Introduction to Group Theory and Applications
Gruppentheorie mit Anwendungen in der Kombinatorik

Jürgen Bierbrauer

September 2, 2000

Contents

Chapter 1

Introduction to Group Theory

1.1 Definition of groups

We start with a formal definition.

1.1 Definition. *Let G be a set and let a product operation* $: G \times G \longrightarrow G$ *be defined. Then* $(G, \cdot)$ *is a* **group** *if the following hold:*

- $g_1(g_2g_3) = (g_1g_2)g_3$ *for all* $g_i \in G$ *(***associativity***).*
- *There is an element* $e \in G$ *(the* **neutral element***) such that* $eg = ge = g$ *for all* $g \in G$*.*
- *For every* $g \in G$ *there is an element* $g^{-1} \in G$ *(the* **inverse element***) such that* $gg^{-1} = g^{-1}g = e$*.*

Observe that the neutral element is uniquely determined (if e' is a neutral element, then by definition $ee' = e = e'$). We also write the neutral element as 1. A first general result are the **cancellation laws,** which hold in any group.

1.2 Theorem (cancellation laws). *Let G be a group. Then the following hold:*

- *If* $ax = ay$*, then* $x = y$
- *If* $xa = ya$*, then* $x = y$*.*

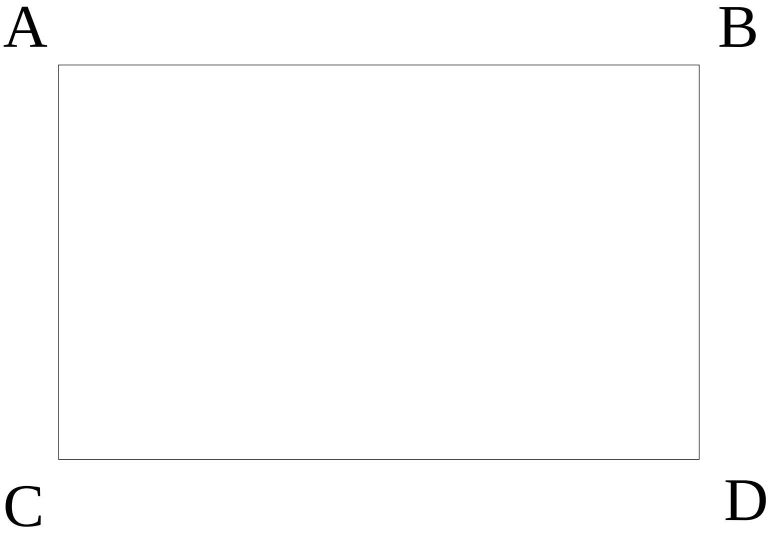


Figure 1.1: The rectangular playing card

Proof. Assume $ax = ay$. Multiply by the inverse a^{-1} from the left and use associativity:

$$x = a^{-1}ax = a^{-1}ay = y.$$

The same procedure works in the other case. $\square$

As a consequence we see that every element a has a **uniquely determined** inverse a^{-1} and that equations $ax = b$ and $xa = b$ have unique solutions x ($x = a^{-1}b$ in the first case, $x = ba^{-1}$ in the second case).
A group G is **finite** if the set G is finite. The cardinality of G is then called the **order** of the group. A group G is **commutative** (or **abelian**) if $ab = ba$ for all $a, b \in G$. If $ab = ba$ we also say that a and b **commute.**

It is one objective of this course to show that all sorts of algebraic, combinatorial or geometric structures give rise to groups in a natural way. Group theory helps understanding the situation in all these seemingly diverse cases. Our first class of examples are groups of symmetry.

1.2 Groups of symmetry

As a toy example consider a rectangular playing card. The **symmetry group** of the card is defined as the set of all permutations of the corners

A, B, C, D which have the property that the card looks alike before and after the permutation is applied. Recall that a **permutation** of a set is a bijective (onto and one-to-one) mapping of the set. There are three types of **pairs of corners** in our card: those pairs connected by a long edge, those connected by a short edge and those not connected by an edge. We can reformulate our condition: a permutation of the corners $\{A, B, C, D\}$ is a **symmetry** if and only if

- the image of any long edge is a long edge,
- the image of any short edge is a short edge, and
- the image of any non-edge is a non-edge

Let us consider the permutation $\begin{pmatrix} A & B & C & D \\ A & C & D & B \end{pmatrix}$. This notation means that the permutation maps $A \mapsto A, B \mapsto C, C \mapsto D, D \mapsto B$. Is this a symmetry of the rectangular playing card or not? No, because the pair $\{A, B\}$ of corners (a long edge) is mapped to $\{A, C\}$ (a short edge). Let us determine all symmetries of our card: one symmetry is always there, the permutation $e = \begin{pmatrix} A & B & C & D \\ A & B & C & D \end{pmatrix}$, which does nothing (the neutral element). Anything else? Geometric intuition will help: if we imagine a horizontal axis through the centers of edges AC and BD and we rotate our card about that axis (in 3-space), we obtain the symmetry $a = \begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix}$. An analogous rotation about a vertical axis yields $b = \begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix}$. Another idea is to reflect at the center of the card. This gives us the symmetry $c = \begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix}$. Is this all? Yes. It is not hard to convince ourselves that any symmetry is uniquely determined as soon as we know the image of A. If for example $A \mapsto D$, then B, the unique partner forming a long edge with A, must be mapped to C, the unique partner to form a long edge with D, and so forth.

1.3 Theorem. *The symmetry group of the rectangular card is the group $V = \{e, a, b, c\}$ of order 4.*

This is the first group we actually saw, and it is an interesting group. Why is it a group and what is the group operation? Each symmetry is a mapping, more specifically a permutation. When two permutations are given, we can form the composite function. If each of f and g is a symmetry, then also the compositions $f \circ g$ and $g \circ f$ are symmetries. We can check the group axioms from Definition 1.1. Associativity is obvious as composition of functions is associative. The neutral element is the lazy permutation e, the inverse f^{-1} of permutation (symmetry) f is the inverse mapping.

1.4 Definition. *We define the* **product** *of two permutations (on the same set) as the composition of functions. Here we adopt the convention that fg is the composite function, which is obtained by applying f first and then g.*

With this terminology we have for example $ab = c$ (in words: if we apply first permutation a, then b, the result is permutation c.) More in general we see, that the product of any two different non-neutral elements of V is the third.

Here is another example, the quadratic card.

This time there are only edges and non-edges. A symmetry is a permutation of the corners, which satisfies

- the image of any edge is an edge, and
- the image of any non-edge is a non-edge

In fact, it suffices that the first condition be satisfied. If the image of every edge is an edge, then the non-edges will automatically be mapped to non-edges. It is also clear, that the group V from Theorem 1.3 is contained in the symmetry group of the quadratic card. Is that all? No, here is a symmetry of the quadratic card, which is not a symmetry of the rectangular card: $u = \begin{pmatrix} A & B & C & D \\ A & C & B & D \end{pmatrix}$. By now we know that the symmetries form a group, with the group product from Definition 1.4. As we already have the symmetries from V, each new symmetry like u gives us at least four new symmetries: $u, v = ua, w = ub, x = uc$. These must be different of each other and of the elements of V, because of the cancellation laws (see Theorem 1.2). We obtain $v = \begin{pmatrix} A & B & C & D \\ C & A & D & B \end{pmatrix}$, $w = \begin{pmatrix} A & B & C & D \\ B & D & A & C \end{pmatrix}$, $x = \begin{pmatrix} A & B & C & D \\ D & B & C & A \end{pmatrix}$. We have eight symmetries so far. This is all. In

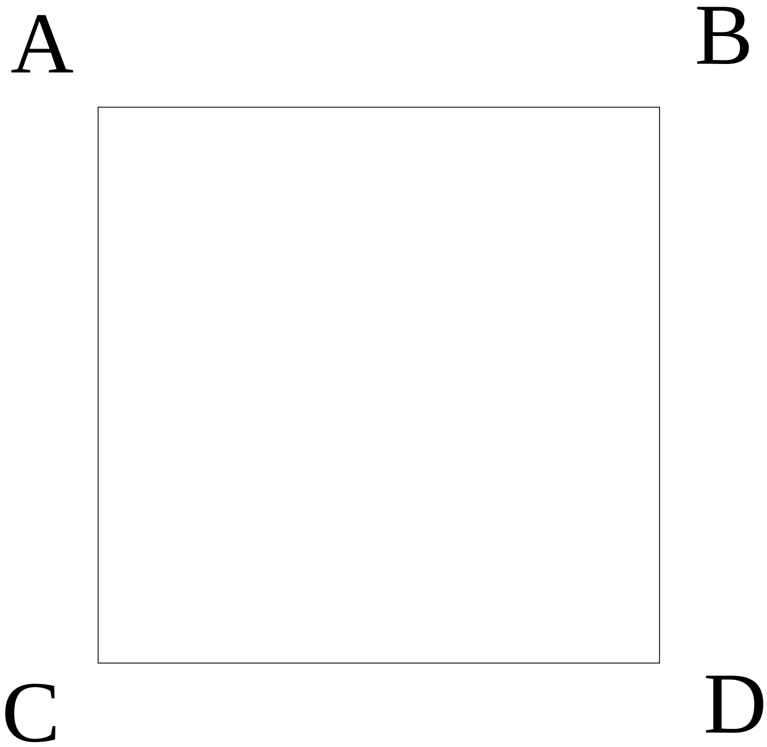


Figure 1.2: The quadratic playing card

fact, we can check that if we know the image of A there are at most two symmetries achieving that. An upper bound on the number of symmetries is therefore $4 \cdot 2 = 8$ and we have already eight symmetries. In later chapters we will learn more efficient and secure ways to determine symmetry groups.

1.5 Theorem. *The symmetry group of the square playing card is the following group of order 8:*

$$D_8 = \{e, a, b, c, u, v, w, x\}$$

1.3 Group tables

If we want complete information about all elements of a group and all group operations (products of any two group elements), we can collect this information in a **group table.** Here is the group table of the group V from Theorem 1.3:

Group table of V				
	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

For example, $ab = c$. As the group table is symmetric about the main diagonal, V is abelian. As the entries on the main diagonal are e, we have that the square of any group element is e. Here is the group table of D_8 :

Group table of D_8								
	e	a	b	c	u	v	w	x
e	e	a	b	c	u	v	w	x
a	a	e	c	b	w	x	u	v
b	b	c	e	a	v	u	x	w
c	c	b	a	e	x	w	v	u
u	u	v	w	x	e	a	b	c
v	v	u	x	w	b	c	e	a
w	w	x	u	v	a	e	c	b
x	x	w	v	u	c	b	a	e

The cancellation laws show that in each row and in each column of a group table every group element appears exactly once. We check that this is true in the case of groups V and D_8. For larger groups it is clearly impractical to write down group tables.

1.4 Permutations and the symmetric groups

We have seen that symmetry groups consist of permutations. Clearly the set of all permutations of a set also forms a group. We may see this as a symmetry group as well, where the underlying set has no structure. The group of all permutations is known as the symmetric group.

1.6 Definition (symmetric group). *Let Ω be a set. The permutations of Ω form a group, the* **symmetric group** *S_Ω. As before group multiplication is composition of functions. If Ω is a finite set of n elements we also write S_n.*

It is an easy combinatorial exercise to see that an n-element set has $n! = n(n-1)(n-2)\cdot\dots\cdot 2\cdot 1$ permutations. The order of S_n is therefore $\mid S_n \mid= n!$ In particular

$$|S_2| = 2,\ |S_3| = 6,\ |S_4| = 24,\ |S_5| = 120, \dots$$

As we will use permutations a great deal we need a more efficient way of writing them. As an example consider the permutation $c = \begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix}$.

It is clearly wasteful to write every symbol of $\Omega = \{A, B, C, D\}$ twice. Here is a more effective notation. Observe that

$$c : A \mapsto D, B \mapsto C, C \mapsto B, D \mapsto A.$$

Let us reorder this in the following way: whenever we have found an image let us check what happens to the image next. This gives us the representation:

$$c : A \mapsto D \mapsto A,\ B \mapsto C \mapsto B.$$

The shorter notation is $c = (A, D)(B, C)$.

1.7 Definition. *Let $a_1, a_2, \ldots, a_n$ be n different objects. We denote the permutation*

$$a_1 \mapsto a_2 \mapsto a_3 \mapsto \ldots \mapsto a_n \mapsto a_1$$

by $(a_1, a_2, a_3, \ldots, a_n)$ and call this an n-cycle or a cycle of length n. The 2-cycles are also known as **transpositions.**

A 1-cycle is simple a fixed element (mapped to itself).

1.8 Lemma. *Every permutation can be written as a product of disjoint cycles.*

This is best seen by examples. The permutation c considered above turned out to be the product of two transpositions (2-cycles). Naturally we call cycles disjoint if they do not have symbols in common. As before the product in the symmetric group is the composition of functions. Consider the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$. This is the mapping

$$1 \mapsto 2 \mapsto 4 \mapsto 1, 3 \mapsto 5 \mapsto 3.$$

In our short cycle notation this becomes $(1, 2, 4)(3, 5)$, the product of a 3-cycle and a transposition. It is obvious that this way of writing a permutation as a product of disjoint cycles is essentially uniquely determined. Why only essentially? Clearly it does not matter in which order the cycles appear: $(1, 2, 4)(3, 5) = (3, 5)(1, 2, 4)$, and each individual cycle can be written with any of its symbols as the first symbol:

$$(1, 2, 3, 4) = (2, 3, 4, 1) = (3, 4, 1, 2) = (4, 1, 2, 3).$$

Fixed points (1-cycles) are often not written. For example, the element of S_3 mapping $1 \mapsto 3 \mapsto 1, 2 \mapsto 2$ is written as $(1,3)$. Here are all the elements of $S_3 : e, d_1 = (1,2,3), d_2 = (1,3,2), z_1 = (1,2), z_2 = (1,3), z_3 = (2,3)$ (there are two 3-cycles and three transpositions in S_3). Here is the group table:

Group table of S_3						
	e	d_1	d_2	z_1	z_2	z_3
e	e	d_1	d_2	z_1	z_2	z_3
d_1	d_1	d_2	e	z_3	z_1	z_2
d_2	d_2	e	d_1	z_2	z_1	z_3
z_1	z_1	z_2	z_3	e	d_1	d_2
z_2	z_2	z_3	z_1	d_2	e	d_1
z_3	z_3	z_1	z_2	d_1	d_2	e

1.5 Subgroups

Whenever one studies an algebraic structure it is inevitable to study also substructures, factor structures, homomorphisms, isomorphisms and automorphisms. We start with subgroups. The definition is obvious.

