycle:

$$(1, 2, \ldots, n-1, n) = (n-1, n)(n-2, n-1) \ldots (2, 3)(1, 2).$$

Here the products denote composition of functions. Choose K as a field in characteristic 0. The determinant is a surjective group homomorphism $det : S_n \longrightarrow \{+1, -1\}$. The **alternating group** A_n is defined as the kernel of the determinant, equivalently the group of all permutations of determinant 1, equivalently the group of all permutations which can be written as product of an even number of transpositions. We have $|A_n| = n!/2$. The elements of A_n are also called **even permutations.** A fact which we will not prove here is that A_n is a simple group when $n \geq 5$.

2.2 The linear groups

q is a prime-power, $\mathbb{F}_q$ the field of that order, $V = V(n,q)$ the vector space of dimension $n \geq 2$ over $\mathbb{F}_q$. The **general linear group** $GL(n,q)$ is defined as the group of all bijective linear mappings $\alpha : V \longrightarrow V$, equivalently the group of all (n,n)-matrices over $\mathbb{F}_q$ with nonzero determinant. Here the group operation is composition of functions. Fix a basis $(v_1, v_2, \dots, v_n)$ of V. A linear mapping $\alpha : V \longrightarrow V$ is in $GL(n,q)$ if and only if the image of the fixed basis is a basis again. It follows that the elements of $GL(n,q)$ are in bijection with the ordered bases. This leads to an efficient way of determining the order of our group:

$$|GL(n,q)| = (q^n - 1)(q^n - q)\dots(q^n - q^{n-1}) = q^{n(n-1)/2}\prod_{i=1}^{n}(q^i - 1).$$

In fact, as first vector of an ordered basis we can choose any nonzero vector. This explains the factor $q^n - 1$. Once it is fixed the second basis element can be chosen as any vector which is not in the 1-dimensional subspace spanned by the first basis vector. We have $q^n - q$ choices. Proceeding like this we arrive at the formula. The power of q involved is $1+2+\dots n-1 = n(n-1)/2 = \binom{n}{2}$. The determinant yields a surjective group homomorphism

$$det : GL(n,q) \longrightarrow \mathbb{F}_q^* \cong Z_{q-1}$$

onto the multiplicative group of the field. The kernel of the determinant is denoted by $SL(n,q)$, the **special linear group.** We have seen that it has index $q-1$ in $GL(n,q)$. The **center** Z of $GL(n,q)$ consists of all scalar matrices $diag(\lambda, \lambda, \dots, \lambda)$, where $\lambda \in \mathbb{F}_q^*$. In particular $Z \cong Z_{q-1}$. The factor group $PGL(n,q) = GL(n,q)/Z$ is known as the **projective linear group.** It is clear that $|Z \cap SL(n,q)| = (n, q-1)$. In fact, a scalar matrix $diag(\lambda, \lambda, \dots, \lambda)$ is in $SL(n,q)$ if and only if $\lambda^n = 1$, and this equation has $(n, q-1)$ solutions λ in the cyclic group of order $q-1$.
The **projective special linear group** $PSL(n,q)$ is defined as the factor group $PSL(n,q) = SL(n,q)/(Z \cap SL(n,q))$. We have seen that its order is

$$|PSL(n,q)| = \frac{1}{(n,q-1)}q^{n(n-1)/2}\prod_{i=2}^{n}(q^i - 1).$$

We remark that $PSL(n,q) \trianglelefteq PGL(n,q)$ is canonically embedded: consider the projection of $GL(n,q)$ to $PGL(n,q)$. When this projection is restricted to the normal subgroup $SL(n,q)$, we obtain as image $PSL(n,q)$. The group $PSL(n,q)$ is simple in all cases except then $n=2, q=2$ and when $n=2, q=3$.

2.3 Scalar products

Let $V=V(n,q)$ as before. Consider mappings

$$(,): V \times V \longrightarrow \mathbb{F}_q,$$

which are biadditive: $(x_1+x_2,y)=(x_1,y)+(x_2,y)$ and $(x,y_1+y_2)=(x,y_1)+(x,y_2)$ (everything in V). In particular $(0,y)=(x,0)=0$ always. This product is **non-degenerate** if the only element x_0 satisfying $(x_0,y)=0$ for all $y \in V$ is $x_0=0$ and analogously the only $y_0 \in V$ satisfying $(x,y_0)=0$ for all $x \in V$ is $y_0=0$. It is **bilinear** if

$$(\lambda x, y)=(x, \lambda y)=\lambda \cdot (x,y) \text{ for all } x,y \in V, \lambda \in \mathbb{F}_q.$$

The group $GL(n,q)$ operates on the scalar products in the following way: if $g \in GL(n,q)$, then $(,)_g$ is defined as

$$(x,y)_g=(x^g,y^g).$$

Such scalar products $(,)$ and $(,)_g$ are called **equivalent.** The stabilizer $\{g \in GL(,n,q) | (,)_g=(,)\}$ is called the **group of isometries** of $(,)$.
A vector $v \in V$ is **isotropic** if $(v,v)=0$. A subspace $U \subset V$ is **totally isotropic** if $(u,u')=0$ for all $u,u' \in U$. Given the scalar product $(,)$ and a basis $\{v_1,v_2,\ldots,v_n\}$ of V we can form the **Gram matrix** $A=((v_i,v_j))_{i,j}$.

2.4 The symplectic groups

Let $(,)$ be a non-degenerate bilinear scalar product, which satisfies in addition

$$(x,x)=0 \text{ for all } x \in V.$$

This says that every vector is isotropic. In the general possibly degenerate case the elements x_0 satisfying $(x_0,V)=0$ form a subspace, the **radical.**

As $0 = (x+y, x+y) = (x,y) + (y,x)$ we see that $(,)$ is **skew-symmetric.** Clearly we must have $n \geq 2$. If $W \subseteq V$, then the orthogonal of W is defined by

$$W^{\perp} = \{x | (x,w) = 0 \text{ for all } w \in W\}.$$

Observe that because of the skew-symmetry we could as well have used (w,x) in this expression. Moreover it is clear that $W^{\perp}$ will always be a subspace of V, for an arbitrary subset W.

2.4.1 Hyperbolic planes

Let $n = 2$. Choose $0 \neq x \in V$. Then $x^{\perp} =< x >$ is 1-dimensional (if it was the whole space, then $(,)$ would be degenerate). It follows that there exists $y \in V$ such that $(x,y) = 1$. The Gram matrix with respect to basis x, y is $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. These 2-dimensional symplectic spaces are called **hyperbolic planes.**

2.4.2 Case $n > 2$

Let $n \geq 3, 0 \neq x \in V$. Just as in case $n = 2$ we find $y \in V$ such that the 2-dimensional space $H =< x, y >$ is a hyperbolic plane (a 2-dimensional non-degenerate symplectic space, that is). In particular $H \cap H^{\perp} = 0$. As $H^{\perp}$ has dimension $n-2$ we must have $V = H \oplus H^{\perp}$. Moreover $H^{\perp}$ is non-degenerate as every element in the radical of $H^{\perp}$ is also in the radical of V, and V is assumed to be non-degenerate. We can use induction. Certainly we can prove by induction that n must be even, but we also get that V is a direct sum of hyperbolic planes: $n = 2m$ and we can choose a basis $\{v_1, v_2, \ldots, v_m\} \cup \{w_1, w_2, \ldots, w_m\}$ such that

$$V = H_1 \perp H_2 \perp \ldots \perp H_n,$$

where $H_i =< v_i, w_i >, (v_i, w_i) = 1$. We speak of a **symplectic basis.** The corresponding Gram matrix A has $(2,2)$-submatrices $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ along the main diagonal. All other entries are 0. We see that $det(A) = 1$.