1.9 Definition. *Let G be a group. A subset $H \subseteq G$ is a* **subgroup** *if the following hold:*

- *For every $h \in H$ we have $h^{-1} \in H$*
- *For every $h_1, h_2 \in H$ we have $h_1 h_2 \in H$.*

In words: H is a subgroup if it is closed under inverses and products. In particular H is then a group in its own right. We write then $H \leq G$ (admitting the possibility that $H = G$) or $H < G$ (H is a proper subgroup). Observe that every subgroup of G must contain the neutral element e, and e is the neutral element of the subgroup as well. In fact, there are two subgroups which always exist: the identity subgroup $\{e\}$ and the full group G. The two groups considered in Section 1.2 are clearly subgroups of each other: $V < D_8$. This also shows in the group table of D_8 as given in Section 1.3, where we see the group table of V in the top left-hand corner. The group table of S_3 reveals a subgroup $\{e, d_1, d_2\}$ in the top left-hand corner. In fact, we can find more subgroups: $\{e, z_i\}$ is a subgroup of order 2, $i = 1, 2, 3$. All of these subgroups of S_3 have the property that they consist of the powers of one element, where we interpret the 0-th power as e. In fact, this procedure always gives us subgroups:

1.10 Lemma. *Let $g \in G$. Let*

$$\langle g \rangle = \{g^i : i = 0, \pm 1, \pm 2, \dots\}$$

Then $\langle g \rangle$ is a subgroup of G, the subgroup **generated by** *g.*

This is obvious. Observe that g^{-2} for example denotes the inverse of the square of g. In the case when G is a finite group, can we determine the order of the subgroup $\langle g \rangle$? This leads us to the following definition:

1.11 Definition. *Let G be a finite group and $g \in G$. There is a smallest natural number n such that $g^n = e$. We call $n = o(g)$ the* **order** *of the element g.*

In particular we have $o(e) = 1$ and e is the unique element having order 1. Elements of order 2 are known as **involutions.** Let us make sure the Definition 1.11 makes sense at all. Can we guarantee that there is a natural number n such that $g^n = e$? Consider the elements $g, g^2, g^3, g^4, \dots$ These are infinitely many names for certain elements of G. As G is a finite group these elements cannot all be distinct. There must be exponents (natural numbers) $i < j$ such that $g^i = g^j$. Multiplication by g^{-i} yields $g^{j-i} = e$. We have seen that there is some exponent $n = j - i$ such that $g^n = e$. In fact, we can go one step further: Consider the powers of the element g of order n :

$$e = g^0, g, g^2, \dots, g^{n-1}, g^n = e, g^{n+1} = g, \dots$$

We see that the pattern keeps repeating. We have $g^{-1} = g^{n-1}$ and at most n powers of g can really be different. On the other hand, assume $g^i = g^j$, where $0 \leq i < j \leq n - 1$. We would obtain $g^{j-i} = e$, where $0 < j - i < n$, which is impossible by the definition of the order of g. We have seen the following:

1.12 Theorem. *Let g be an element of the finite group $G, o(g) = n$. The subgroup $\langle g \rangle$ has order n. The different powers of g are $e = g^0, g, g^2, \dots, g^{n-1}$ and we have $g^m = e$ if and only if m is a multiple of n.*

Theorem 1.12 explains why we used the notion of **order** with apparently different meanings. We see that the order of an element as in Definition 1.11 really is the order of a subgroup: $o(g) = |\langle g\rangle|$. As an example, consider the element $d_1 = (1,2,3) \in S_3$. It is obvious that we have $o(g) = 3$. The subgroup $\langle d_1\rangle$ generated by d_1 is $\{e, d_1, d_2 = d_1^2\}$, of order 3. In fact, it is clear that an n-cycle has order n.

1.13 Lemma. *The order of an n-cycle is n.*

1.6 Cosets and Lagrange's theorem

In this section we prove our first structural theorem. As a tool in the proof we use the notion of cosets, which will we useful later in the lecture as well.

1.14 Definition (cosets). *Let G be a group, $H \subseteq G$ a subgroup and $g \in G$. The set $Hg = \{hg|h \in H\}$ is a* **right coset** *of H in G (with g as representative). The left coset gH is analogously defined.*

If H is finite, then $|gH| = |Hg| = |H|$ for every $g \in G$, as follows from the cancellation laws Theorem 1.2. We see that cosets are certain subsets of G, which are closely related to the subgroup H. In the case of finite groups the number of elements in each coset is the same as the order of H.

1.15 Lemma. *Let G be a finite group, $H < G$. Then the following hold:*

- *If $g' \in Hg$, then $Hg' = Hg$.*
- *If $Hg' \neq Hg$, then $Hg' \cap Hg = \emptyset$.*

Proof. If $g' \in Hg$, then $g' = h_0 g$ for some $h_0 \in H$. For every $h \in H$ we have $hg' = hh_0 g \in Hg$, and also $hg = hh_0^{-1}h_0 g = hh_0^{-1}g' \in Hg'$. We obtain $Hg = Hg'$. The second statement is now obvious. □

We see that G is partitioned into the different right cosets. This leads us to the promised first interesting theorem of group theory:

1.16 Theorem (Lagrange's theorem). *If H is a subgroup of the finite group G, then the order of H divides the order of G.*

Proof. Denote by G/H the collection of right cosets of H in G. We have seen that the right cosets partition G and the number of elements in each such coset equals the order of H. This proves our theorem. $\square$

1.17 Definition (index). *Let $H \leq G$. The* **index** $[G : H]$ *of H in G is the number of right cosets of H in G, hence*

$$[G : H] = |G/H| = |G|/|H|.$$

For example, we have seen that $V < D_8$ (see Section 1.2). As V has order 4 and D_8 has order 8 we have $[D_8 : V] = 8/4 = 2$. This means also that there are precisely 2 cosets of V in D_8. One of them is the subgroup V itself. It follows that the second coset must be the complement $D_8 \setminus V$. This argument is valid for every subgroup of index 2.

We have seen in the preceding section that the order of an element $g \in G$ also is the order of the subgroup generated by g. It follows from Theorem 1.16 that $o(g)$ must divide $|G|$.

1.18 Corollary. *If G is a finite group, $g \in G$, then $o(g)$ divides $|G|$.*

We see that the order of G contains a lot of information about the possible subgroup structure and about possible orders of elements. If $|G| = 12$, then the possible orders of subgroups and of elements are to be found among $1, 2, 3, 4, 6, 12$. Clearly $\{e\}$ is the only subgroup of order 1 and G itself is the only subgroup of order 12. It is natural to ask if we can decide which divisors of the group order will be orders of subgroups. An important partial answer will be given later (Section 1.30).

Consider the case that $|G| = p$ is a prime. It follows that every element and every subgroup of G must have order 1 or p.

1.19 Corollary. *A group G of prime order p has only the trivial subgroups $\{e\}$ and G. Each element $e \neq g \in G$ has order p.*

1.7 Divisors and the Euclidean algorithm

We review in this section some basic facts from elementary number theory, which will be used routinely for the study of groups. Let d, n be integers ($d, n \in \mathbb{Z}$). We say that d **divides** n, in symbols $d \mid n$, if there is an integer m such that $n = dm$ (or: d is a **divisor** of n, or: n is a **multiple** of d.) For example, the multiples of 2 are the even numbers. 0 is divided by every integer n (because $0 = n \cdot 0$), but 0 does not divide any integer except itself.

1.20 Definition. *Let n, m be natural numbers. The* **greatest common divisor** *$gcd(n, m)$ is the largest natural number dividing both n and m.*

Clearly, $gcd(n, m)$ cannot be larger than the minimum $min(n, m)$ and we have $gcd(n, m) = m$ if and only if $m \mid n$. If $gcd(n, m) = 1$, we say that n and m are **coprime.** Some examples: $gcd(7, 21) = 7$, $gcd(16, 24) = 8$, $gcd(100, 37) = 1$. The **Euclidean algorithm** is an efficient method to compute the gcd of two given numbers. Its basis is long division: given nonzero integers a, b ($|a| \geq |b| > 0$) we can find integers q, r such that

$$a = q \cdot b + r,$$

where $|r| < |b|$. We illustrate with the example $gcd(910, 143)$:

910	=	6	·	143	+ 52
143	=	2	·	52	+ 39
52	=	1	·	39	+ 13
39	=	3	·	13	+ 0

At each step we divide the larger of the two numbers by the smaller one, with remainder. In the next step we consider the pair consisting of the smaller number in the previous step and of the remainder. As soon as the remainder becomes 0 we read off the gcd. It is the remainder in the previous step. In the example

$$gcd(910, 143) = gcd(143, 52) = gcd(52, 39) = gcd(39, 13) = gcd(13, 0) = 13.$$

Another consequence, both of practical and theoretical importance, is the fact that $gcd(n, m)$ can be written as a linear combination of n and m. In our example we start from the penultimate row. It has the gcd as remainder. We solve for the remainder and obtain $13 = 1 \cdot 52 - 1 \cdot 39$, an expression of 13 as linear combination of 52 and 39. Then we work our way up. The previous row expresses 39 as a linear combination of 143 and 52. Substituting this into our expression we obtain $13 = 3 \cdot 52 - 1 \cdot 143$. Proceeding like this once more we obtain $13 = 3 \cdot 910 - 19 \cdot 143$. This is the desired expression $(910, 143) = u \cdot 910 + v \cdot 143$. Here $u = 3, v = -19$.

1.21 Theorem. *Let n, m be integers. Then there exist integers u, v such that*

$$gcd(n, m) = u \cdot n + v \cdot m$$

1.22 Definition. *[Euler's $\phi-$function] Let n be a natural number. The number of numbers m between 0 and $n-1$, which are coprime to n, is $\phi(n)$.*

Let p be a prime. For every n we have that $gcd(p,n)=1$ if p does not divide n and $gcd(p,n)=p$ otherwise. It follows that every number between 1 and $p-1$ is coprime to p, hence $\phi(p)=p-1$. Let $n=p^a$. The numbers, which are not coprime to p^a, are those divided by p. As they come in steps of p on the number line, there are $n/p=p^{a-1}$ such numbers in our interval. It follows $\phi(p^a)=p^a-p^{a-1}$. In order to calculate ϕ efficiently the following theorem is needed.

1.23 Theorem. *If $gcd(n,m)=1$, then $\phi(nm)=\phi(n)\phi(m)$.*

We will obtain a group-theoretic proof of Theorem 1.23 a little later, in Section 1.12. Theorem 1.23 yields a method to compute the $\phi-$function: Write n as a product of prime-powers: $n=\prod_p p^{n(p)}$. Then $\phi(n)=\prod_p(p^{n(p)}-p^{n(p)-1})$. As an example let $n=1001=7\cdot 11\cdot 13$. We obtain $\phi(1001)=6\cdot 10\cdot 12=720$. As $168=2^3 3\cdot 7$ we have $\phi(168)=4\cdot 2\cdot 6=48$.

Finally, if n and m are written as products of prime-powers, the gcd and the least common multiple $lcm(n,m)$ can be read off right away: Let prime p appear with exponent $n(p)$ in n and with exponent $m(p)$ in m. Then the exponent of p is $Min(n(p),m(p))$ in the gcd, it is $Max(n(p),m(p))$ in the lcm. Here is an example:

$$n=2^3\cdot 3^5\cdot 7^2 \text{ and } m=2\cdot 3^2\cdot 5\cdot 7^6.$$

$$gcd(n,m)=2\cdot 3^2\cdot 7^2,\ lcm(n,m)=2^3\cdot 3^5\cdot 5\cdot 7^6.$$

As a consequence we obtain the following relationship between the gcd and the lcm:

1.24 Theorem.

$$gcd(n,m)\cdot lcm(n,m)=n\cdot m$$

The Euclidean algorithm is not restricted to the ring $\mathbb{Z}$ of integers. A version can be applied in each **Euclidean ring.** We will apply it in a later section to the polynomial ring $F[X]$ over a field F. The basis of the Euclidean algorithm in $F[X]$ is division with remainder: if a,b are polynomials of degrees $deg(a)\geq deg(b)>0$, then we can find polynomials q,r such that

$$a=q\cdot b+r,$$

where $deg(r) < deg(b)$. Comparison with the Euclidean algorithm in $\mathbb{Z}$ shows that we have replaced the absolute value of an integer by the degree of a polynomial.

1.8 Congruences and the cyclic groups

Let n be a natural number. When we calculate mod n we treat n as 0 and we identify any two integers if their difference is a multiple of n. $\mathbb{Z}/n\mathbb{Z}$ has only n objects, which we may identify with the n possible remainders when an integer is divided by n (long division). If that case we write $a \equiv b(\mod n)$, which simply means that $n \mid (a-b)$. Addition and multiplication in $\mathbb{Z}/n\mathbb{Z}$ is inherited from the integers. We just read the result mod n. Observe that there are precisely n classes mod n, in other words $|\mathbb{Z}/n\mathbb{Z}| = n$. Mod 2 we have just two classes (even and odd). If we write $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$ we have for example $1 + 1 = 0$ as the only rule, which would not be true for integers.

Fix attention to addition in $\mathbb{Z}/n\mathbb{Z}$. Compare with the axioms of Definition 1.1 and check that we have a group. The neutral element is 0, the group operation is written as addition (and not as usual as a multiplication). Associativity is certainly satisfied as addition of integers is associative. The "inverse" of a is $-a$. We have found a group of order n, which consists of the powers (in additive notation: multiples) of the element 1. If we wish to write our group multiplicatively we use the integers mod n as exponents. In that notation the group $\mathbb{Z}/4\mathbb{Z}$ appears as $\{e, g, g^2, g^3\}$, where g has order 4 and the exponents are mod 4. These groups are called cyclic groups.