The symplectic group $Sp(2m, q)$ is defined as the group of isometries of a

non-degenerate symplectic scalar product. We have seen that these symplectic scalar products form one orbit under the general linear group. It follows that the same holds for the symplectic groups: they form a conjugate class of subgroups of $GL(2m, q)$.
Fix a symplectic basis as above. An element $g \in GL(2m, q)$ is in the symplectic group of and only if the image of the symplectic basis is a symplectic basis again. This makes it easy to determine the order of $Sp(2m, q)$. The image of v_1 is any nonzero vector v'_1. This gives us a factor of $q^{2m} - 1$. Once v'_1 has been chosen the image w'_1 of w_1 is a vector satisfying $(v_1, w_1) = 1$. The number of such vectors is $(q^{2m} - q^{2m-1})/(q-1)$, as $q^{2m} - q^{2m-1}$ are not orthogonal to v'_1 and each nonzero scalar product occurs the same number of times. Put $H_1 =< v_1, w_1 >, H'_1 =< v'_1, w'_1 >$. Then H_1, H'_1 are hyperbolic planes and $H_1^\perp, H_1'^\perp$ are nondegenerate symplectic spaces of dimension $2(m-1)$. Moreover, an element of $Sp(2m, q)$ mapping $v_1 \longrightarrow v'_1, w_1 \longrightarrow w'_1$ must map $H_1^\perp \longrightarrow H_1'^\perp$. We are in an inductive situation and obtain $|Sp(2m, q)| = \prod_{i=1}^m (q^{2i} - 1) q^{2i-1}$. The q-part of the order is therefore $q^{1+3+\ldots+(2m-1)}$. As $\sum_{i=1}^m (2i+1) = m^2$ we obtain

Theorem (2.1) $|Sp(2m, q)| = q^{m^2} \prod_{i=1}^m (q^{2i} - 1)$.

Let us use coordinates: so A is the Gram matrix of a non-degenerate symplectic scalar product, with respect to a fixed basis $x_1, x_2, \ldots, x_{2m}$. We know that A is a skew-symmetric matrix. Moreover A is regular (has determinant $det(A) \neq 0$) as a nontrivial vanishing linear combination of the rows is equivalent to a nonzero vector in the radical. Let $g \in GL(n, q)$ be represented by matrix T with respect to the fixed basis (x_i). Then $(x_i^g, x_j^g) = (x_i T, x_j T) = (\sum_k t_{ik} x_k, \sum_l t_{jl} x_l) = \sum_{k,l} t_{ik} a_{k,l} t_{jl}$. This is the entry in position (i, j) of the matrix TAT^t, where T^t denotes the transpose of T. We have proved the following:

Lemma (2.1) *Let A be the Gram matrix of the non-degenerate symplectic $2m$-dimensional scalar product $(,)$ with respect to a fixed basis. Let $g \in GL(n, q)$ be represented by matrix T with respect to this basis. Then $g \in SP(2m, q)$ with respect to $(,)$ if and only if $TAT^t = A$.*

Because of the multiplicativity of the determinant we see that $det(T)^2 = 1$, hence $det(T) = \pm 1$. It is in fact true that necessarily $det(T) = 1$, hence $SP(2m, q) \subset SL(2m, q)$. This will be shown in the following subsection.

2.4.3 The Pfaffian

We have seen that there is an equivalence between

- Symplectic scalar products (,) with respect to a fixed basis $\{x_i\}$, and
- skew-symmetric matrices $A = ((x_i, x_j))$.

Moreover we know what happens to this equivalence under the action of the general linear group. In fact, we have the equivalence between

- Equivalence classes (orbits) of symplectic scalar products, and
- $\{TAT^t \mid T \in GL\}$.

Under this equivalence the symplectic scalar product is **nondegenerate** if and only if $det(A) \neq 0$.
Denote the ground field by K. We see that $det(A) \pmod{K^2}$ is an invariant of the equivalence class. As $det(A) = 1$ with respect to a symplectic basis and application of the general linear group amounts to an arbitrary choice of basis, we conclude that $det(A)$ is a square for every skew-symmetric matrix A. We shall use this information to the utmost:
Let $K = I\!R$. Consider the universal (n, n)-skew-symmetric matrix (x_{ij}), where $x_{ii} = 0$ and $x_{ji} = -x_{ij}$. Consider the x_{ij}, where $i < j$ as indeterminates. The matrix (x_{ij}) is considered as a matrix with entries in the field $K(\{x_{ij}\})$ of rational functions in the indeterminates. We have seen above that the determinant of this matrix is a square:

$$det(x_{ij}) = (f/g)^2,$$

where f, g are polynomials in the indeterminates and can be chosen coprime, with integer coefficients. As $det(x_{ij})$ is a polynomial with integer coefficients, we see that $g \mid f$, hence $g = \pm 1$. It follows $det(x_{ij}) = f^2$. We conclude that this is true over any field and any set of values x_{ij}. We can choose the sign of f such that in the case of a symplectic base we get $f = 1$.

Theorem (2.2) *There is a polynomial $Pf(\{x_{ij}\})$ in the indeterminates x_{ij} with integer coefficients (the* **Pfaffian***) such that for any skew-symmetric matrix (g_{ij}) we have*

$$det(g_{ij}) = Pf(g_{ij})^2.$$

If moreover (g_{ij}) *corresponds to a symplectic base (meaning that we have (2,2)-matrices* $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ *along the main diagonal, all other entries zero), then* $Pf(g_{ij}) = 1$..

Let us introduce more indeterminates $a_{ij}, i, j = 1, 2, \ldots, n$. Consider the skew-symmetric matrix $(y_{ij}) = (a_{ji})(x_{ij})(a_{ij})$. Then $det(y_{ij}) = det(x_{ij}) \cdot det(a_{ij})^2$. For the Pfaffian this means $Pf(y_{ij}) = \epsilon \cdot Pf(x_{ij}) \cdot det(a_{ij})$, where $\epsilon = \pm 1$.

Theorem (2.3) *If* (g_{ij}) *is skew-symmetric and* T *is nonsingular, then*

$$Pf(T(g_{ij})T^t) = det(T) \cdot Pf(g_{ij}).$$

Let now (g_{ij}) correspond to a symplectic base and $T \in Sp_{2n}(K)$. This means that $T(g_{ij})T^t = (g_{ij})$. Application of Theorem (2.3) yields $1 = Pf(g_{ij}) = det(T)$.

Corollary (2.1)

$$Sp_{2n}(q) \leq SL_{2n}(q).$$

$Sp_{2n}(q) \cap Z = \pm I$.

Proof: If a scalar matrix $\lambda \cdot I \in Sp_{2n}(q)$, then $\lambda^2 = 1$, hence $\lambda = \pm 1$.■

We note without proof that the factor group $S_{2n}(q) = PSp_{2n}(q) = Sp_{2n}(q)/\pm I$ is a simple group, with the exceptions of $S_2(2), S_2(3)$ and $S_4(2)$. Finally we determine $S_2(q)$. By definition a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is symplectic if and only if

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} 0 & ad-bc \\ -(ad-bc) & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Theorem (2.4)

$$S_2(q) = L_2(q).$$

2.5 The unitary groups

$I\!F_{q^2} \mid I\!F_q$ has the involutory field automorphism $\alpha \mapsto \overline{\alpha} = \alpha^q$ (the **Frobenius** automorphism). Clearly $\alpha = \overline{\alpha}$ if and only if $\alpha \in I\!F_q$. The situation is analogous to complex conjugation in the complex field. $(,)$ is called a **unitary scalar product** if

$$(w, v) = \overline{(u, v)}$$

and

$$(\alpha \cdot v, w) = \alpha(v, w),\ (v, \alpha w) = \overline{\alpha}(v, w)$$

always hold (we speak of **semilinearity** with respect to the Frobenius). We assume in the sequel that $(,)$ is non-degenerate and $n \geq 2$. Assume now $(x, x) = 0$ for all $x \in V$. Choose x_1, x_2 such that $(x_1, x_2) = 1$. Then $(x_1 + \lambda x_2, x_1 + \lambda x_2) = \lambda + \overline{\lambda}$. For a suitable choice of λ this will be $\neq 0$, leading to a contradiction. We have shows that we can find x_1 such that $(x_1, x_1) \neq 0$. As $(x_1, x_1) \in I\!F_q$ and $(\lambda x_1, \lambda x_1) = \lambda^{q+1}(x_1, x_1)$ we can choose $(x_1, x_1) = 1$. We get $V =< x_1 >\perp x_1^{\perp}$. By induction we obtain an orthonormal basis. In particular the non-degenerate unitary scalar products form one orbit under the action of the general linear group. The general unitary group is given by

$$GU_n(q) = \{T \mid T \in GL_n(q), T\overline{T}^t = I\} = \{T \mid T \in GL_n(q), \overline{T}^t = T^{-1}\}.$$