1.25 Definition. *The cyclic group Z_n of order n consists of the powers of an element of order n. In additive notation (with group operation written as addition, the neutral element as 0) we obtain the additive group of $\mathbb{Z}/n\mathbb{Z}$.*

Here is the group table of the cyclic group of order 6:

Group table of Z_6						
	e	g	g^2	g^3	g^4	g^5
e	e	g	g^2	g^3	g^4	g^5
g	g	g^2	g^3	g^4	g^5	e
g^2	g^2	g^3	g^4	g^5	e	g
g^3	g^3	g^4	g^5	e	g	g^2
g^4	g^4	g^5	e	g	g^2	g^3
g^5	g^5	e	g	g^2	g^3	g^4

If we go to the right or down in the table we increase the exponent by 1 (observing $5 + 1 = 6 = 0$). This yields precisely the same structure as addition in the exponents, mod 6. In the next section we will be more precise about what it means that two groups have the same structure and should be considered as the same group.

Another representation of the cyclic groups is as groups of symmetry. In fact, consider a regular n-gon or simply n points, which we may choose as $1, 2, \ldots, n$ joined by edges in a circle. Mapping each edge to its neighbour in clockwise direction clearly is a symmetry (it maps edges to edges). This element is the n-cycle $(1, 2, \ldots, n) \in S_n$. It has order n and the group generated by it is the cyclic group Z_n. We realize that we have already met cyclic groups before. We will come back to the symmetries of an n-gon in a later section.

1.9 Generation

Let G be a group and $S \subset G$ a subset. The group $\langle S \rangle$ consists of all products with finitely many factors $\prod_{i=1}^{n} g_i$, where $g_i \in S$ or $g_i^{-1} \in S$. It is clear that $\langle S \rangle$ is a subgroup of G, in fact the smallest subgroup of G containing the set S. We call $\langle S \rangle$ the subgroup **generated by** S. In that perspective we can describe cyclic groups as the groups, which can be generated by one element ($|S| = 1$).

1.10 Isomorphisms

We have said in the preceding section that for example a subgroup of S_n generated by an n-cycle and the additive group of $\mathbb{Z}/n\mathbb{Z}$ have the same group structure and should be considered as two ways of writing the same group. We need a precise notion to express this situation.

1.26 Definition. *Let G and H be groups (written multiplicatively). A mapping $f : G \longrightarrow H$ is a* **group isomorphism** *if the following hold:*

- *f is a bijective mapping (one-to-one and onto), and*
- *For every $g \in G$ we have $f(g^{-1}) = f(g)^{-1}$, and*
- *For every $g_1, g_2 \in G$ we have $f(g_1g_2) = f(g_1)f(g_2)$.*

If there is an isomorphism between G and H, we call G and H isomorphic groups and write $G \cong H$.

We can see the application of the isomorphism f as a renaming of the elements of G such that the multiplication remains unchanged. This shows that isomorphic groups should be considered essentially the same. Observe that isomorphism forms what is called an equivalence relation: $G \cong G$ (given by the identity mapping), if $G \cong H$, then $H \cong G$ (consider the inverse mapping), and finally transitivity: if $G_1 \cong G_2$ and $G_2 \cong G_3$, then $G_1 \cong G_3$ (because the composition of two isomorphisms is an isomorphism). An isomorphism between the additive group of $\mathbb{Z}/n\mathbb{Z}$ and the subgroup $\langle(1, 2, \ldots, n)\rangle$ is given by $f(a) = (1, 2, \ldots, n)^a$. Here is a more general but equally obvious observation:

1.27 Theorem. *Let $g \in G, o(g) = n$. The subgroup $\langle g\rangle$ of G as considered in Theorem 1.12 is isomorphic to the cyclic group Z_n.*

1.28 Theorem. *For every prime p there is only one isomorphism type of group of order p, the cyclic group Z_p.*

This follows from Corollary 1.19.

1.11 Calculating in cyclic groups

A finite group is cyclic if it consists of the powers of one of its elements g. If $o(g) = n$, then the group is Z_n. Let us calculate the order of each element of the cyclic group $\langle g\rangle \cong Z_n$. An arbitrary element has the form g^i, where $i = 0, 1, \ldots, n-1$. By definition $o(g^i)$ is the smallest natural number j such that $(g^i)^j = g^{ij} = e$. The exponent ij is a multiple of i and of n and it is minimal with these properties, in other words $ij = lcm(i, n) = in/gcd(i, n)$ (see Theorem 1.24). We conclude $j = n/gcd(i, n)$.

1.29 Theorem. *Let g be a generator of Z_n. Then*

$$o(g^i) = \frac{n}{gcd(i, n)}.$$

g^i is a generator of Z_n if $o(g^i) = n$. By Theorem 1.29 this is equivalent with $gcd(i, n) = 1$. Comparison with Definition 1.22 shows that the number of such elements is $\phi(n)$.

1.30 Theorem. *The number of generators of Z_n is $\phi(n)$.*

This gives us a purely group-theoretical interpretation of the $\phi-$function. We can count the number of elements of any given order in Z_n. Let $d|n$ be given (do not forget Corollary 1.18). We have $o(g^i) = d$ if and only if $gcd(i, n) = n/d$ by Theorem 1.29. Write $i = \frac{n}{d} \cdot j$. The condition on j is $gcd(j, d) = 1$. We obtain the following generalization of Theorem 1.30:

1.31 Theorem. *For every divisor d of n there are precisely $\phi(d)$ elements of order d in Z_n. For every $d|n$ there is precisely one cyclic subgroup of order d in Z_n. There are no other subgroups in Z_n.*

Proof. As before let g be a generator of Z_n. We have already proved the first two statements. It remains to prove that every subgroup $U < Z_n$ is cyclic. Let $i > 0$ be minimal such that $g^i \in U$. It follows $\langle g^i \rangle \leq U$. Let $g^j \in U$. Divide j by i, with remainder: $j = ai + r$, where $0 \leq r < i$. Then $g^r \in U$. The minimality of i shows $r = 0$, hence $g^j \in \langle g^i \rangle$. □

1.32 Proposition. *The number of elements $x \in Z_n$ satisfying $x^m = e$ is $gcd(n, m)$.*

We leave the proof as an exercise.

1.12 Direct products

We describe the easiest and most formal way of constructing a new group out of two given groups. Let groups G and H be given. Our new group will consist of the pairs (g, h), where $g \in G, h \in H$. Multiplication is defined coordinatewise: $(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2)$. Here multiplication on the left is in G, multiplication on the right is in H. It is clear that this defines a group, the **direct product** $G \times H$ of G and H. It is also clear that $|G \times H| = |G| \cdot |H|$ and $G \times H \cong H \times G$. The generalization to more than two components is equally obvious. This notion gives us a direct construction of an interesting family of groups:

1.33 Definition. *Let p be a prime. The* **elementary-abelian** *group of order p^n is defined as the direct product of n copies of Z_p. We denote it by $E(p^n)$.*

The elementary-abelian groups $E(p^n)$ have the property that every element $\neq e$ has order p.

1.34 Theorem. *If n and m are coprime, then $Z_n \times Z_m \cong Z_{nm}$.*

Proof. Let g be a generator of Z_n and h a generator of Z_m. The element (g, h) in the direct product has order $lcm(n, m) = nm$. □

We also see that in the situation of Theorem 1.34 an element (g^i, h^j) generates $Z_n \times Z_m$ if and only if g^i generates Z_n and h^j generates Z_m. As we have already seen that the number of generators of Z_n is $\phi(n)$ (see Theorem 1.30) we see that Theorem 1.34 yields the promised group-theoretic proof of Theorem 1.23.

1.13 Normal subgroups and factor groups

We turn to another point of our check list given in the beginning of Section 1.5, factor groups. Let $H < G$. The idea is to define a group where multiplication is like in G but elements of H are treated as if they were the neutral element. As we talk about groups in general (not just abelian groups) we use right cosets, keeping in mind that we could have used left cosets just as well. So the elements of the factor group are the right cosets Ha. There are $[G : H]$ such cosets (see Section 1.6). We want to define the product of two right cosets as

$$(Ha)(Hb) = Hab$$

(multiply arbitrary elements of the coset. The product is a representative of the product coset). The question is if this definition makes sense. In fact, replace a and b by other representatives from the same cosets: ha and $h'b$ respectively. We must prove that the product coset is the same, hence that $(ha)(h'b) = h''ab$ for some $h'' \in H$. As $(ha)(h'b) = h(ah'a^{-1})ab$ this is equivalent with $ah'a^{-1} \in H$. This condition has to be satisfied for all $h' \in H$ and all $a \in G$. We conclude that a factor group can be defined if and only if the following condition is satisfied for all $g \in G : g^{-1}Hg = H$, or equivalently $Hg = gH$. This leads us to the definition of a normal subgroup:

1.35 Definition. *A subgroup $N \leq G$ is a* **normal subgroup** *if and only if the following equivalent conditions are satisfied for all $g \in G$.*

- $Ng = gN$,
- $g^{-1}Ng = N$

If N is a normal subgroup of G we write $N \lhd G$ (if case $N = G$ is excluded), respectively $N \unlhd G$.

The condition in Definition 1.35 says that for every $n \in N$ and $g \in G$ we have $g^{-1}ng \in N$.

1.36 Definition. *Let $N \unlhd G$. The* **factor group** *G/N is the set of all (right or left) cosets of N in G, where the product is defined by*

$$(Ng)(Ng') = Ngg'.$$

Observe that the condition in Definition 1.35 is symmetric. This shows that fortunately we do not have to distinguish between right and left factor groups. The order of the factor group G/N is the index $[G : N]$ (see Definition 1.17). Two trivial normal subgroups are $N = \{e\}$ and $N = G$. In the first case we have $G/N \cong G$, in the second case G/N has order 1. In general it may not be easy to find nontrivial normal subgroups.

1.37 Proposition. *Every subgroup of an abelian group is normal.*

This is immediately clear from the definition. A little more interesting is the following:

1.38 Proposition. *Every subgroup of index 2 is normal.*

Proof. Let $[G : H] = 2$. One of the two right cosets of H is H itself. The second must therefore be the complement $G \setminus H$. The same is true of left cosets. We see that every right coset is also a left coset. $\square$

As an example consider the subgroup $V < D_8$, in the group table of D_8 as given in Section 1.3. In the top left-hand corner we see the group table of V. If we divide the group table of D_8 in four $(4,4)-$submatrices we see that these form the group table of the group of order 2. The same happens with the subgroup of order 3 in S_3. Clearly $D_8/V \cong S_3/Z_3 \cong Z_2$ as there is only one group of order 2.

The concept of a factor group also helps us to understand congruences (see Section 1.8) from a different perspective. The integers $\mathbb{Z}$ form an abelian group under addition. This is an infinite cyclic group. It has only two generators, 1 and its "inverse" -1 (recall that we use additive notation and that the neutral element is 0). In fact every integer is either a multiple ("power") of 1 (for example $4 = 1 + 1 + 1 + 1$) or a negative ("inverse") thereof. The set $n\mathbb{Z}$ of all multiples of n forms a subgroup. Our set of congruence classes $\mathbb{Z}/n\mathbb{Z}$ is simply the factor group in the sense of the present section.

1.14 Group homomorphisms

We defined group isomorphisms in Section 1.10. An important and natural generalization are homomorphisms.

1.39 Definition. *Let G, H be groups. A mapping $f : G \longrightarrow H$ is a* **(group) homomorphism** *if the following always hold:*

- $f(g_1g_2) = f(g_1)f(g_2)$.
- $f(g^{-1}) = f(g)^{-1}$.

The conditions in Definition 1.39 mean that f respects the group structures of G and H. Observe that a group homomorphism, which is one-to-one and onto, is an isomorphism (compare Section 1.10).

1.40 Definition. *The* **image** $Im(f) \subset H$ *of the group homomorphism $f : G \longrightarrow H$ is of course the set of images. The* **kernel** *is defined as*

$$Ker(f) = \{g : g \in G, f(g) = e\}.$$

Clearly f is onto if and only if $Im(\alpha) = H$. The kernel will help us determine when f is one-to-one.

1.41 Theorem. *The image of a group homomorphism is a subgroup, the kernel is a normal subgroup.*

Proof. Let $f : G \longrightarrow H$, $h_1 = f(g_1), h_2 = f(g_2) \in Im(f)$. We have to show that $h_1 h_2$ and h_1^{-1} belong to $Im(f)$. This follows from the definition of a group homomorphism: $h_1 h_2 = f(g_1 g_2)$ and $h_1^{-1} = f(g_1^{-1})$. The proof that $Ker(f) \leq G$ is analogous. Let us prove it is a normal subgroup. So let $k \in Ker(f), g \in G$. We have to prove that $g^{-1}kg \in Ker(f)$. In fact, $f(g^{-1}kg) = f(g)^{-1}f(k)f(g) = f(g)^{-1}ef(g) = e$. □

Theorem 1.41 often helps to prove that certain subgroups are normal. It suffices to find a group homomorphism, which has the subgroup as its kernel. The kernel determines if f is one-to-one (injective).

1.42 Proposition. *Let $f : G \longrightarrow H$ be a group homomorphism. Then f is injective (one-to-one) if and only if $Ker(f) = \{e\}$.*

Proof. One direction is obvious. $Ker(f)$ is defined as the inverse image of e. If f is injective, then we must have $Ker(f) = \{e\}$. Assume $Ker(f) = \{e\}$ and consider elements g_1, g_2 such that $f(g_1) = f(g_2)$. It follows $f(g_1 g_2^{-1}) = e$, hence $g_1 g_2^{-1} \in Ker(f)$. We conclude $g_1 g_2^{-1} = e$, hence $g_1 = g_2$. □

We come to our next structural theorem.

1.43 Theorem (first isomorphism theorem). *Let $f : G \longrightarrow H$ be a group homomorphism. Then*

$$G/Ker(f) \cong Im(f).$$

Proof. Let $K = Ker(f)$. We have to find a mapping : $G/K \longrightarrow Im(f)$, which is an isomorphism. This means we must map cosets to elements of H. Let $kg \in Kg$. Then $f(kg) = f(k)f(g) = ef(g) = f(g)$. This means that f is a constant function on each coset. This shows how to define our mapping: $\overline{f}(Kg) = f(g)$. We have just made sure that $\overline{f}$ is well-defined. It is a group homomorphism as f is. Clearly its image is $Im(f)$. Also, by definition of K, the coset K (the neutral element of the factor group) is the kernel of $\overline{f}$. We conclude from Proposition 1.42 that $\overline{f}$ is indeed an isomorphism. □

1.15 The signum and alternating groups

We return to permutations and the symmetric group, which we left in Section 1.4. It will turn out that there are two types of permutations, which we will call even and odd, respectively.

1.44 Definition. *Let $\pi \in S_n$, where S_n acts on $\Omega = \{1, 2, \dots, n\}$. Fix the natural total ordering $1 < 2 < 3 \cdots < n$. Call a pair $\{i, j\}$ of symbols an* **inversion** *of π if $i < j$ but $\pi(i) > \pi(j)$ (or $i > j$ but $\pi(i) < \pi(j)$).*

A pair is an inversion if the order is inverted by application of π. The essential combinatorial idea is in the following lemma:

1.45 Lemma. *Every transposition has an odd number of inversions.*

Proof. Let our transposition be $\tau = (a, b)$, where we choose notation such that $a < b$. When will a pair $\{i, j\}$, be an inversion of τ? As τ moves only a and b this can only happen if either i or j equals one of a or b. If $i = a$ or $i = b$ and $j < a$ or $j > b$, again we have no inversion. So let $a < j < b$. In this case both $\{a, j\}$ and $\{j, b\}$ are inversions. The inversions come in pairs. The only pair we have not considered yet is $\{a, b\}$, and this definitely is an inversion. □

The same argument yields a stronger conclusion:

1.46 Theorem. *Let $\pi \in S_n$ and τ a transposition in S_n. Then the following hold:*

- *If π has an even number of inversions, then $\pi\tau$ has an odd number of inversions.*
- *If π has an odd number of inversions, then $\pi\tau$ has an even number of inversions.*

This motivates the following definition:

1.47 Definition. *A permutation is* **even** *if it has an even number of inversions, it is* **odd** *if it has an odd number of inversions.*

Clearly the neutral permutation is even, and we have seen that transpositions are odd. Also, multiplication by a transposition changes the parity (Theorem 1.46). This implies that products of an even number of transpositions are even, and vice versa. Can we write every permutation as a product of transpositions? It suffices to consider cycles.

1.48 Lemma. *We have*

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

We check right away that this formula is true. Consider the small cases:

$$(1,2,3,4)=(1,2)(1,3)(1,4) \text{ and } (1,2,3,4,5)=(1,2)(1,3)(1,4)(1,5)$$

1.49 Corollary. *Every permutation can be written as a product of transpositions.*

Every odd cycle is a product of an even number of transpositions and every even cycle is a product of an odd number of transpositions. In particular odd cycles are even permutations and even cycles are odd permutations. A permutation is even if and only if it can be written as a product of an even number of transpositions. All this is best expressed by the signum.

1.50 Definition. *The* **signum** *of a permutation is* $sgn(\pi)=1$ *if* π *is even,* $sgn(\pi)=-1$ *if* π *is odd.*

The link between the signum and the parity of the number of transpositions involved proves that the signum is multiplicative: $sgn(\pi_1\pi_2)=sgn(\pi_1)sgn(\pi_2)$, where the product on the right side is in $\{1,-1\}$. As $\{1,-1\}$ is one way of writing the group of order 2 we finally see that sgn is a group homomorphism.

1.51 Theorem. $sgn : S_n \longrightarrow \{1,-1\} \cong Z_2$ *is a surjective (onto) group homomorphism. The kernel of* sgn *consists of the even permutations.*

In particular $Ker(sgn)$ is a normal subgroup of index 2 in S_n (see Theorem 1.43).

1.52 Definition. *The* **alternating group** $A_n = Ker(sgn)$ *is the normal subgroup of* S_n *consisting of the even permutations.*

In particular $[S_n : A_n] = 2$ and $|A_n| = \frac{1}{2}n!$ The group A_3 is the cyclic subgroup generated by a 3-cycle, A_4 has order 12 and consists of the neutral element, the eight 3-cycles and the three elements, which are products of two disjoint transpositions. If we wish to check the parity of a permutation, here is the handiest criterion:

1.53 Proposition. *Write permutation π as a product of cycles. Then π will be even if and only if there is an even number of cycles of even length.*

Example: $(1,2,4,8)(1,3,5)(6,7)(1,8,7,6,5,4)$ is an odd permutation as it is written as a product with three cycles of even length. As a product of disjoint cycles the same element can be written as $(1,2)(3,4,7,5,8)$.

We take the opportunity to recall an instance where the signum of permutations is used in linear algebra. Here is the usual definition of the determinant:

1.54 Definition. *Let $A = (a_{i,j})$ be an (n,n)-matrix. The* **determinant** *of A is*

$$det(A) = \sum_{\pi \in S_n} sgn(\pi) a_{1,\pi(1)} \dots a_{n,\pi(n)}.$$

Here S_n acts on $\{1, 2, \dots, n\}$. We see that $det(A)$ is a sum of $n!$ terms. Each term is determined by a permutation π. We form the product of n entries of the matrix, where row i contributes $a_{i,\pi(1)}$. This product is added or subtracted, according to $sgn(\pi)$. Observe that this definition makes sense whenever the entries of the matrix can be added and multiplied. In case $n = 2$ we obtain the familiar rule $det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$. Here the neutral permutation yields the term ad, the transposition $(1,2)$ (of signum -1) yields $-bc$. We will use some basic facts about matrices and determinants in Section 1.22.

1.16 Permutation representations

We started out with groups of symmetries. These are groups consisting of permutations. In general we call a group $G \leq S_n$, which is embedded in a symmetric group, a **permutation group** of **degree** n. When starting from an arbitrary group G we wish to find symbols on which G acts, such that every $g \in G$ becomes a permutation and the product of group elements acts as the product permutation. Our general notion of group homomorphisms (see Definition 1.39) shows how this can be made precise:

1.55 Definition. *A* **permutation representation** *of* **degree** *n of a group G is a group homomorphism $\pi : G \longrightarrow S_n$.*

This is the general notion we were looking for. If the homomorphism π is given we also write g instead of the more precise $\pi(g)$. A permutation representation amounts to finding a set Ω of n objects, on which the elements of G act as permutations. One also speaks of an **action** of G on Ω. The difference from the notion of a permutation group is that there can be a kernel. $Ker(\pi)$ consists of those elements of g that act as the neutral permutation. We see from the first isomorphism theorem (Theorem 1.43) that $G/Ker(\pi)$ is a permutation group of degree n.

As an example let us study S_4. Its natural permutation representation is as the group of all permutations on a set $\{1,2,3,4\}$. Every permutation of $\{1,2,3,4\}$ also permutes the pairs of points. There are $\binom{4}{2} = 6$ such unordered pairs. This gives us a permutation representation of degree 6 of S_4. We refine this argument. If I know the image of some pair $\{i,j\}$ I also know the image of the complementary pair $\{1,2,3,4\} \setminus \{i,j\}$. We see that every $g \in G$ also permutes the 3 pairs of complementary pairs. Let us fix notation.

$$a = (1,2) \mid (3,4) \ , \ b = (1,3) \mid (2,4) \ , \ c = (1,4) \mid (2,3)$$

We have seen that S_4 has a permutation representation on the set $\{a,b,c\}$. For example consider $(1,2,3)$. It maps $\{1,2\} \mapsto \{2,3\}$ and thus $\{3,4\} \mapsto \{1,4\}$. It follows that $\pi((1,2,3)) : a \mapsto c$. We continue calculating in the same way and obtain $\pi((1,2,3)) = (a,c,b)$. As π is a permutation representation (group homomorphism) $\pi : S_4 \longrightarrow S_3$, it is impossible that π is injective. There must be a rather large kernel. An element $g \in S_4$ belongs to $Ker(\pi)$ if it fixes a,b,c. We have $g \in Ker(\pi)$ if and only if the image of any pair is either the same pair or its complement. We see that transpositions and 3-cycles do not have that property. The three permutations that are products of two disjoint transpositions do have the property.

1.56 Proposition. *Let π be the permutation representation of S_4 on the pairs of complementary pairs. Then*

$$Ker(\pi) = V = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}.$$

We have $V \lhd S_4$ and $S_4/V \cong S_3$.

Proof. We have seen $V = Ker(\pi)$. As π is a group homomorphism we conclude from Theorem 1.41 that $V \lhd S_4$. By Theorem 1.43 we have that S_4/V is isomorphic to a subgroup of S_3. As both groups have order 6 it must be that $S_4/V \cong S_3$ □

We see that permutation representations may be used to prove that certain subgroups are normal. Just find such a representation, which has the group in question as its kernel.

1.17 Orbits and the orbit lemma

1.57 Definition. *Let $\pi : G \longrightarrow S_\Omega$ be a permutation representation. Let $i \in \Omega$ be one of the symbols. The* **orbit** *of i consists of all symbols j such that there is some $g \in G$, which maps $i \mapsto j$.*

1.58 Proposition. *Let $\pi : G \longrightarrow S_\Omega$ be a permutation representation. Then Ω is a disjoint union of the orbits.*

Proof. Write $i \sim j$ if j is in the orbit of i. It is immediate, using the group axioms, to check the following:

- $i \sim i$ (using the neutral element)
- If $i \sim j$, then $j \sim i$ (using the inverse)
- If $i \sim j$ and $j \sim k$, then $i \sim k$ (using products).

This shows that $\sim$ is an equivalence relation. The claim follows immediately. □

1.59 Definition. *A permutation representation $\pi : G \longrightarrow S_\Omega$ is* **transitive** *if Ω forms one orbit. This means that for every $i, j \in \Omega$ there is some $g \in G$ such that $\pi(g) : i \mapsto j$. π is* **faithful** *if $Ker(\pi) = \{e\}$.*

1.60 Definition. *Let $\pi : G \longrightarrow S_\Omega$ be a permutation representation and $i \in \Omega$. The* **stabilizer** *of i is defined as*

$$G_i = \{g : g \in G, \pi(g) : i \mapsto i\}$$

(all the elements of G, which fix symbol i)

1.61 Proposition. *Let $\pi : G \longrightarrow S_\Omega$ be a permutation representation and $i \in \Omega$. The stabilizer G_i is a subgroup of G.*

This is immediate (see the Problems). The following easy theorem is extremely useful for many applications.

1.62 Theorem (The orbit lemma). *Let $\pi : G \longrightarrow S_\Omega$ be a permutation representation, $i \in \Omega$ and $\mathcal{O}$ the orbit of i. Then we have*

$$[G : G_i] = |\mathcal{O}|$$

(the length of the orbit is the index of the stabilizer).

Proof. We have to establish a bijection between cosets of G_i and elements of the orbit. Let $h \in G_i, g \in G$. Then

$$i\pi(hg) = i\pi(h)\pi(g) = i\pi(g).$$

This follows from the definition of the stabilizer: $\pi(h) : i \mapsto i$. This shows that every element of the coset $G_i g$ maps i to the same element element of the orbit. This shows already that the length of the orbit cannot be larger than the number of cosets. Assume now we have $g_1, g_2 \in G$ such that $i\pi(g_1) = i\pi(g_2)$. It follows $i = i\pi(g_1 g_2^{-1})$, equivalently $g_1 g_2^{-1} \in G_i$. We conclude that $g_1 \in G_i g_2$. This shows that elements mapping i to the same image must be in the same coset. □

1.18 The dihedral groups

Let us determine the symmetry group of the regular n-gon. That means we have n points ordered on a circle, and each point is connected by an edge to its two neighbours along the circle. Here is a picture of the regular hexagon (=6-gon).

The symmetry group G is the subgroup of S_n (in its action on the points), whose elements map edges to edges (and non-edges to non-edges). The case $n = 4$ has been considered much earlier, in Section 1.2. The symmetry group turned out to be D_8 in this case (see Theorem 1.5). Our attack on the case of the general n-gon will be greatly facilitated by the theory we have developed. Observe that $Z_n \leq G$, where Z_n consists of rotations. This subgroup shows already that G is transitive on the points (the points form one single orbit). The orbit lemma (Theorem 1.62) shows that $|G| = n \cdot |H|$, where $H = G_1$ is the stabilizer of point 1. It suffices to determine H. Let $g \in H$. Then g must permute the two neighbours 2 and n of 1. Assume g fixes 2. Then g must fix the unique new neighbour 3 of 2. Proceding in this fashion we see that $g = e$. The only other possibility is $g : 2 \leftrightarrow n$. The continuation is uniquely determined: $g : 3 \leftrightarrow n - 1, \ldots$. In our hexagonexample we have

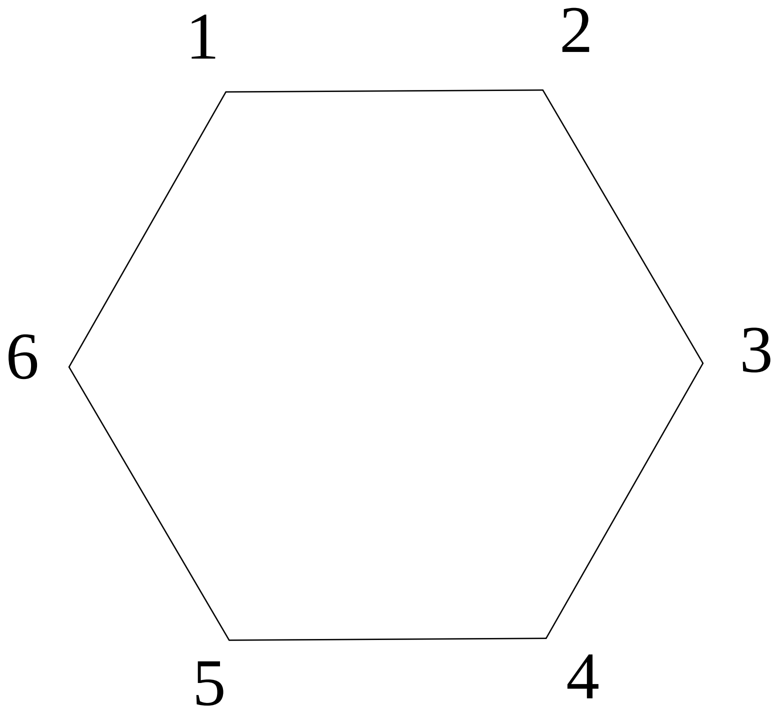


Figure 1.3: The regular hexagon

$g = (2, 6)(3, 5)$. Geometrically g is the reflexion across the line connecting 1 and 4. We have seen that $|H| = 2$ and conclude $|G| = 2n$.