It follows $GU_n(q) \cap Z = \{\lambda I \mid \lambda^{q+1} = 1\} \cong Z_{q+1}$.
Let us consider the 2-dimensional case. Pick an element α such that $\alpha^{q-1} = -1$, equivalently $\overline{\alpha} = -\alpha$. Then $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is an isometry of the unitary scalar product with Gram matrix $\begin{pmatrix} 0 & \alpha \\ -\alpha & 0 \end{pmatrix}$ is symplectic if and only if

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & \alpha \\ -\alpha & 0 \end{pmatrix} \begin{pmatrix} \overline{a} & \overline{c} \\ \overline{b} & \overline{d} \end{pmatrix} = \alpha \begin{pmatrix} a\overline{b} - \overline{a}b & a\overline{d} - \overline{c}b \\ b\overline{c} - \overline{d}a & c\overline{d} - \overline{c}d \end{pmatrix} = \begin{pmatrix} 0 & \alpha \\ -\alpha & 0 \end{pmatrix}.$$

If we choose $a, b, c, d \in I\!F_q$ such that $ad - bc = 1$ this is satisfied. This shows $SL_2(q) \leq SU_2(q^2)$. We are going to see shortly that the orders of these groups are the same. This shows:

Theorem (2.5)

$$SL_2(q) \cong SU_2(q^2).$$

Let $x_1, x_2, \ldots, x_n$ be an orthonormal basis and $g \in GL_n(q^2)$. Then $g \in GU_n(q^2)$ if and only if $x_1^g, \ldots, x_n^g$ form an orthonormal basis. We have to determine the numbers of elements $v \in V$ such that (v,v) takes on a certain value.

Proposition (2.1) *The number of $v \in V$ such that $(v,v) = 0$ is $q^{n-1}(q^n + (-1)^n(q-1))$. For every $0 \neq \alpha \in \mathbb{F}_q$ the number of vectors $v \in V$ satisfying $(v,v) = \alpha$ is $q^{n-1}(q^n - (-1)^n)$.*

Proof: Denote by $f(n,\alpha)$ the number of $v \in V$ such that $(v,v) = \alpha$. Write $v = \sum_{i=1}^n a_i x_i$. Then $(v,v) = \sum_i a_i^{q+1}$. We see that each value $\alpha \neq 0$ occurs equally often, in other words $f(n,\alpha) = f(n,1)$. Clearly $q^{2n} = f(n,0) + (q-1)f(n,1)$. Distinguishing according to the value of a_n we obtain: $f(n,0) = f(n-1,0) + (q^2-1)f(n-1,1)$. The Proposition follows by induction.■

Theorem (2.6) *The orders of the unitary groups are as follows:*

- $|GU(n,q^2)| = \prod_{i=1}^n q^{i-1}(q^i - (-1)^i) = q^{n(n-1)/2}(q+1)(q^2-1) \cdot \ldots \cdot (q^n - (-1)^n)$
- $|SU(n,q^2)| = \prod_{i=2}^n q^{i-1}(q^i - (-1)^i)$.
- *Let $U_n(q) = SU_n(q^2)/(Z \cap SU_n(q^2)$. Then $|U_n(q)| = \frac{1}{gcd(n,q+1)}|SU_n(q^2)|$.*

Proof: This follows from Proposition (2.1). The image of x_1 is to chosen among the $f(n,1)$ vectors v satisfying $(v,v) = 1$. The order of the general unitary group is clearly $f(n,1)f(n-1,1)\ldots f(1,1)$. As the determinant takes on each $(q+1)$-st root of unity as a value we see that SU has index $q+1$ in GU. A scalar matrix $\lambda \cdot I$ is in $SU_n(q)$ if and only if $\lambda^n = \lambda^{q+1} = 1$. It follows that $Z \cap SU_n(q)$ has order $gcd(n,q+1)$.■
We note without proof that the groups $U_n(q), n \geq 3$ are simple, with the only exception of $U_3(2)$.

2.6 The orthogonal groups in odd characteristic

The non-degenerate scalar product $(,)$ is **symmetric** (or **orthogonal**) if

$$(v, w) = (w, v)$$

always holds. We can proceed like in the symplectic case. A hyperbolic pair v, w is defined by $(v, v) = (w, w) = 0, (v, w) = 1$. The corresponding matrix is therefore $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

If v is given such that $(v, v) = 0$, we can find a partner w such that $\{v, w\}$ form a hyperbolic pair. Then $V =< v, w >\perp< v, w >^\perp$ and $< v, w >^\perp$ is a non-degenerate orthogonal space. We can use induction. Let now $U \subset V$ be given. Write $U = R \perp U_0$, where R is totally isotropic and U_0 is non-degenerate ($R = U \cap U^\perp = rad(U)$ is the **radical** of U). Let $R =< u_1, u_2, \ldots, u_m >$. Find vectors v_i such that $\{u_i, v_i\}$ is a hyperbolic pair and $< U, v_1, v_2, \ldots, v_m >= H_1 \perp \ldots \perp H_m \perp U_0$ is non-degenerate. Here $H_i =< u_i, v_i >$ are hyperbolic planes. Denote by $ind(V)$ (the **index**) the maximal dimension of a totally isotropic subspace. We have seen that $ind(V) \leq n/2$.
Let now $U \subset V$ be a maximal isotropic subspace, $U =< u_1, u_2, \ldots, u_m >$. Then $V =< u_1, v_1 >\perp \ldots \perp< u_m, v_m >\perp V_0$, where V_0 is an **anisotropic** subspace, meaning that $(v_0, v_0) \neq 0$ whenever $0 \neq v_0 \in V_0$. This raises the question about the possible dimensions of anisotropic spaces.
So let $V_0 \neq 0$ be an anisotropic space. We work under the assumption that the ground field $\mathbb{F}_q$ has odd characteristic.

Lemma (2.2) *Let G be a finite abelian group (written additively). The following hold:*

1. *If $M, N \subseteq G, |M|, |N| > |G|/2$, then $G = M + N$.*
2. *If K is a finite field, $a \cdot b \neq 0$, then $K = aK^2 + bK^2$.*

Proof: Consider 1. Let $g \in G$ be given. Put $A = -g + M, B = -N$. As $|A| = |M|, |B| = N$ we must have $A \cap B \neq \emptyset$. This shows that $g = m + n$ for some $m \in M, n \in N$. The second statement is obvious in characteristic 2, it follows from 1. in odd characteristic.■

Assume the anisotropic space V_0 has dimension > 2. Choose an orthonormal basis $u_1, u_2, u_3, \ldots$. Put $(u_i, u_i) = a_i \in \mathbb{F}_q^*$. By Lemma (2.2) we can find α, β such that $\alpha^2 a_1 + \beta^2 a_2 = -a_3$. Then $w = \alpha u_1 + \beta u_2 + u_3$ satisfies $(w, w) = 0$, contradiction. We conclude $dim(V_0) \leq 2$. Let $V_0 =< u_1, u_2 >$. By Lemma (2.2) we can find α, β such that $\alpha^2 a_1 + \beta^2 a_2 = 1$. Put $v_1 = \alpha u_1 + \beta u_2$. Then $(v_1, v_1) = 1$. Let $v_2 \in v_1^\perp, (v_2, v_2) = b$. As $0 \neq (xv_1 + v_2, xv_1 + v_2) = x^2 + b$, it follows that $b \notin -K^2$. Let c_0 be a fixed nonsquare. Without restriction $b = -c_0$.