1.63 Theorem. *The symmetry group of the regular n-gon is a group D_{2n} of order $2n$. This group is known as the* **dihedral group.**

It can be shown that every element in $D_{2n} \setminus Z_n$ has order 2 (is an involution).

1.19 The cube

We want to use our methods to describe the symmetry group G of the cube. The cube has 8 vertices (points), 12 edges and 6 faces. In fact, it is easy to see that there are exactly 6 sets of four vertices, on which a square (of 4 edges) is induced. These are the faces, which we denote by A, B, C, D, E, F. It follows that G permutes not only the 12 edges, but also the 6 faces. The complement (opposite) of each face is a face. It follows that G also permutes the 3 pairs of opposite faces. Likewise, every vertex has an opposite partner (the only vertex, which is neither a neighbour nor a neighbour of a neighbour of the original vertex). The opposite of 1 is 7, for example. This gives us a permutation representation of G on the 4 pairs of opposite edges. We can use all these permutation representations to gain information on G.

1.64 Proposition. *The group of symmetries of the cube has order 48.*

Proof. Consider the permutation representation on the faces. It is geometrically obvious that G is transitive on the faces. We conclude from Theorem 1.62 that $|G| = 6|H|$, where $H = G_A$ is the stabilizer of face A in G. The group H permutes the vertices 1,2,3,4 of face A. These form a square (a 4-gon). It follows that the permutation group induced by H cannot be larger than D_8 (see Theorem 1.63). We see that Z_4 (the rotations) is certainly present, but clearly we also have the permutation $(2, 4)(6, 8) \in H$. This shows that the permutation group of $\{1, 2, 3, 4\}$ induced by H is indeed D_8. We have $|H| = 8 \cdot |K|$, where $K < H$ is the kernel of the permutation representation of H, hence the stabilizer of vertices 1,2,3 and 4. It is easy to see that $K = \{e\}$. In fact, the image of 5 under an element of K must be a neighbour of 1. As 5 is the only neighbour of 1 among $\{5, 6, 7, 8\}$ we see 5 must be fixed. The same argument holds for all other vertices. We conclude $|G| = 6 \cdot 8 = 48$. □

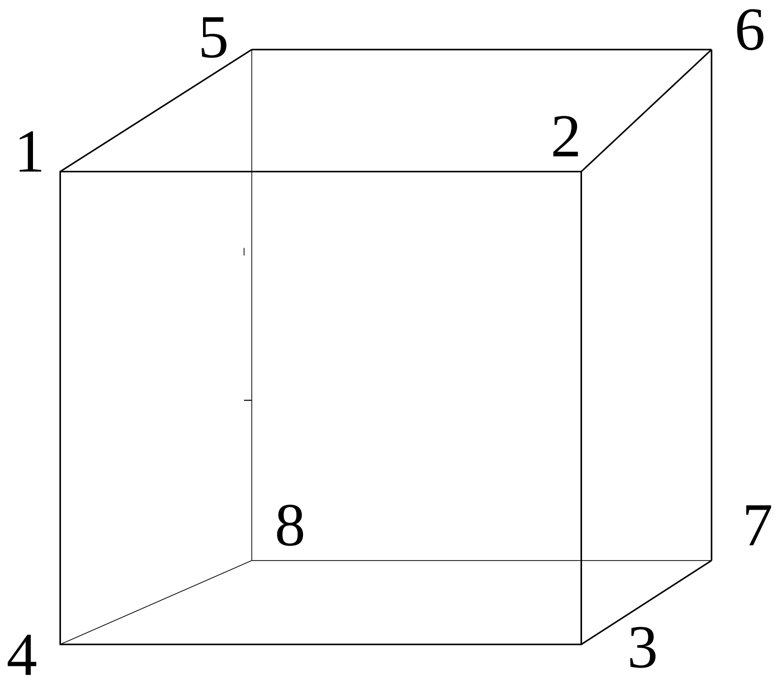


Figure 1.4: The cube

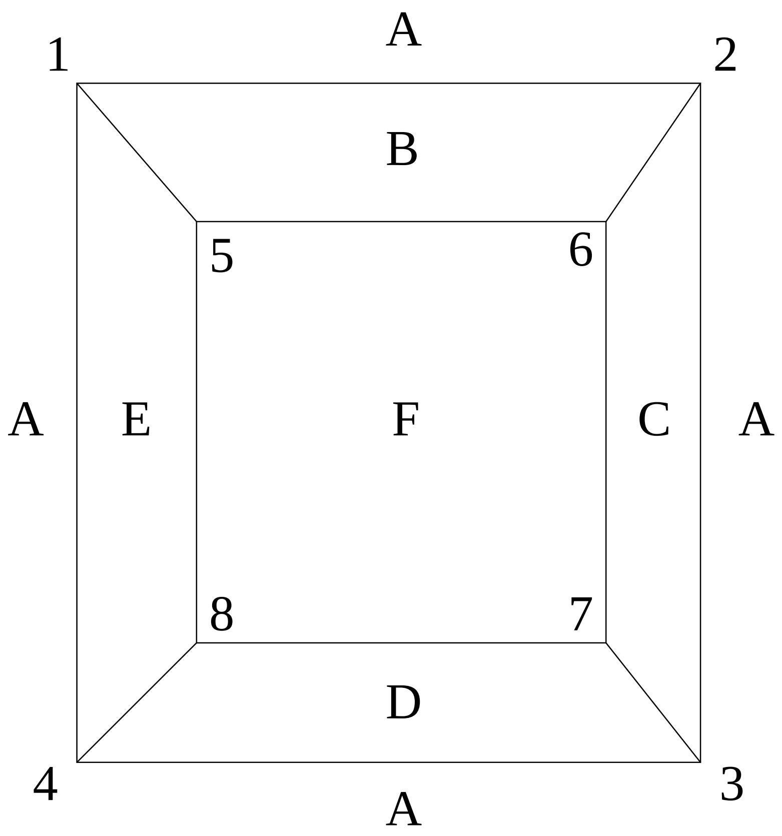


Figure 1.5: A flat version of the cube

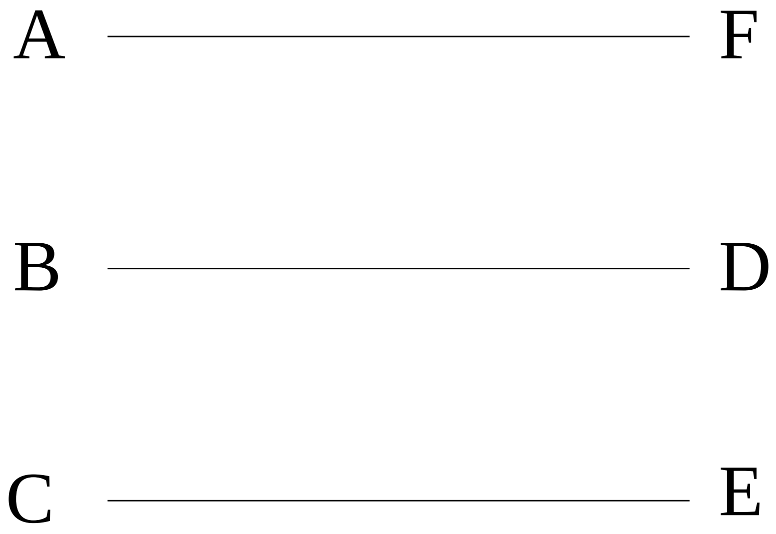


Figure 1.6: A graph related to the cube

Along the way we have also seen that the stabilizer of a face is D_8. Consider the action of G on the 4 pairs of opposite vertices. As $|G| = 48 > 24 = |S_4|$, this action cannot be faithful. Let K be the kernel, $g \in K$. This means that $g \in G$ and for every vertex i we have that $g(i)$ is either i or the opposite of i. Assume $g(1) = 1$. Automatically $g(7) = 7$. As $g(2)$ must be a neighbour of 1 and 8, the opposite of 2, is not a neighbour of 1, we must have $g(2) = 2$. We can continue in this fashion and see $g = e$. We have seen that no non-neutral element of the kernel K can fix a vertex. The only non-neutral permutation that can be in K is therefore $z = (1,7)(2,8)(3,5)(4,6)$, mapping each vertex to its opposite. As we have seen that $K > \{e\}$ we must have that z is a symmetry and $K = \langle z \rangle$. It follows from Theorem 1.43 that G/K is isomorphic to a subgroup of S_4. As $|G/K| = 24 = |S_4|$ it follows $G/K \cong S_4$.

1.65 Proposition. *The element $z = (1,7)(2,8)(3,5)(4,6) \in G$ has the property that $\langle z \rangle \lhd G$ and $G/\langle z \rangle \cong S_4$.*

Finally we consider the action of G on the faces. As they come in opposite pairs it follows that G acts as a group of symmetries of the structure, which is obtained, when we represent each face by a vertex and connect opposite vertices by edges.

This is yet another example of what is known as a graph.

1.66 Definition. *A* **graph** Γ *consists of a set of vertices and of a set of edges, where each edge is a pair of vertices. The* **symmetry group** *(or* **automorphism group***)* $Aut(\Gamma)$ *of* Γ *consists of all permutations of the vertices, which map edges to edges (and non-edges to non-edges).*

The n-gons are graphs and we have determined their automorphism group D_{2n} (Theorem 1.63). The cube is a graph. We are just comparing its automorphism group G to the group of the face-graph with the faces as vertices, where the edges connect each face to its opposite. Clearly each element of G yields a symmetry of the face-graph. We leave it as easy exercises that the representation of G on the faces is faithful (a symmetry of the cube, which fixes all faces, must also fix all vertices) and that the automorphism group of the face-graph has order 48. It follows from Theorem 1.43 that the permutation representation of G on the faces yields an isomorphism between G and the automorphism group of the face-graph.

1.67 Proposition. *The cube and the graph on 6 vertices, which consists of 3 disjoint edges, have isomorphic group of symmetries.*

This means that for every permutation of the faces, which respects the opposite-pair structure, there is precisely one symmetry of the cube, which induces this action. As an example, consider the permutation $(A, D, C)(B, E, F)$, which clearly is a symmetry of the face-graph. The corresponding symmetry of the cube is $(1, 8, 6)(2, 4, 7)$.

1.20 Prime fields

1.68 Definition. *Let F be a set with a an additive and a multiplicative structure. This means that whenever $x, y \in F$ then $x + y \in F$ and $x \cdot y \in F$ are defined. Then F is called a* **field** *if the following are satisfied:*

- *F is an abelian group under addition. Denote the neutral element by* 0.
- $0 \cdot x = x \cdot 0 = 0$ *for all $x \in F$.*
- *$F \setminus \{0\} = F^*$ is an abelian group under multiplication. Denote the neutral element of F^* by* 1.
- $a(b + c) = ab + ac$ *for all $a, b, c \in F$ (distributive law).*

We see that the basic notion of a group appears in the definition of a field. The field structure consists of an additive group and a multiplicative group, where the collaboration between these groups is regulated by the distributive law. Well-known examples of fields are the rationals, the reals and the complex numbers. As we are most interested in finite groups let us consider finite fields. We have encountered some of them already.

1.69 Theorem. *Let p be prime. Then $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is a field (a* **prime field***).*

Proof. As addition and multiplication in $\mathbb{F}_p$ are inherited from the integers it is clear that distributivity holds and that addition and multiplication are commutative. It has been observed earlier that addition turns $\mathbb{F}_p$ into a group, the cyclic group of order p. It remains to show that multiplication defines a group structure on $\mathbb{F}_p^*$. The most important point is to show that the product of two nonzero elements is nonzero again. This is true because p is a prime. It is equivalent to the statement, that the product of two integers, none of which is divisible by p, is not divisible by p either. Going back to Definition 1.1 we see that the only remaining problem is the existence of an inverse. Recall that we are calculating mod p. In terms of integers we are given an integer a, which is not divisible by p, and we need to find an integer b such that $ab \equiv 1 \pmod{p}$. The Euclidean algorithm will help us out. As a is not divisible by p and p is a prime we have $gcd(a,p) = 1$. It follows from Theorem 1.21 that there are integers b and w such that $ab + pw = 1$. This proves our claim. □

1.21 Finite fields

Let p be a prime number. We have seen in the preceding section that $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ is a finite field. Are there any other finite fields? Let F be any finite field. Denote the sum of n copies of 1 by $n \cdot 1 \in F$. As F is finite the $n \cdot 1 \in F$ cannot all be different. So there must be some $m < n$ such that $n \cdot 1 = m \cdot 1$. It follows $(n - m) \cdot 1 = 0$. Denote by a the smallest natural number such that $a \cdot 1 = 0$. As F has no zero divisors we conclude that $a = p$ must be prime. It follows from the minimality that p is the only prime with this property and that $n \cdot 1 = 0$ if and only if n is a multiple of p. We see that the $i \cdot 1, i = 0, 1, \ldots p - 1$ form a subfield of F, which is isomorphic to $\mathbb{F}_p$. We call p the **characteristic** of F and $\mathbb{F}_p$, the subfield of F generated by 1, its **prime field.** So every finite field F may be described as an extension of its prime field $\mathbb{F}_p$. As F is by definition a vector space over $\mathbb{F}_p$ its number of elements is p^n for some n.

1.70 Theorem. *Every finite field has p^n elements for some prime p. The subfield generated by the element 1 is $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.*

In order to generate finite fields we use irreducible polynomials. So let $f(X) \in \mathbb{F}_p[X]$ be an irreducible polynomial of degree n. Take $f(X)$ to be monic (its leading coefficient is 1), so that $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$. We claim that $F = \mathbb{F}_p[X]/(f(X))$, the factor ring of the polynomial ring over the ideal generated by $f(X)$, is a field with p^n elements:
denote by x the image of X mod the ideal $(f(X))$. Remark that $(f(X))$ simply is the set of all polynomials, which are divisible by $f(X)$. At first we see that F is a vector space of dimension n over $\mathbb{F}_p$, so $|F| = p^n$. The elements of F can be uniquely represented in the form $u = \sum_{i=0}^{n-1} c_i x^i$. In fact, as $x^n = -a_{n-1}x^{n-1} - \cdots - a_1x - a_0$, every element of F has this form. On the other hand, the $x^i, i = 0, 1, \ldots, n-1$ are linearly independent as otherwise $f(X)$ would divide a nonzero polynomial of degree $< n$, which is impossible. So every element of F can be written in a unique way as a polynomial of degree $< n$ with coefficients in $\mathbb{F}_p$. Assume $g(x), h(x)$ are such polynomials and $g(x)h(x) = 0$. This means that $f(X)$ divides $g(X)h(X)$. As $f(X)$ is irreducible it must divide either $g(X)$ or $h(X)$. Thus either $g(x) = 0$ or $h(x) = 0$. We have shown that F has no zero divisors. It remains to show that every nonzero element of F has a multiplicative inverse. So let $g(X)$ a nonzero polynomial of degree $< n$. As $f(X)$ is irreducible, it must be coprime to $g(X)$. We use the **Euclidean algorithm** (see Section 1.7) in the polynomial ring $\mathbb{F}_q[X]$. One of the most important consequences of the Euclidean algorithm is that the greatest common divisor (a, b) of elements a, b can be written in the form $(a, b) = u \cdot a + v \cdot b$. In our situation we have $(g(X), f(X)) = 1$ as $f(X)$ is irreducible. We can therefore find polynomials such that $1 = g(X)h(X) + f(X)l(X)$. If we read this mod $(f(X))$ we get $1 = g(x)h(x)$ and have found the multiplicative inverse. In fact, these arguments are valid for any ground field. We have shown the following:

1.71 Theorem. *Let K be a field and $f(X)$ an irreducible monic polynomial of degree n over K. Then $F = K[X]/(f(X))$ is a field. It contains K as a subfield and is a vector space of dimension n over K. If x denotes the image of X mod $f(X)$, then the $x^i, i = 0, 1, \ldots, n-1$ form a basis of F as a K-vector space. We call n the* **degree** *of F over K.*

In order to illustrate this mechanism we construct the field $\mathbb{F}_4$ of 4 elements.

1.72 Example. *The only irreducible polynomial of degree 2 over $\mathbb{F}_2$ is $f(X) = X^2 + X + 1$. Let us check that $f(X)$ is indeed irreducible: if it was reducible it would have a root. As $f(0) = f(1) = 1 \neq 0$ we conclude that $f(X)$ is irreducible. We have $\mathbb{F}_2[X]/(f(X)) = \{0, 1, x, x+1\}$, where x is the image of X mod $(f(X))$. We have $1 = f(X) + X(X+1)$. Reading this mod $(f(X))$ we obtain $1 = x(x+1)$. It follows that x and $x+1$ are multiplicative inverses. We conclude that $\mathbb{F}_2[X]/(f(X)) = \{0, 1, x, x+1\} = \mathbb{F}_4$ is a field with 4 elements.*

We accept from field theory the fact that an **algebraic closure** always exists and is uniquely determined. Denote by $\overline{\mathbb{F}}_p$ a fixed algebraic closure of $\mathbb{F}_p$. Recall that this means two things: firstly every element $a \in \overline{\mathbb{F}}_p$ is **algebraic** over $\mathbb{F}_p$, that is it satisfies a polynomial equation with coefficients in $\mathbb{F}_p$. Secondly, $\overline{\mathbb{F}}_p$ is **algebraically closed,** equivalently every polynomial with coefficients in $\overline{\mathbb{F}}_p$ splits into linear factors over that same field. Consider the polynomial $X^{p^n} - X$. Assume a field with p^n elements exists. As it is finite it must be algebraic over $\mathbb{F}_p$, so it can be considered as a subfield of $\overline{\mathbb{F}}_p$. As the multiplicative group of this field has order $p^n - 1$, each nonzero element u satisfies $u^{p^{n-1}} = 1$. Thus every element of a field of p^n elements is a root of our polynomial. We see that a field of order p^n is uniquely determined as a subfield of the algebraic closure, if it exists. On the other hand, the polynomial $X^{p^n} - X$ has p^n different roots. It suffices to check that these do form a field. As we are working inside a field it is sufficient to prove that sums, products and multiplicative inverses of roots are roots. For products and inverses this is obvious. For sums this is a consequence of the following lemma:

1.73 Lemma (Frobenius automorphism). *Let F be a field of characteristic p. Then the mapping σ, where $\sigma(x) = x^p$, is a field automorphism from F onto the field F^p of p-th powers. In the case of a finite field we have $F^p = F$. The fixed field of σ is $\mathbb{F}_p$.*

Proof. It suffices to prove that σ is linear with respect to addition and multiplication. In the case of multiplication this is obvious. Consider addition: obviously the binomial theorem applies, hence $(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i}$. Here the binomial coefficients are field elements, hence in $\mathbb{F}_p$. We see that

$\binom{p}{i}$ is divisible by p and hence $= 0$ unless $i = 0$ or $i = p$. Hence the sum simplifies, giving the desired result: $(x + y)^p = x^p + y^p$. $\square$

We conclude that our field of p^n elements exists and is uniquely determined.

1.74 Theorem. *For every prime p and natural number n there is a field with p^n elements. Moreover a fixed algebraic closure $\overline{\mathbb{F}_p}$ contains precisely one subfield with p^n elements, consisting of the roots of the polynomial $X^{p^n} - X$. We denote this field by $\mathbb{F}_{p^n}$.*

Once a field $\mathbb{F}_{q^n}$ is constructed we can go through the same process and construct fields of q^{nk} elements as extensions of $\mathbb{F}_{q^n}$, for every k. As we saw that these fields are uniquely determined we conclude that $\mathbb{F}_{q^n} \subset \mathbb{F}_{q^m}$ provided n divides m. On the other hand, assume $\mathbb{F}_{q^n} \subset \mathbb{F}_{q^m}$. Then the big field is a vector space over the small field. It follows that q^m must be a power of q^n, so n divides m. We have seen the following:

1.75 Theorem. *We have $\mathbb{F}_{q^n} \subseteq \mathbb{F}_{q^m}$ if and only if n divides m.*

What is the structure of the multiplicative group of $\mathbb{F}_q$. Recall that this is a group of order $q - 1$.

1.76 Theorem. *The multiplicative group of the field $\mathbb{F}_q$ is cyclic.*

Proof. Let $d \mid q - 1$. Every element $x \in \mathbb{F}_q^*$ satisfying $x^d = 1$ is a root of the polynomial $X^d - 1$ (with coefficients in the field $\mathbb{F}_p$). As polynomials of degree $d > 0$ cannot have more than d roots it follows that there are at most d solutions of the equation $x^d = 1$. Assume an element x of order d exists. It generates a cyclic subgroup $\langle x \rangle$ of order d. The elements of $\langle x \rangle$ are all the elements satisfying $x^d = 1$. It follows that the number of elements of order d in $\mathbb{F}_q$ is the number of generators of Z_d, which by Theorem 1.30 is $\phi(d)$. We have seen that for every divisor d of the group order $q - 1$ the number of elements of order d is either 0 or $\phi(d)$. Comparison with Theorem 1.31 shows that it is impossible that our group has no elements of order $q - 1$. The group is therefore cyclic. $\square$

1.77 Corollary. *Let q be an odd prime-power. Then -1 is a square in $\mathbb{F}_q$ if and only if $q \equiv 1 (mod\ 4)$.*

Proof. We have just seen that the multiplicative group of $\mathbb{F}_q$ is cyclic. The element -1 is the unique involution (= element of order 2) in this group. It is a square if and only if elements of order 4 exist. □

To sum up: we have found, for every $q = p^m$, a uniquely determined field $\mathbb{F}_q$ of q elements. Consider its extension field $\mathbb{F}_{q^n}$.

1.78 Lemma. *Consider the field extension $\mathbb{F}_{q^n} \supset \mathbb{F}_q$ for some prime-power q. The mapping σ, where $\sigma(x) = x^q$, is a field automorphism of $\mathbb{F}_{q^n}$* **over** *$\mathbb{F}_q$, this last term meaning that each element of the ground field is fixed under σ. More precisely we have $\sigma(x) = x$ if and only if $x \in \mathbb{F}_q$. The powers of σ form a group of automorphisms of order n. We call this group the Galois group $G(\mathbb{F}_{q^n}|\mathbb{F}_q)$.*

Proof. Our σ is a power of the Frobenius automorphism introduced in Lemma 1.73, so it certainly is a field automorphism of $\mathbb{F}_{q^n}$. As the elements of $\mathbb{F}_q$ satisfy $x^q = x$ we see that each element of $\mathbb{F}_q$ is fixed by σ. For the same reason we see that σ^n acts as the identity mapping on $\mathbb{F}_{q^n}$, and this is not the case for any smaller power of σ. As the polynomial $X^q - X$ of degree q cannot have more than q roots we conclude that the fixed points of σ are precisely the elements of $\mathbb{F}_q$. □

Let us have a look at the smallest fields of non-prime order. It is in general handy to fix the multiplicative structure of the field (simply a cyclic group, as we know) and to determine the additive structure afterwards, using the irreducible polynomial. Write $\mathbb{F}_q = \{0\} \cup \{\epsilon^i \mid i = 0, 1, \ldots, q-1\}$. We know that the field is independent of the irreducible polynomial $f(X)$ chosen to describe it. However, there are good and bad choices. It is for example advantageous to choose a polynomial such that the image of the indeterminate X becomes a generator of the multiplicative group (a **primitive element**) of the field. The addition in $\mathbb{F}_q$ will be completely known once the $1 + \epsilon^i$ are known for all i.

$\mathbb{F}_4$: The only irreducible $\mathbb{F}_2$-polynomial of degree 2 is $f(X) = X^2 + X + 1$. It follows $1+\epsilon = \epsilon^2$. This determines the addition. For example $1+\epsilon^2 = \epsilon, \epsilon + \epsilon^2 = \epsilon(1+\epsilon) = \epsilon\epsilon^2 = 1$.

$\mathbb{F}_8$: We choose $f(X) = X^3 + X^2 + 1$, hence $1 + \epsilon^2 + \epsilon^3 = 0$. Further $1 + \epsilon^4 = (1+\epsilon^2)^2 = (\epsilon^3)^2 = \epsilon^6$, and then necessarily $1 + \epsilon = \epsilon^5$. We know that these relations:

$$1+\epsilon^2+\epsilon^3=0,\ 1+\epsilon^4=\epsilon^6,\ \text{and } 1+\epsilon=\epsilon^5$$

determine the field structure completely. As an example, $\epsilon^3+\epsilon^4=\epsilon^3(1+\epsilon)=\epsilon^3\epsilon^5=\epsilon$.

$\mathbb{F}_9$: Take X^2-X-1 as irreducible polynomial. This leads to the relation $\epsilon^2=\epsilon+1$. Then $\epsilon^3=-\epsilon+1, \epsilon^4=-1$, as it should be.

1.22 Linear groups

Recall from linear algebra the product formula $det(AB)=det(A)det(B)$ for the determinants of $(n,n)-$matrices. Also, such a square matrix A is invertible if and only if $det(A)\neq 0$. Here the inverse A^{-1} is defined by $AA^{-1}=I$, where I is the unit matrix. This theory works not only over the reals, the complex numbers and the rationals. It works over any field. We can now understand the meaning of these laws: the invertible matrices form a group, with the unit matrix as neutral element. Moreover the determinant is a group homomorphism from this group to the multiplicative group of the underlying field.

1.79 Definition. *Let F be a field and n a natural number. The* **general linear group** *$GL(n,F)$ is the group of all $(n,n)-$matrices A with entries from F, which satisfy $det(A)\neq 0$.*

1.80 Theorem. *The determinant is a surjective (onto) homomorphism from the group $GL(n,F)$ to the multiplicative group of the field.*

It is in fact clear that det is onto.

1.81 Definition. *The kernel of the homomorphism det in $GL(n,F)$ is denoted by $SL(n,F)$, the* **special linear group.**

Let us specialize to $F=\mathbb{F}_q$. In that case one uses the shorter notation $GL(n,q), SL(n,q)$ instead of $GL(n,\mathbb{F}_q), SL(n,\mathbb{F}_q)$. Our groups consist of quadratic matrices, and matrices act in a natural way on vectors. Denote the space of vectors of length n by $\mathbb{F}_q^n$. If $x\in\mathbb{F}_q^n$ and $A\in GL(n,q)$, then $xA\in\mathbb{F}_q^n$. This gives us a permutation representation of $GL(n,q)$ on the vectors. The 0-vector is fixed by all matrices. These functions $x \mapsto xA$ are **linear functions** because they satisfy the linearity conditions

$$(x+y)A = xA + yA \text{ and } (\lambda x)A = \lambda xA, \text{ where } \lambda \in \mathbb{F}_q.$$

Naturally $GL(n,q)$ also permutes the subspaces of any fixed dimension of the n-dimensional vector space $\mathbb{F}_q^n$. Consider the 1-dimensional subspaces. As there are $q^n - 1$ nonzero vectors and each 1-dimensional space contains $q-1$ of them, the number of 1-dimensional subspaces is $(q^n-1)/(q-1)$.

1.82 Proposition. *$GL(n,q)$ has a transitive faithful permutation representation of degree $q^n - 1$ on the nonzero vectors, and it has a transitive permutation representation on the $(q^n-1)/(q-1) = q^{n-1} + q^{n-2} + \cdots + q + 1$ one-dimensional subspaces.*

Let g be in the kernel of the action of $GL(n,q)$ on the 1-dimensional subspaces. Denote by e_i the vector with entry 1 in coordinate i, entry 0 otherwise. The e_i form the standard basis. As the spaces $\mathbb{F}_q e_i$ generated by the e_i must be mapped to itself, g is a diagonal matrix $diag(\lambda_1, \lambda_2, \ldots, \lambda_n)$. Consideration of $\mathbb{F}_q(e_i - e_j)$ shows $\lambda_i = \lambda_j$, in other words g is a scalar matrix. As all scalar matrices have the required property, we have determined the kernel.