Definition (2.1) *Let V be a non-degenerate symmetric bilinear form in odd characteristic. The* **discriminant** *$D(V)$ is the determinant of the Gram matrix A, mod $(\mathbb{F}_q^*)^2$. As a basis transformation T leads to the transformation TAT^t of the Gram matrix, the discriminant is uniquely determined.*

Lemma (2.3) *Let q be a power of the prime p, where $p \neq 2$, and $(,)$ a non-degenerate symmetric bilinear form over $\mathbb{F}_q$. Let c_0 be a nonsquare in $\mathbb{F}_q$. If $V_0 \neq 0$ is an anisotropic subspace, then $dim(V_0) \leq 2$ and V_0 is isometric to one of the following spaces:*

1. *$V_0 =< v_0 >$ and $(v_0, v_0) = 1$.*
2. *$V_0 =< v_0 >$ and $(v_0, v_0) = c_0$.*
3. *$V_0 =< v_1, v_2 >$, where $(v_1, v_2) = 0, (v_1, v_1) = 1, (v_2, v_2) = -c_0$.*

In the last case the discriminant of V_0 is $-c_0$ mod $\mathbb{F}_q^2$, and hence is

$$D(V_0) = \begin{cases} +1 & \text{if } q \equiv 3 \bmod 4 \\ -1 & \text{if } q \equiv 1 \bmod 4 \end{cases}.$$

The following is now an easy consequence:

Theorem (2.7) *Let V be a vector space of dimension n over $\mathbb{F}_q$, where q is a power of an odd prime, endowed with a symmetric non-degenerate scalar product $(,)$. Then V is isometric to one of the following spaces:*

1. *$dim(V) = n = 2m+1, V = H_1 \perp \ldots \perp H_m \perp < v_0 >$, with hyperbolic planes H_i and either $(v_0, v_0) = 1$ or $(v_0, v_0) = c_0$, where c_0 is a nonsquare. In these cases $ind(V) = m$ and $D(V) = 1$ or $D(V) = -1$, respectively.*

2. *$dim(V) = n = 2m$ and either*

$$V = H_1 \perp \ldots \perp H_m \text{ (the (+)-type)}$$

or

$$V = H_1 \perp \ldots \perp H_{m-1} \perp V_0 \text{ (the (-)-type),}$$

where V_0 is the 2-dimensional anisotropic space given in Lemma (2.3). In both cases $ind(V) = m-1$.

In order to be able and compute the orders of the orthogonal groups we have to count the numbers of vectors with a given value of (v, v) as before. These results are also of independent interest.
Consider at first the case of the (+)-type in dimension $n = 2m$. Let $f(m, c)$ be the number of vectors v such that $(v, v) = c$. As multiplication by the fixed nonsquare c_0 yields an equivalent scaler product we see that $f(m, c) = f(m, 1)$ for all $c \neq 0$. It follows $q^{2m} = f(m, 0) + (q-1)f(m, 1)$. Further $f(m+1, 0) = f(m, 0)(2q-1) + (q^{2m} - f(m, 0))(q-1)$, hence $f(m+1, 0) = (2q-1)f(m, 0) + (q-1)^2 f(m, 1)$. Here we have used the obvious fact that $f(1, 0) = 2q-1, f(1, 1) = q-1$. The values of $f(m, 0)$ and $f(m, 1)$ follow by induction.

Lemma (2.4) *In the orthogonal space of even dimension $2m$ and (+)-type the following holds: the number of vectors v satisfying $(v, v) = 0$ is $f(m, 0) = q^{m-1}(q^m + q - 1)$. For every $\alpha \neq 0$ the number of vectors v satisfying $(v, v) = \alpha$ is $f(m, 1) = q^{m-1}(q^m - 1)$.*

Let now $n = 2m+1$. Consider the case $(v_0, v_0) = 1$. As the second symmetric scalar product in odd dimension can be obtained by multiplication with a constant (a nonsquare), the isometry groups are the same. Denote by $g(m, c)$ the number of vectors v such that $(v, v) = c$. We continue to use the terminology $f(m, c)$ for the case of the scalar product in dimension $2m$ with index m. The numbers $g(m,c)$ can be obtained from the numbers $f(m,c)$ by distinguishing the coefficient at v_0 :

$$g(m,0) = f(m,0) + (q-1)f(m,1) = q^{2m}.$$

$$g(m,1) = f(m,1) + 2f(m,0) + (q-3)f(m,1) = q^m(q^m+1).$$

$$g(m,c_0) = f(m,1) + (q-1)f(m,1) = qf(m,1).$$

Lemma (2.5) *In the orthogonal space of odd dimension $2m+1$ with anisotropic complement $V_0 =< v_0 >$, where $(v_0, v_0) = 1$, the following hold: the number of vectors v satisfying $(v,v) = 0$ is $g(m,0) = q^{2m}$. For every square $\alpha \neq 0$ the number of vectors v satisfying $(v,v) = \alpha$ is $g(m,1) = q^m(q^m+1)$. If α is nonsquare, then the corresponding number is $g(m,c_0) = q^m(q^m-1)$.*

The isometry groups in our three cases are denoted by O_{2m+1}, O_{2m}^+ and O_{2m}^-, respectively. The orders are obtained by the usual counting arguments. Consider at first O_{2m+1}. The image of the isotropic vector v_1 is one of the $q^{2m}-1$ nonzero isotropic vectors. Once the image of v_1 is chosen, the number of choices for the image of its hyperbolic partner w_1 is $(q^{2m}-q\cdot q^{2m-2})/(q-1)$ (start from all isotropic vectors, subtract those in $v_1^\perp$, divide by $q-1$). This number is q^{2m-1}. As $< v_1, w_1 >^\perp$ is of the same type as V, we can use induction and obtain

$$|O_{2m+1}(q)| = 2\cdot q^{m^2}\prod_{i=1}^{m}(q^{2i}-1)$$

(observe that the sum of the odd numbers up to $2m-1$ is m^2 and that $O_1(q)$ has order 2).
Similar arguments yield the order of O_{2m}^+. There are $f(m,0)-1 = q^{m-1}(q^m+q-1)-1 = (q^{m-1}+1)(q^m-1)$ possible images of v_1. The number of images of its partner w_1 is then $(f(m,0)-q\cdot f(m-1,0))/(q-1) = q^{2m-2}$. It follows

$$|O_{2m}^+(q)| = q^{m(m-1)}2(q^2-1)(q^4-1)\dots(q^{2m-2}-1)(q^m-1).$$

It is an easy exercise to show that $|O_2^-(q)| = 2(q+1)$. Consider the orthogonal $2m$-dimensional geometry of (-)type. Denote the number of vectors with $(v,v) = c$ by $h(m,c)$. Consideration of the anisotropic part yields

$$h(m,0) = f(m-1,0) + (q+1)(q^{2m-2} - f(m-1,0)) = q^{m-1}(q^m-q+1).$$

As multiplication by a nonzero constant does not change the type of our scalar product we obtain $h(m,c) = h(m,1)$ for all $c \neq 0$. It follows

$$h(m,1) = (q^{2m} - h(m,0))/(q-1) = q^{2m-1} + q^{m-1}.$$

Lemma (2.6) *In the orthogonal space of even dimension $2m$ and (-)type the following hold: the number of vectors v satisfying $(v,v) = 0$ is $h(m,0) = q^{m-1}(q^m - q + 1)$. For every $\alpha \neq 0$ the number of vectors v satisfying $(v,v) = \alpha$ is $h(m,1) = q^{2m-1} + q^{m-1}$.*

In order to determine the order of the group in this case we observe that v_1 has $h(m,0) - 1 = (q^m + 1)(q^{m-1} - 1)$ possible images. By induction we obtain

$$|O^-_{2m}(q)| = 2q^{m(m-1)}[\prod_{i=1}^{m-1}(q^{2i} - 1)](q^m + 1).$$

Observe that this is also true for $m = 1$.

2.7 Witt's theorem

Theorem (2.8) (Witt's theorem) *Let V be endowed with a non-degenerate scalar product $(,)$. Assume one of the following cases occurs:*

1. *V symplectic, or*
2. *V bilinear symmetric in odd characteristic, or*
3. *V unitary*

Then the following holds: Assume $U_1, U_2 \subset V$ and $h : U_1 \longrightarrow U_2$ an isometry from U_1 onto U_2.
Then there is an isometry g of V with itself, whose restriction to U_1 agrees with h.