1.83 Proposition. *The kernel Z of $GL(n,q)$ in its action on the 1-dimensional subspaces consists of the scalar matrices $diag(\lambda, \ldots, \lambda)$, where $\lambda \in \mathbb{F}_q^*$. It follows from Theorem 1.76 that $Z \cong Z_{q-1}$.*

1.84 Definition. *The group $PGL(n,q) = GL(n,q)/Z$ is the* **projective general linear group.** *It has a faithful transitive action on the 1-dimensional subspaces.*

Let us determine the orders of the linear groups. Fix a basis, for example the standard basis $e_1, e_2, \ldots, e_n$. A linear function (matrix) is uniquely determined by the images of the e_i (the image of e_i is row number i of the matrix). This matrix will be invertible if and only if the image of our basis forms a basis again. We conclude that $GL(n,q)$ is in bijection with the ordered bases of our space $\mathbb{F}_q^n$. Let us count these bases: The first vector v_1 is an arbitrary nonzero vector. There are $q^n - 1$ choices for v_1. Once v_1 is fixed, it generates a 1-dimensional subspace. The second vector of our basis can be chosen from the vectors not in $\mathbb{F}_q v_1$. The number of choices is $q^n - q$. The number of choices for the pair (v_1, v_2) is $(q^n - 1)(q^n - q)$. Continue counting in this fashion. Assume $v_1, v_2, \ldots, v_i$ have already been chosen, where $i < n$. The number of choices for v_{i+1} is $q^n - q^i$, as the vectors from the subspace generated by $v_1, v_2, \ldots, v_i$ are forbidden. We obtain the following formula:

1.85 Theorem.

$$|GL(n, q)| = (q^n - 1)(q^n - q) \cdot \ldots (q^n - q^{n-1})$$

$$|SL(n, q)| = |PGL(n, q)| = |GL(n, q)|/(q - 1).$$

1.86 Proposition. *We have* $|Z \cap SL(n, q)| = gcd(n, q - 1)$.

Proof. A scalar matrix $diag(\lambda, \ldots, \lambda)$ has determinant 1 if and only if $\lambda^n = 1$. The number of solutions λ is given by Proposition 1.32. □

1.87 Definition. *The factor group* $PSL(n, q) = SL(n, q)/(Z \cap SL(n, q))$ *is the* **projective special linear group.** *Its order is clearly* $|PSL(n, q)| = |SL(n, q)|/gcd(n, q - 1)$.

In case $q = 2$ there are no scalar multiples. It follows that $GL(n, 2) = SL(n, 2) = PGL(n, 2) = PSL(n, 2)$. The group $GL(2, 2)$ has order 6. It possesses a faithful action on the 3 nonzero vectors, hence is a subgroup of S_3. We conclude $GL(2, 2) \cong S_3$. The group $GL(3, 2)$ has order $(2^3 - 1)(2^3 - 2)(2^3 - 2^2) = 168$. Its transitive faithful action on the 7 nonzero vectors shows that $GL(3, 2) < S_7$.

Consider the group $SL(2, 3)$, of order 24. Clearly the scalar matrix $-1 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in SL(2, 3)$, and it has order 2. Here are some more matrices in $SL(2, 3)$:

$$a = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, b = \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}, ab = -ba = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Each of these matrices has order 4. They form a subgroup.

1.88 Proposition. *The matrices* $\pm 1, \pm a, \pm b, \pm ab$ *form a subgroup* $Q_8 < SL(2, 3)$. *The group* Q_8 *is known as the* **quaternion group.** *It has only one element of order 2 and 6 elements of order 4.*

1.23 Group automorphisms and conjugation

The most fruitful source of groups is the idea of symmetry groups. Can't we use groups as the underlying structure and consider symmetries of groups? This is a natural procedure. Symmetries of groups are known as automorphisms.

1.89 Definition. *A group isomorphism $f : G \longrightarrow G$ is an* **automorphism** *of G (see also Section 1.10). The automorphisms of a group G form a group $Aut(G)$, the* **automorphism group** *of G.*

We want to describe how a certain subgroup of $Aut(G)$ can be constructed in a unified way. The basic idea is conjugation.

1.90 Definition. *The* **conjugation** *of $x \in G$ by $y \in G$ is*

$$x^y = y^{-1}xy.$$

An element x^y is a **conjugate** *of x.*

This operation has made its appearance in Section 1.13 already. A subgroup $N < G$ is a normal subgroup if and only if N is closed under conjugation in G. Here we want to show that conjugation is an automorphism.

1.91 Theorem. *Conjugation with $y \in G$ is an automorphism. If we denote it by $I(y)$, then the mapping $G \longrightarrow Aut(G)$ given by $y \mapsto I(y)$ is a group homomorphism. Its image is called the* **inner automorphism group** *$Inn(G)$. The $I(y)$ are* **inner automorphisms.**

Proof. First we show that $I(y)$ is a group homomorphism. This follows from

$$a^y b^y = (y^{-1}ay)(y^{-1}by) = y^{-1}aby = (ab)^y$$

and $(a^{-1})^y a^y = (y^{-1}a^{-1}y)(y^{-1}ay) = e$. Consider the equation $x^y = z$, where y is fixed. It has a unique solution $x = yzy^{-1}$. This proves that conjugation by y is a bijection, and hence an automorphism.

In order to show that $y \mapsto I(y)$ is a group homomorphism we must show $I(y)I(z) = I(yz)$ and $I(y^{-1}) = I(y)^{-1}$. Let us prove the first statement:

$$(x^y)^z = z^{-1}y^{-1}xyz = (yz)^{-1}x(yz) = x^{yz}.$$

The second statement is another easy formality. $\square$

1.92 Proposition. *The kernel of the homomorphism* $: G \longrightarrow Inn(G)$ *given by conjugation is the* **center** *of* G :

$$\mathbb{Z}(G) = \{x : x \in G, xy = yx \text{ for all } y \in G\}$$

Proof. $y \in G$ is in the kernel of our mapping if conjugation by y fixes every group element $x \in G$. This means $y^{-1}xy = x$, equivalently $xy = yx$. □

By the first isomorphism theorem we have $Inn(G) \cong G/\mathbb{Z}(G)$. The fact that conjugation is a group automorphism has important consequences, as follows: For every $A \subseteq G$ and $g \in G$ we call A^g a conjugate of A. If A is a subgroup, then A and A^g are isomorphic groups, and they play symmetric roles in G. Conjugate group elements have the same orders, and so forth.

1.24 Commutators

The **commutator** of group elements $x, y \in G$ is defined as

$$[x, y] = x^{-1}y^{-1}xy.$$

Observe that $[x, y] = x^{-1}x^y$. In particular $[x, y] = 1$ if and only if x and y commute. Also, the image of a commutator under a group homomorphism α is a commutator again: $\alpha([x, y]) = [\alpha(x), \alpha(y)]$. The **commutator group** of G is defined as the subgroup generated by the commutators. It is often denoted by G' :

$$G' = [G, G] = \langle [x, y] : x, y \in G \rangle$$

As the image of a commutator under conjugation in G is a commutator we have that $G' \trianglelefteq G$ is a normal subgroup.

1.93 Lemma. *The commutator group* G' *is the smallest normal subgroup* $N \trianglelefteq G$ *such that* G/N *is abelian.*

Proof. Observe at first that a group G is abelian if and only if $G' = 1$, in other words if all commutators are 1. It follows that a factor group G/N is abelian if and only if $G' \subseteq N$. □

1.25 Characteristic subgroups

The relation of being a normal subgroup is not transitive. It is easy to find examples. Recall that a subgroup $H < G$ is normal if and only if it is stable under inner automorphisms ($H^g = H$ for all $g \in G$).

1.94 Definition. *A subgroup $H < G$ is a* **characteristic subgroup** *if $\alpha(H) = H$ for every $\alpha \in Aut(G)$.*

A characteristic subgroup is also normal. The concept of a characteristic subgroup is important because of the following obvious property:

1.95 Proposition. *If H is a characteristic subgroup of K and $K \trianglelefteq G$, then $H \trianglelefteq G$.*

We have seen in the preceding section that the image of a commutator under a group homomorphism is a commutator. This implies that the commutator subgroup G' is a characteristic subgroup of G.

1.26 The semidirect product

The semidirect product is an important generalization of the direct product from Section 1.12.

1.96 Definition. *Let G be a group and $\pi : A \longrightarrow Aut(G)$ a group homomorphism. We define a group structure on $G \times A$ as follows:*

$$(g_1, a_1)(g_2, a_2) = (g_1 g_2^{\pi(a_1^{-1})}, a_1 a_2).$$

This is the **semidirect product** *of G and A with respect to π.*

The direct product corresponds to the special case when π is the trivial homomorphism with image 1. If we identify $g \in G$ with $(g, 1)$ and $a \in A$ with $(1, a)$, then we see G and A as subgroups of the semidirect product, which we also write simpler as GA. Moreover G is a normal subgroup and conjugation in GA of an element $g \in G$ with some $a \in A$ is the same as application of the automorphism $\pi(a)$. Application of the automorphism $\pi(a)$ to the element $g \in G$ is the same as conjugation of g by $\pi(a)$ in the semidirect product. Typically one chooses A as a subgroup of $Aut(G)$ and π as the identity mapping.

1.97 Example. *Let G be an abelian group. Then $g \mapsto g^{-1}$ is an involutory automorphism. This defines a semidirect product GZ, where $|Z| = 2$. When $G = Z_n$ is cyclic the semidirect product GZ is the dihedral group D_{2n} from Section 1.18. Let us check that every element in $D_{2n} \setminus Z_n$ is an* **involution** *(= element of order 2): such an element has the form gz, where $\langle z \rangle = Z$. We have*

$$(gz)^2 = g(zg)z = g(g^{-1}z)z = z^2 = 1.$$

1.27 Permutation representations inside G

Let the group G be given. How can we in general find and describe the sets Ω on which G acts transitively? At first we need a precise notion, when two permutation representations are essentially the same. This is very natural:

1.98 Definition. *Let two permutation representations of G be given: π_1 on Ω_1 and π_2 on Ω_2. We call π_1 and π_2* **similar** *if there is an automorphism $\alpha : G \longrightarrow G$ and a bijection $\beta : \Omega_1 \mapsto \Omega_2$ such that for all $i \in \Omega_1$ and $g \in G$ we have*

$$\beta(i\pi_1(g)) = \beta(i)\pi_2(g^\alpha).$$

In most cases the automorphism α will be the identity.

The methods and notions developed so far (subgroups, cosets, conjugation,...) motivate two general constructions for permutation representations, which arise out of the group structure itself:

1.99 Definition. *Let G be a group, let Ω consist of the subsets of G of some fixed cardinality, and let $A \subseteq G$ be such a subset. We consider two permutation representations of G on Ω :*

- **multiplication:** *g maps A to Ag.*
- **conjugation:** *g maps A to $A^g = g^{-1}Ag$.*

We are certainly interested in determining the kernels and the stabilizers. This automatically leads to the following notions:

1.100 Definition. *Let $A \subseteq G$ be a subset of G. The* **centralizer** *of A in G is*

$$\mathbb{C}_G(A) = \{g : g \in G, a^g = a \text{ for all } a \in A\}.$$

The **normalizer** *of A in G is defined as*

$$\mathbb{N}_G(A) = \{g : g \in G, A^g = A\}.$$

Another way of looking at the normalizer is the following: The normalizer $\mathbb{N}_G(A)$ of a subgroup $A \leq G$ is the largest subgroup of G, which contains A as a normal subgroup. For example, if $A \lhd G$, then $\mathbb{N}_G(A) = G$. The order of $\mathbb{N}_G(A)$ measures how far A is from being normal. Clearly $A \leq \mathbb{N}_G(A) \leq G$.

Observe that $a^g = a$ is equivalent with $ag = ga$. The normalizer of A is the stabilizer of A under the conjugation representation. The orbit lemma implies the following:

1.101 Theorem. *Let $A \subseteq G$. The number of different conjugates $A^g, g \in G$ is the index $[G : \mathbb{N}_G(A)]$.*

If $A = \{g\}$ is a subset consisting of just one element, then clearly the notions of normalizer and centralizer coincide. We record the corresponding special case of Theorem 1.101:

1.102 Corollary. *Let $g \in G$. The number of different conjugates of g is the index $[G : \mathbb{C}_G(g)]$.*

Observe the following obvious special cases: $\mathbb{C}_G(e) = G$ and $\mathbb{C}_G(G) = \mathbb{Z}(G)$ (compare Proposition 1.92).

The case of multiplication from the right is just as important as conjugation. Let H be a subgroup of G. The orbit of H under the multiplication representation clearly consists of the different right cosets Hg and the stabilizer of H is H. The orbit lemma implies that the number of right cosets (the length of the orbit) is $[G : H]$, but we knew this already (see Section 1.6). Finally we show that multiplication from the right is in principle sufficient to describe all transitive permutation representations.

1.103 Theorem. *Let G act transitively on $\Omega, i \in \Omega$ and $H = G_i$ the stabilizer of i. Then the action of G on Ω is similar to the action of G on the right cosets of H by multiplication from the right.*

Proof. Let Ω' consist of the different right cosets of H. We have $|\Omega'| = [G : H] = |\Omega|$. Let $j \in \Omega$. Because of transitivity there is some $g \in G$ mapping $i \mapsto j$ and we have seen in Theorem 1.62 that all the elements mapping $i \mapsto j$ form the coset Hg. This gives us the desired bijection. $\square$

1.28 Conjugacy classes

1.104 Definition. *The* **conjugacy class** *of $g \in G$ is the set g^G of all conjugates of g.*

A conjugacy class is by definition an orbit of G in its representation by conjugation on elements of G. It follows that G is the disjoint union of conjugacy classes. We have noted in Corollary 1.102 that as a consequence of the orbit length lemma we have $|g^G| = [G : \mathbb{C}_G(g)]$. This gives us the opportunity to express the normal subgroup condition in yet another fashion:

1.105 Theorem. *A subgroup $N \leq G$ is a normal subgroup if and only if it is a union of conjugacy classes of G.*

In fact, the defining condition of normality is $N^g = N$ for every $g \in G$. This says that every conjugate of an element in N must be in N again.