Observe that in cases 2. and 3. there are orthonormal bases. We prepare the proof. Consider at first the symmetric case.

Definition (2.2) *Let the scalar product be non-degenerate symmetric in odd characteristic. Further let* $(w,w)\neq 0$. *Then the mapping* S *given by*

$$vS = v - 2\frac{(v,w)}{(w,w)}w$$

is an isometry of V. *The restriction of* S *to* $w^\perp$ *is the identity and* $S: w\mapsto -w$. *We have* $det(S)=-1$ *Call the involution* $S=S_w$ *the* **reflection** *at* w.

Most of the claims made in Definition (2.2) are obvious. Let us show that S is indeed an isometry:

$$(v_1S, v_2S) = (v_1 - 2\frac{(v_1,w)}{(w,w)}w, v_2 - 2\frac{(v_2,w)}{(w,w)}w) =$$

$$= (v_1,v_2) - 2\frac{(v_1,w)(w,v_2)}{(w,w)} - 2\frac{(v_2,w)(v_1,w)}{(w,w)} + 4\frac{(v_1,w)(v_2,w)}{(w,w)} = (v_1,v_2).$$

Lemma (2.7) *Let the scalar product be non-degenerate symmetric in odd characteristic. If* $(v,v)=(w,w)\neq 0$, *then there is a an isometry* g, *which is a product of reflections and maps* $g: v\mapsto w$.

Proof: We have $(v+w, v-w)=0$. It is not possible that $v+w$ and $v-w$ are both isotropic as this would mean that the space generated by v and w is totally isotropic, which is not the case. Assume at first $v+w$ is not isotropic. Put $S=S_{v+w}$. Then $S: v\mapsto -w$. An orthogonal basis shows that -1 is a product of reflections. We are done in this case. Assume now that $v-w$ is not isotropic. Choose $S=S_{v-w}$. Then $S: v\mapsto w$.■

Lemma (2.8) *Let the scalar product by non-degenerate unitary. If* $(v,v)=(w,w)\neq 0$, *then there is a an isometry* g *such that* $g: v\mapsto w$.

Proof: Assume at first $w=av$. Then $a\overline{a}=1$. Choose g such that $g: v\mapsto av$ and g is the identity on $v^\perp$.
We can assume $dim(< v,w >)=2$. Consider first the case that $< v,w >$ is non-degenerate. Then $V =< v,w >\perp< v,w >^\perp$ and we can assume without restriction that $V =< v,w >$. Assume $(v-w)^\perp =< v >$. Then

$$0=(v,v-w)=(v,v)-(v,w)=(w,w)-(v,w)=(w-v,w).$$

It follows $< v >=< w >= (v-w)^{\perp}$, contradicting the dimensional assumption. We have that $(v-w)^{\perp}$ is different from $< v >$, and analogously also different from $< w >$. Let $< t >= (v-w)^{\perp}$. Then $< v, w >=< v, t >=< w, t >$, where $(v, t) = (w, t)$. It follows that there is an isometry fixing t and mapping $v \mapsto w$.
The last case is that $dim(< v, w >) = 2$ and $< v, w >$ is degenerate. The dimension of the radical can only be 1. Let $Rad(< v, w >) =< u >$. We can find $u' \in V$ such that $W =< u, u' > \perp < v >$ is non-degenerate (u, u' form a hyperbolic pair). As before we can assume without restriction $V = W$. As $(w, w) \neq 0$ we have $W = w^{\perp} \perp < w >$. As $w^{\perp}$ is non-degenerate it must be a hyperbolic plane (the existence of an orthonormal basis shows that non-degenerate unitary spaces are uniquely determined by their dimension). It follows that there must be an isometry mapping $v \mapsto w$, as claimed. ■

Lemma (2.9) *Let the scalar product by non-degenerate symplectic. For every $0 \neq w \in V$ and $0 \neq c \in K$ the mapping T defined by*

$$vT = v - v(v, w)w$$

is an isometry of V, which operates as the identity on $w^{\perp}$ and on $V/ < w >^{perp}$. We call T a **symplectic transvection.**

Proof: Most of the claims are obvious. We show that T preserves scalar products:

$$(v_1T, v_2T) = (v_1 - c(v_1, w)w, v_2 - c(v_2, w)w) =$$

$$= (v_1, v_2) - c(v_1, w)(w, v_2) - c(v_2, w)(v_1, w) = (v_1, v_2).$$

Lemma (2.10) *Let the scalar product by non-degenerate symplectic. If v_1, v_2 and w_1, w_2 are hyperbolic pairs in V, then there is a product g of symplectic transvections such that $g : v_1 \mapsto w_1, v_2 \mapsto w_2$.*

Proof: At first we show that we can find $h : v_1 \mapsto w_1$. If $(v_1, w_1) \neq 0$, then $vT = v + \frac{1}{(v_1, w_1)}(v, v_1 - w_1)(v_1 - w_1)$ defines a symplectic transvection such that $v_1T = w_1$. If $(v_1, w_1) = 0$, then choose u such that $(v_1, u) \neq 0 \neq (w_1, u)$ and apply the above procedure twice. As we have found $h : v_1 \mapsto w_1$ we can assume without restriction $v_1 = w_1$. If $(v_2, w_2) \neq 0$ we can use the symplectic transvection defined by $vT = v + \frac{1}{(v_2,w_2)}(v, v_2 - w_2)(v_2 - w_2)$ and are done. Assume $(v_2, w_2) = 0$. Then $v_1, v_1 + v_2$ is a hyperbolic pair and we can apply the preceding case twice.■

2.7.1 Proof of Witt's theorem

We use induction on $dim(U_1)$.

- Let V be symplectic, U_1 non degenerate.

Write $U_1 = H \perp W$. By Lemma (2.10) there is an isometry α of V such that $\alpha : H \longrightarrow H^h$. As W^h and W^α are both in $(H^h)^\perp$ we can use induction and find an isometry β of $(H^h)^\perp$ such that $wh = w\alpha\beta$ for all $w \in W$. After extension to V the isometry $\alpha\beta$ does the job.

- Let V be symmetric or unitary, U_1 non degenerate.

U_1 has an orthonormal basis $u_1, \ldots, u_m$. We have proved that there is an isometry α of V such that $\alpha : u_m \mapsto u_m^h$. By induction we find an isometry β of $(u_m^h)^\perp$ such that $\beta : u_i^\alpha \mapsto u_i^h$. Then $\alpha\beta$ does the job.

- Let U_1 be degenerate.

Put $U_1 = Rad(U_1) \perp W$, where $rad(U_1) =< x_1, \ldots, x_m >$, analogously for U_2. Embed U_i in non-degenerate spaces:

$$U_1 \subset < U_1, y_1, \ldots, y_m > = < x_1, y_1 > \perp \ldots \perp < x_m, y_m > \perp W,$$

analogously for U_2. Define an isometry between these spaces such that $y_i \mapsto y_i'$, which restricts to h. This isometry can be extended to an isometry of V. We are done.■

Witt's theorem states that the group of isometries operates transitively on the set of subspaces of a given isometry type. We mention a number of important corollaries:

Corollary (2.2) *Under the assumptions of Theorem (2.8) the following hold:*

1. *If $U_1, U_2 \subset V$ are isometric, then also $U_1^\perp$ and $U_2^\perp$ are isometric.*

2. *The* **cancellation theorem:** *if $V = U_1 \perp W = U_2 \perp W'$ and U_1, U_2 are isometric, then W, W' are isometric.*

3. *The* **index:** *Every maximal totally isotropic subspace of V has the same dimension $ind(V)$.*

4. *Each isometry of a symmetric non-degenerate scalar product in odd characteristic is a product of reflections.*

5. *Each element of $Sp_{2m}(q)$ is a product of symplectic transvections.*

Proof: Only the last two items deserve a proof. We concider only the symmetric case, the symplectic case being analogous. Write $V = H_1 \perp \ldots \perp H_{m-1} \perp V_0$, where V_0 either is a hyperbolic plane H_m or a 1-dimensional anisotropic space $< v >$. Let g be an isometry of V. By Lemma (2.7) we can find a product of reflections which agrees with g on H_1. Calculate in $(H_1^g)^\perp$. It is to be observed that a reflection on a space W, extended by the identity on U, is a reflection on $U \perp W$. Ultimately one is reduced to the trivial case $V = V_0$.■

We continue with the orthogonal groups in odd characteristic. If the isometry g is represented by matrix T and A is the Gram matrix with respect to the same basis, then $TAT^t = A$. This shows $det(T) = \pm 1$. As reflections have determinant -1 we conclude that the group SO_n has index 2 in the orthogonal group. One can construct a smaller normal subgroup:

There are two types of 1-dimensional non-isotropic subspaces, according to the cases when (v, v) is a square or a nonsquare. Accordingly there are two essentially different types of reflections S_v, the quadratic type and the nonquadratic type. Let $g \in SO(V)$. Then $g = s_1 s_2 \ldots s_r$, where the s_i are reflections and r is even. Using the **Clifford algebra** one can construct a homomorphism, the **Spinor norm** : $SO(V) \longrightarrow \mathbb{F}_q^*/(\mathbb{F}_q^*)^2 = \{Q, NQ\}$. The kernel of the Spinor norm is by definition the normal subgroup $\Omega(V)$ of $SO(V)$, of index 2. See [1], chapter V, paragraphs 4 and 5. Here $g \in \Omega(V)$ if and only if an even number of the s_i have type NQ (nonsquare). The equation $TAT^t = A$ shows that $Z \cap O(V) = \{1, -1\}$. If n is odd, then clearly $Z \cap SO(V) = 1$. Let $n = 2m$ be even. An orthonormal basis leads to $-1 = \prod_{i=1}^n S_{v_i}$. When is this in $\Omega(V)$? We see that this is equivalent with

$det(A)$ being a square and with $D(V) = 1$. Let $V = H_1 \perp \ldots \perp H_m$ (of index m). Then $-I \in \Omega(V)$ if and only if either q is 1(mod 4) or m is even. In the case when $V = H_1 \perp \ldots \perp H_{m-1} \perp V_0$ (of index $m-1$) we have $-I \in \Omega(V)$ if and only if q is 3(mod 4) **and** m is odd. The projective orthogonal group is defined as

$$P\Omega(V) = \Omega(V)/(Z \cap \Omega(V)).$$

Comparison with the order of the full orthogonal group yields the following formulas for the order of the projective group:

Lemma (2.11) *In odd characteristic the orders of the projective orthogonal groups are as follows:*

$$|P\Omega_{2m+1}(q)| = |\Omega_{2m+1}(q)| = \frac{1}{2} q^{m^2} \prod_{i=1}^{m} (q^{2i} - 1).$$

$$|P\Omega^+_{2m}(q) = \frac{1}{(4, q^m - 1)} q^{m(m-1)}(q^m - 1) \prod_{i=1}^{m-1} (q^{2i} - 1)$$

$$|P\Omega^-_{2m}(q) = \frac{1}{(4, q^m + 1)} q^{m(m-1)}(q^m + 1) \prod_{i=1}^{m-1} (q^{2i} - 1)$$

2.8 Symmetric scalar products in even characteristic

In characteristic 2 the notions of symmetry and skew symmetry coincide. What happens on the diagonal? Let $(,)$ be a symmetric nondegenerate scalar product, G the group of isometries. If $(v, v) = 0$ for all $v \in V$, then $(,)$ is symplectic. Note that when $(v, v) = 0 = (w, w)$, then the subspace $< v, w >$ is symplectic. Let $V_0 = \{v \mid (v, v) = 0\}$. Then V_0 is a subspace. Let $(v, v) = \alpha \neq 0, (w, w) = \beta \neq 0$. Then $(v + \sqrt{alpha/\beta} w, v + \sqrt{alpha/\beta} w) = 0$. It follows that $codim(V_0) \leq 1$. If $V_0 = V$, then we have a symplectic space. Let $codim(V_0) = 1$. Then V_0 inherits the structure of a (degenerate?) symplectic space.
Let $n = 2m+1$. We have $dim(V_0) = 2m$. If V_0 was degenerate, then its radical would have dimension ≥ 2, which would lead to a nontrivial radical of V. We conclude that V_0 is nondegenerate in this case. This shows $V = V_0 \perp < v >$

and G has $SP_{2m}(q)$ as a direct factor.
Let $n = 2m$. Then $dim(V_0) = 2m-1$ and V_0 must have a radical. This radical must be 1-dimensional: $rad(V_0) =< v_0 >$. We have $V_0 = W_0 \perp < v_0 >$, where W_0 is a non-degenerate symplectic space. It follows $V = W_0 \perp < v_0, v >$, where $W_0 = V_0 \cap v^\perp$, $(v, v) = (v_0, v) = 1$. The group G operates on V_0 and on $< v_0 >$. The space $V_0 / < v_0 >$ is endowed with a nondegenerate sypllectic scalar product. We obtain $Sp_{2m-2}(q)$ as a factor group of G. Let K be the kernel. Every element $g \in G$ must afford an operation $v \mapsto \alpha v + x$, where $x \in V_0$. Let $v \notin V_0$. Choose $(v, v) = 1$. Then $1 = (v, v) = (\alpha v + x, \alpha v + x) = \alpha^2$. It follows $\alpha = 1$. If $g : v_0 \mapsto \beta v_0$, then $1 = (v_0, v) = (\beta v_0, v + x) = \beta$. It follows that g fixes v_0. The kernel K consists of those elements $g \in G$ which operate trivially on $V_0 / < v_0 >$. Let $K_0 \leq K$ consist of the elements operating trivially on V_0. The group K/K_0 is clearly an elementary abelian group $E(q^{2m-2})$ of order q^{2m-2}. If $g \in K_0$, then g operates on $< v, v_0 >= W_0^\perp$. It follows that K_0 is elementary abelian of order q. It particular we see that g does not give us any new simple group. In order to obtain the orthogonal groups in characteristic 2 one has to use quadratic forms.

2.9 Quadratic forms and orthogonal groups in characteristic 2

The idea is to associate to the scalar product $(,)$ the function $Q : V \longrightarrow F$, which is defined by $Q(v) = (v, v)$ (an analog to the squared length of vector v. In the symplectif case this is not interesting as $Q = 0$ all the time. In the unitary case we have $Q(x) \in \mathbb{F}_q$. As the ground field is $\mathbb{F}_{q^2}$ we see in particular that we cannot recover $(,)$ from the knowledge of Q. This is not very interesting. Let $(,)$ be symmetric in odd characteristic. Then Q satisfies

$$Q(\lambda x) = \lambda^2 Q(x)$$

$$Q(x + y) = Q(x) + Q(y) + 2(x, y).$$

In particular we recover the scalar product from the quadratic form. The two theories (symmetric scalar products and quadratic forms) are equivalent in this case. In characteristic 2 the factor of 2 is a real nuisance. This motivates the following definition:

Definition (2.3) *Let $F = \mathbb{F}_q$, where q is a power of 2. $Q : V \longrightarrow F$ is a* **quadratic form** *with respect to the symplectic scalar product $(,)$ if the following are satisfied:*

- $Q(\lambda x) = \lambda^2 Q(x)$ *for all* $x \in V, \lambda \in F$.
- $Q(x + y) = Q(x) + Q(y) + (x, y)$ *for all* $x, y \in V$.

We note that $(,)$ is necessarily symplectic as $(x, x) = Q(2x) + Q(x) + Q(x) = 0$. Let $dim(V) = n$. It should be noted that any homogeneous quadratic polynomial in n indeterminates with coefficients in F yields a quadratic form.
Let $V_0 = Rad(V)$ with respect to $(,)$. If $x, y \in V_0$, then $Q(\alpha x + \beta y) = \alpha^2 Q(x) + \beta^2 Q(y)$. It follows that the restriction h of Q to V_0 is semilinear with respect to the Frobenius automorphism $\alpha \mapsto \alpha^2$. We call the quadratic form Q **nondegenerate** if $Ker(h) = 0$. Let $d = dim(V_0)$ be the **defect** of Q. If Q is nondegenerate, then $d \leq 1$. We see that $d = 1$ if n is odd, and $d = 0$ if n is even. A vector x is **singular** if $Q(x) = 0$. A subspace $U \subset V$ is **singular** if $Q(u) = 0$ for all $u \in U$. A 2-dimensional space $H =< u, v >$ is a **quadratic hyperbolic space** if $Q(u) = Q(v) = 0, (u, v) = 1$. It follows $Q(\alpha u + \beta v) = \alpha\beta$. In particular H is a hyperbolic plane with respect to $(,)$.

Lemma (2.12) *Let (V, Q) be a quadratic space, $0 \neq v \in V \setminus Rad(V), Q(v) = 0$. There exists an $w \in V$ such that $Q(w) = 0, (v, w) = 1$. The space $H =< v, w >$ is a quadratic hyperbolic plane and we have $V = H \perp H^\perp$, where $d(H^\perp) = d(V)$ and $H^\perp$ is nondegenerate.*

Proof: As $v \notin Rad(V)$ there is some $w' \in V$ such that $(v, w') = 1$. Put $w = w' + \alpha v$. Then $Q(w) = Q(w') + \alpha$. We can choose α such that $Q(w) = 0$. The remaining claims are obvious.■

As usual we can use induction and obtain a structural description:

Lemma (2.13) *Let $U =< u_1, \ldots, u_m >$ be a maximal singular subspace of the nondegenerate quadratic space (V, Q). There exist vectors $v_1, \ldots, v_m$ such that $V =< u_1, v_1 >\perp \ldots \perp< u_m, v_m >\perp V_0$, where $< u_i, v_i >$ is a quadratic hyperbolic plane and $V_0 = W_0 \perp Rad(V)$. Here $Rad(V)$ has by definition dimension $d(V)$ (0 or 1) and W_0 is* **asingular** *meaning that $Q(w) \neq 0$ whenever $0 \neq w \in W_0$.*

Theorem (2.9) *Let (V, Q) be an asingular quadratic space in characteristic 2. The following hold:*

1. *$dim(V) \leq 2$.*

2. *If (V, Q) is nondegenerate, then either $V =< v_0 >, Q(v_0) = 1$ or $dim(V) = 2, d(V) = 0$ and*

$$Q(\alpha v + \beta w) = \alpha^2 + a\beta^2 + \alpha\beta,$$

where $a \in \mathbb{F}_q$ cannot be written in the form $a = b + b^2$.

3. *Asingular nondegenerate 2-dimensional spaces (V, Q) are uniquely determined up to isometry.*

Proof: Assume $dim(V) = 3$. Pick $0 \neq v \in V$. There is some $w \in v^\perp \setminus < v >$. It follows $Q(v + \alpha w) = Q(v) + \alpha^2 Q(w)$. As $Q(w) \neq 0$ we can choose α such that $Q(v + \alpha w) = 0$, contradiction.
The 1-dimensional case of 2. is obvious. Let $dim(V) = 2$. As certainly $d(V) < 2$ it follows $d(V) = 0$. In particular V is a hyperbolic plane with respect to $(,)$. Let $V =< v, w >$, where we choose notation such that $Q(v) = 1, (v, w) = 1$. Put $Q(w) = a$. Then $Q(\alpha v + \beta w) = \alpha^2 + \beta^2 a + \alpha\beta$. This expression has to be nonzero whenever $(\alpha, \beta) \neq (0, 0)$. Division by α^2 shows that the general case is indeed equivalent to the case $\beta = 1$. We need $\alpha^2 + \alpha + a \neq 0$ for every $\alpha \in \mathbb{F}_q$.
3. An element a satisfying the conditions of 2. can always be chosen. In fact, consider the mapping f, where $f(\alpha) = \alpha^2 + \alpha$. Then β is an $\mathbb{F}_2$-linear homomorphism : $\mathbb{F}_q \longrightarrow \mathbb{F}_q$. We have $ker(f) = \{0, 1\}$. As $ker(f)$ is 1-dimensional we have that $f(\mathbb{F}_q)$ is a hyperplane (as $\mathbb{F}_2$-vectorspaces). If we choose $a \in \mathbb{F}_q \setminus f(\mathbb{F}_q)$, then $\mathbb{F}_q$ is the disjoint union of $f(\mathbb{F}_q)$ and $f(\mathbb{F}_q) + a$. Put $w' = w + \alpha v$. Then $(v, w') = 1$ and $Q(w') = a + \alpha^2 + \alpha$ runs through $f(\mathbb{F}_q) + a$. This also shows the uniqueness.■

The condition in part 2. of the preceding Theorem is not as artificial as it might seem. In fact, let $tr : \mathbb{F}_q \longrightarrow \mathbb{F}_2$ be the **absolute trace.** As $tr(\alpha) = tr(\alpha^2)$ we see that elements of the form $\alpha + \alpha^2$ have trace 0. The proof of part 2. shows that this characterizes the elements of trace 0. This is a special case of a theorem, which is valid for cyclic Galois extensions. Its

multiplicative counterpart is known as **Hilbert Satz 90,** see for example [2], part I, paragraph 7. The condition on $a \in \mathbb{F}_q$ as given in 2. of Theorem (2.9) is therefore equivalent to $tr(a) = 1$.
Let now $d = 1$, hence $n = 2m+1, V = H_1 \perp \ldots \perp H_m \perp < v_0 >$, where the $H_i = < u_i, v_i >$ are quadratic hyperbolic planes, $Q(v_0) = 1$. In particular the isometry type is uniquely determined. We denote the isometry group by $G = O_{2m+1}(q)$. Clearly G fixes v_0. Let K be the kernel of the operation of G on $V/ < v_0 >$. If $g \in K$, then $g : u_i \mapsto u_i + \alpha v_0$. It follows $0 = Q(u_i) = 0 + \alpha^2$. We see that g is the identity, hence $K = 1$. As $V/ < v_0 >$ carries a nondegenerate symplectic scalar product it follows that G is embedded in the group $Sp_{2m}(q)$. Let now $\tilde{g} \in Sp(V/ < v_0 >)$. Then $\tilde{g}$ maps the hyperbolic plane $H_i + < v_0 > / < v_0 >$ onto a hyperbolic plane $< u_i' + < v_0 >, v_i' + < v_0 >>$. We wish to find $\alpha, \beta \in \mathbb{F}_q$ such that $< u_i' + \alpha v_0, v_i' + \beta v_0 >$ is a quadratic hyperbolic plane. We have to solve: $0 = Q(u_i' + \alpha v_0) = Q(u_i') + \alpha^2$ and $0 = Q(v_i' + \beta v_0) = Q(v_i') + \beta^2$, which is uniquely solvable. We conclude

$$O_{2m+1}(q) \cong Sp_{2m}(q) \text{ in characteristic two}$$

Let now $d = 0, n = 2m$. It follows that V is a non-degenerate symplectic space. As a quadratic space we obtain one of two possible isometry types.

$$V = H_1 \perp \ldots \perp H_m \text{ (the (+)type)},$$

where the H_i are quadratic hyperbolic planes, or

$$V = H_1 \perp \ldots \perp H_{m-1} \perp V_0 \text{ (the (-)type)},$$

where V_0 is a 2-dimensional asingular quadratic space. The corresponding groups are denoted by $O^+_{2m}(q)$ and $O^-_{2m}(q)$, respectively.
Denote by $f(m,c)$ the number of vectors $v \in V^+(2m,q)$ satisfying $Q(v) = c$, by $h(m,c)$ the corresponding number in $V^-(2m,q)$. We obtain the same formulas as in the case of odd characteristic, and in the same manner. In fact

$$f(m,1) = q^{m-1}(q^m - 1), f(m,0) = q^{m-1}(q^m + q - 1),$$
$$h(m,1) = q^{2m-1} + q^{m-1}, h(m,0) = q^{m-1}(q^m - q + 1).$$

We observe that in both cases the group G is transitive on quadratic hyperbolic pairs. In the same spirit we see that G is transitive on the pairs (u,v), where $(u, v) = 1, Q(u) = 1, Q(v) = a, tr(a) = 1$. Remember that $< u, v >$ is then asingular of dimension 2. Likewise G is transitive on the $v \in V$ satisfying $Q(v) = c$, where $c \neq 0$ is fixed (in fact, we can assume $c = 1$ and embed v in a hyperbolic plane).

Theorem (2.10) ('Witt's theorem', due to Arf) *Let (V, Q) be a nondegenerate quadratic space, d(V)=0, in characteristic 2, hence $V = V_{2m}^{+}(q)$ or $V = V_{2m}^{-}(q)$. If $h : U_1 \longrightarrow V_1$ is an isometry between subspaces of V, then there is an isometry of V, which restricts to h.*

Proof: Analogous to the case of odd characteristic. If U_1 is nondegenerate we have proved this already. The reduction of the general case to the nondegenerate case works as before.■

As $|O_2^{+}(q)| = 2(q-1)$ and $|O_2^{-}(q)| = 2(q+1)$ we obtain the same formulas for the orders of the groups $O_{2m}^{\pm}(q)$ as in odd characteristic. The Clifford algebra allows the conctruction of a **Dickson invariant** : $O_{2m}^{\epsilon}(q) \longrightarrow \mathbb{F}_2$. The kernel of the Dickson invariant is denoted by $SO_{2m}^{\epsilon}(q)$, has index 2 in the full orthogonal group and is usually a simple group.

2.9.1 The 3-dimensional case in characteristic 2

Consider the general quadratic form

$$Q(X_1, X_2, X_3) = a_1X_1^2 + a_2X_2^2 + a_3X_2^2 + a_{12}X_1X_2 + a_{13}X_1X_3 + a_{23}X_2X_3$$

in characteristic 2. The corresponding symplectic form is given by

$$(x, y) = a_{12}(x_1y_2 + x_2y_1) + a_{13}(x_1y_3 + x_3y_1) + a_{23}(x_2y_3 + x_3y_2).$$

We assume $(a_{12}, a_{13}, a_{23}) \neq (0, 0, 0)$. The radical $V_0 = Rad(V)$ with respect to the symplectic scalar product is then 1-dimensional and we have $V_0 = (a_{23} : a_{13} : a_{12})$. The quadratic form Q will be degenerate if and only of $Q(V_0) = 0$. This is equivalent to

$$a_1a_{23}^2 + a_2a_{13}^2 + a_3a_{12}^2 + a_{12} \cdot a_{13} \cdot a_{23} = 0.$$

Assume Q is nondegenerate. We know that $V(Q)$, the set of singular points in $PG(2, q)$, has $q+1$ points and forms an oval (no three on a line). Moreover a line containing two singular points corresponds to a quadratic hyperbolic plane and can therefore not contain V_0. It follows that the point V_0 is the intersection of the tangents to $V(Q)$. In geometry V_0 is known as the **nucleus** of $V(Q)$. The point set $V(Q) \cup \{V_0\}$ is a **hyperoval** ($q+2$ points, no three on a line).

2.10 A table of groups, orders and isomorphisms

The first Table presents the family of classical simple groups and their orders:

name	restrictions	order
A_n	$n \geq 5$	n!/2
$L_n(q)$	$n \geq 2, (n,q) \neq (2,2), (2,3)$	$\frac{1}{(n,q-1)} q^{n(n-1)/2} \prod_{i=2}^{n} (q^i - 1)$
$S_{2n}(q)$	$n \geq 2, (n,q) \neq (2,2)$	$\frac{1}{(2,q+1)} q^{n^2} \prod_{i=1}^{n} (q^{2i} - 1)$
$U_n(q) = PSU_n(q^2)$	$n \geq 3, (n,q) \neq (3,2)$	$\frac{1}{(n,q+1)} q^{n(n-1)/2} \prod_{i=2}^{n} (q^i - (-1)^i$
$\Omega_{2n+1}(q)$	q odd,$n \geq 3$	$\frac{1}{2} q^{n^2} \prod_{i=1}^{n} (q^{2i} - 1)$
$P\Omega_{2n}^{\epsilon}(q)$	$\epsilon = \pm 1, n \geq 4$	$\frac{1}{(4,q^n-\epsilon)} q^{n(n-1)} (q^n - \epsilon) \prod_{i=1}^{m-1} (q^{2i} - 1)$

We note that the groups $S_{2n}(q)$ and $\Omega_{2n+1}(q)$ form two infinite families of simple groups with the same group orders. These groups are not isomorphic when q is odd. In the following table we list the isomorphisms of groups in the main table:

isomorphies	group order
$A_5 \cong L_2(4) \cong L_2(5)$	60
$A_6 \cong L_2(9)$	$2^3 \cdot 3^2 \cdot 5 = 360$
$A_8 \cong L_4(2)$	$2^6 \cdot 3^2 \cdot 5 \cdot 7$
$L_2(7) \cong L_3(2)$	$2^3 \cdot 3 \cdot 7 = 168$
$S_4(3) \cong U_4(2)$	$2^6 \cdot 3^4 \cdot 5$

Here are more isomorphisms between (mostly simple) groups:

isomorphisms between groups
$L_2(q) \cong U_2(q) \cong S_2(q) \cong \Omega_3(q)$
$S_{2n}(q) \cong \Omega_{2n+1}(q)$, even q
$P\Omega_4^+(q) \cong L_2(q) \times L_2(q)$
$P\Omega_4^-(q) \cong L_2(q^2)$
$P\Omega_5(q) \cong S_4(q)$
$P\Omega_6^+(q) \cong L_4(q)$

Let us see that we understand the isomorphism $P\Omega_6^+(q) \cong L_4(q)$. We start from a 4-dimensional vector space $V =< e_1, e_2, e_3, e_4 >$. Consider the second homogeneous component of the exterior algebra:

$$W = V^{(2)} =< e_1 \wedge e_2, e_1 \wedge e_3, e_1 \wedge e_4, e_2 \wedge e_3, e_2 \wedge e_4, e_3 \wedge e_4 > .$$

Put $v_1 = e_1 \wedge e_2, v_2 = e_1 \wedge e_3, v_3 = e_1 \wedge e_4, v_4 = e_2 \wedge e_3, v_5 = e_2 \wedge e_4, v_6 = e_3 \wedge e_4$. We have a natural symmetric scalar product $(,)$ on W, given by

$$w \wedge w' = (w, w')e_1 \wedge e_2 \wedge e_3 \wedge e_4 + \dots$$

This scalar product is respected by $SL(V)$. It is nondegenerate of index 3, as we see from

$$W =< v_1, v_6 > \perp < v_2, v_5 > \perp < v_3, v_4 > .$$

In odd characteristic this shows $SL_4(q) \subseteq O_6^+(q)$. The isomorphism now follows from the simplicity of the groups involved. Let now the characteristic be 2. Consider the quadratic form given by $Q(v_i) = 0, i = 1, 2, \dots, 6$. The group $SL_4(q)$ respects this quadratic form. Let $f \in SL_4(q)$ be given by matrix A. Then $v_1 = e_1 \wedge e_2$ is mapped to $(\sum_k a_{1k}e_k) \wedge (\sum_l a_{2l}e_l) = \sum_{r<s} \alpha_{rs}e_r \wedge e_s$, where $\alpha_{rs} = a_{1r}a_{2s} + a_{1s}a_{2r}$. We have to check that $Q(\sum_{i=1}^6 \alpha_i v_i) = 0$. In fact, we have

$$Q(\sum_{i=1}^{6} \alpha_i v_i = \alpha_{1,2}\alpha_{3,4} + \alpha_{1,3}\alpha_{2,4} + \alpha_{1,4}\alpha_{2,3} = 0.$$

For the last identity check the business of **Plücker coordinates.** We have $SL_3(q) \subseteq O_6^+(q)$ again.

Bibliography

[1] E. Artin, *Geometric Algebra.*

[2] I.Kaplansky, *Fields and Rings, Chicago Lectures in Mathematics, The University of Chicago Press, Chicago and London, 1969.*