What are the conjugacy classes in the symmetric groups? We start from a useful formula:

1.106 Lemma. *The conjugate of the m-cycle $(1, 2, 3, \ldots, m)$ under the permutation π is*

$$(1, 2, 3, \ldots, m)^\pi = (\pi(1), \pi(2), \ldots, \pi(m)).$$

In particular the conjugate of an m-cycle is an m-cycle.

Proof. This is easy to verify. The image of $\pi(i)$ under $(1, 2, 3, \ldots, m)^\pi = \pi^{-1}(1, 2, 3, \ldots, m)\pi$ is $\pi(i + 1)$ (where the i are mod m). $\square$

As an example, consider the permutation $(1, 2, 5, 3)$. The conjugate under $(1, 3, 5)$ is

$$(1, 2, 5, 3)^{(1,3,5)} = (3, 2, 1, 5) = (1, 5, 3, 2).$$

The conjugacy class of an m-cycle in S_n consists of m-cycles. It is clear from Lemma 1.106 that the m-cycles form one conjugate class.

1.107 Definition. *If a permutation π can be written as a product of disjoint cycles of lengths $m_1, m_2, \ldots, m_k$, where $m_1 \geq m_2 \geq \cdots \geq m_k$ we call $(m_1, m_2, \ldots, m_k)$ the* **cycle type** *of π.*

We know from Section 1.4 that the cycle type is uniquely determined. Lemma 1.106 shows that conjugate permutations have the same cycle type, and it is also clear that any two permutations of the same cycle type are conjugate in the symmetric group. We record this:

1.108 Theorem. *The permutations of same cycle type are the conjugacy classes in S_n.*

As an example, consider permutations $(1,2)(3,4)$ and $(1,4)(2,3)$ (of cycle type $(2,2)$) in S_4. How can we find an element $\pi \in S_4$ conjugating $(1,2)(3,4)$ into $(1,4)(2,3)$? By Lemma 1.106 it suffices to choose $\pi : 1 \mapsto 1, 2 \mapsto 4, 3 \mapsto 2, 4 \mapsto 3$, hence $\pi = (2,4,3)$. Another choice is $\pi = (1,4,3,2)$.

The normal subgroup $V \lhd S_4$ is the union of the neutral element (forming a conjugacy class, of course) and of the permutations with cycle type $(2,2)$.

1.29 Products of subgroups

Let A and B be subgroups of G. Clearly $A \cap B \leq G$. On the other hand, it is easy to find examples showing that the product

$$AB = \{ab : a \in A, b \in B\}$$

is not always a subgroup. The concept of a normalizer (see Definition 1.100) helps us to describe situations when AB is a subgroup.

1.109 Theorem. *Let A and B be subgroups of G. Assume that either $B \leq \mathbb{N}_G(A)$ or $A \leq \mathbb{N}_G(B)$. Then $AB \leq G$ and $AB = BA$.*

Proof. Assume without restriction $B \leq \mathbb{N}_G(A)$. Observe that this means that every product ba can be written as $a'b$ for some $a' \in A$. We obtain

$$aba'b' = a(ba')b = a(a''b)b' \in AB.$$

This shows that AB is closed under products. A similar calculation shows it is closed under inverses. $\square$

1.110 Theorem (second isomorphism theorem). *Let A, B be subgroups of G and $B \leq \mathbb{N}_G(A)$. Then*

$$AB/A \cong B/(A \cap B).$$

Proof. Let us make sure that everything makes sense. AB is a subgroup by Lemma 1.109, and A is of course normal in AB. It is also clear that $A \cap B \trianglelefteq B$. Let $f : AB \longrightarrow AB/A$ be the canonical homomorphism and g the restriction of f to B (this means $g(b) = Ab$.) Then $Im(g) = AB/A$. By the first isomorphism theorem we have $AB/A \cong B/Ker(g)$. As $Ker(g) = Ker(f) \cap B = A \cap B$ we are done. $\square$

The concept of conjugation is particularly fruitful. We showed in Section 1.23 how conjugation allows us to construct the inner automorphisms. In the case when G is abelian the inner automorphism group is trivial. Here is a more general method to construct automorphisms.

1.111 Theorem. *Let $A \leq G$. Then $\mathbb{C}_G(A)$ is a normal subgroup of $\mathbb{N}_G(A)$ and the factor group $\mathbb{N}_G(A)/\mathbb{C}_G(A)$ is isomorphic to a subgroup of $Aut(A)$. We call $\mathbb{N}_G(A)/\mathbb{C}_G(A)$ the group of automorphisms of A* **induced by** *G.*

Proof. It is clear that $\mathbb{C}(A) \leq \mathbb{N}(A)$ are subgroups. Let $h \in \mathbb{C}(A), g \in \mathbb{N}(A), a \in A$. Then $a^{h^g} = a^{g^{-1}hg} = a^{g^{-1}g} = a$ as $a^{g^{-1}} \in A$, and therefore is centralized by h. This shows $h^g \in \mathbb{C}(A)$. It follows $\mathbb{C}(A) \trianglelefteq \mathbb{N}(A)$.
Every $g \in \mathbb{N}(A)$ acts on A by conjugation. We have seen that this is an automorphism of A (see the proof of Theorem 1.91). This defines a group homomorphism : $\mathbb{N}(A) \longrightarrow Aut(A)$. An element $g \in A$ is in the kernel if and only if $a^g = a$ for all $a \in A$, equivalently if $g \in \mathbb{C}(A)$. This proves our last claim, by the first isomorphism theorem. □

Consider the group $V \triangleleft S_4$. As V is (elementary) abelian, it has no inner automorphisms. Apply Theorem 1.111. The normalizer of V is all of S_4. It is easy to see that the centralizer is just V itself. Consequently $S_4/V \subseteq Aut(V)$. We have seen in Proposition 1.56 that $S_4/V \cong S_3$. This shows $S_3 \leq Aut(V)$. On the other hand, V has only three non-neutral elements and every automorphism of V is a permutation of these. The automorphism group of V can therefore not be larger than S_3. We have $Aut(V) \cong S_3$ and all automorphisms of V are induced by S_4.

1.30 p-groups and Sylow's theorems

We are now equipped to tackle the most important and deepest problem in elementary group theory. Our very first structural theorem was the theorem of Lagrange (Theorem 1.16): the order of any subgroup divides the order of the group. It is natural to ask when the reverse holds. Given a divisor d of the group order, when is there a subgroup of order d and what can we say about its structure. Sylow's theorems give an affirmative answer in the case when d is a prime-power. This directs our attention to $p-$groups.

1.112 Definition. *A finite group P is a $p-$group if its order is a power of p.*

There is something special about $p-$groups. For example, the center of a p-group is never trivial.

1.113 Theorem. *Let P be a nontrivial p-group. Then $\mathbb{Z}(P)$ is nontrivial.*

Proof. Consider the partition of P into conjugacy classes. The length of every conjugacy class, being the index of a subgroup (see Corollary 1.102), is a power of p. An element $g \in P$ is in the center if and only if it forms a conjugacy class of length 1. As e certainly is central, it follows that at least $p - 1$ more elements of P must be central. □

1.114 Lemma. *Let the p-group P act on the set Ω. Denote by $F_\Omega(P)$ the set of fixed points. Then $|F_\Omega(P)| \equiv |\Omega|$ (mod p).*

Proof. This argument is similar to the proof of Theorem 1.113 (in fact, it is a generalization). By the orbit length lemma all orbits have length a power of p and the orbits of length 1 are precisely the fixed points. □

1.115 Theorem (The Sylow theorems). *Let G be a finite group of order $p^n m$, where m is coprime to the prime p. Then the following hold:*

1. *G possesses a subgroup of order p^n (such subgroups are called p-**Sylowsubgroups**).*

2. *All p-Sylowsubgroups of G are conjugate (in particular they are isomorphic). Their number is*

$$[G : \mathbb{N}_G(P)] \equiv 1 \ (mod\ p).$$

   Here P denotes a p-Sylowsubgroup.

3. *$P \leq G$ is a p-Sylowsubgroup of G if and only if P is a p-group and p does not divide $|\mathbb{N}_G(P)/P|$.*

4. *If $R \leq G$ is a p-group, then R is contained in a p-Sylowsubgroup.*

The set of all p-Sylowsubgroups of G is denoted by $Syl_p(G)$.

Here is an application of the Sylow theorems:

1.116 Theorem (the Frattini argument). *Let $P \leq N \trianglelefteq G$, where $P \in Syl_p(G)$. Then $G = N\mathbb{N}_G(P)$.*

Proof. Let $g \in G$. We have $P^g \in Syl_p(N)$. As by Sylow's theorems all p-Sylowsubgroups of N are conjugate there must exist some $h \in N$ such that $P^g = P^h$. It follows $gh^{-1} \in \mathbb{N}(P)$, thus $g \in \mathbb{N}_G(P)N = N\mathbb{N}_G(P)$. □

1.31 Proof of the Sylow theorems

1.117 Lemma (Cauchy's theorem). *Let the order of G be divisible by p and $m \geq 1$. Then the number of solutions of equation $x^{p^m} = 1$ in G is a multiple of p. Case $m = 1$ shows that G does contain elements of order p.*

Proof. Let $q = p^m, \Omega = \{(x_1, x_2, \dots, x_q) | x_i \in G, x_1 x_2 \cdot \dots x_q = e\}$. We have $|\Omega| = |G|^{q-1}$. If $x_1 x_2 \cdot \dots x_q = e$ then also $x_2 x_3 \cdot \dots x_q x_1 = e$. It follows that the cyclic permutation $(x_1, x_2, \dots, x_q) \mapsto (x_2, \dots, x_q, x_1)$ generates a p-group of permutations of Ω. The fixed points under this group are precisely the q-tupels $(a, a, \dots, a)$, where $a^q = 1$. It follows that they are in bijection with the solutions of equation $x^q = 1$. As $|X|$ is a power of p we conclude from Lemma 1.114 that we are done. □

Cauchy's theorem is a first step in the Sylow direction. It shows that if the group order is divisible by p, then subgroups of order p exist.

Let us denote by $Syl_p(G)$ the set of all p-subgroups of G, which are not contained in a larger p-subgroup. Let $P \in Syl_p(G)$ and $\Omega = \{P^g | g \in G\}$. Clearly P acts on Ω by conjugation. Let Q be a fixed point. This means in clear that $Q \in Syl_p(G)$ is conjugate to P under the action of G and $P \leq I\!N(Q)$. It follows from Theorem 1.109 that PQ is a group. As $PQ/Q \cong P/(P \cap Q)$ by Theorem 1.110 we see that PQ is a p-group. As $P \leq PQ$ and P was chosen maximal, we have $PQ = P$, hence $P = Q$. We have shown that P has exactly one fixedpoint in its action on Ω. It follows from Lemma 1.114 that the cardinality of Ω is $\equiv 1 \pmod p$.
We show next that $\Omega = Syl_p(G)$. Assume $R \in Syl_p(G) \setminus \Omega$, let $\Omega' = \{R^g | g \in G\}$. We have seen above that $|\Omega'| \equiv 1 \pmod p$. The action of P shows, via the same argument, that $|\Omega'| \equiv 0 \pmod p$, contradiction.

We have already proved some of the claims. Next we show that $|P| = p^n$. Observe $[G : P] = [G : I\!N_G(P)][I\!N_G(P) : P]$. Assume $|P| < p^n$. Then $[G : P]$ is a multiple of p. We know that the first factor equals the cardinality of $Syl_p(G)$ and is not divisible by p. It follows that $|I\!N_G(P)/P|$ is divisible by p. By Cauchy's theorem we can find a group of order p in $I\!N_G(P)/P$. This yields a group of order $p \cdot |P|$ containing P, which contradicts the maximality of P. We conclude that $Syl_p(G)$ consists of the subgroups of order p^n. All the statements of the Sylow theorems have been proved.

1.32 Simple groups

If $N \lhd G$, then we can form the factor group G/N. In a way, this decomposes G into smaller groups, N and G/N. Groups which cannot be decomposed in this way at all are called simple groups.

1.118 Definition. *A group G is* **simple** *if it has no normal subgroups beside $\{e\}$ and G.*

As every subgroup of an abelian group is normal and because of Sylow's theorems it is clear that the only abelian simple groups are the cyclic groups Z_p, p a prime. Are there any non-abelian simple groups?

1.119 Theorem. *The alternating group A_5 is simple.*

Proof. Let us write down at first the conjugacy classes of S_5. These are in bijection with the 7 partitions of the number 5 (see Theorem 1.108). We obtain the following table:

number	representative	centralizer	length
1	e	S_5	1
2	$(1,2,3,4,5)$	$\langle(1,2,3,4,5)\rangle$	24
3	$(1,2,3)$	$\langle(1,2,3)(4,5)\rangle \cong Z_6$	20
4	$(1,2)$	$\langle(1,2)\rangle \times S_3$	10
5	$(1,2)(3,4)$	$\langle(1,3,2,4),(1,2)\rangle \cong D_8$	15
6	$(1,2,3,4)$	$\langle(1,2,3,4)\rangle$	30
7	(1,2,3)(4,5)	$\langle(1,2,3)(4,5)\rangle \cong Z_6$	20

The normal subgroup A_5 of order 60 consists of the union of conjugacy classes 1,2,3,5 (the even permutations). Let $g \in A_5$. The orbit length lemma shows the following: if$\mathbb{C}(g) \subseteq A_5$, then the conjugacy class g^{S_5} splits into two conjugacy classes of equal length in A_5. In the contrary case, when$\mathbb{C}(g) \not\subseteq A_5$, then $g^{S_5} = g^{A_5}$. Upon inspection of the table we see that A_5 has five conjugacy classes of lengths 1,12 (5-cycles),12 (5-cycles),20 (3-cycles),15 (products of two transpositions).

Assume $\{e\} < N \lhd A_5$. Then N is a union of conjugacy classes of A_5. On the other hand $e \in N$ and $|N|$ must divide 60. This is impossible. □

We can prove more:

1.120 Theorem. *A_5 is the only simple group of order 60.*

Proof. Assume now G is a simple group of order 60. Sylow's theorem gives us $S \in Syl_2(G)$ of order 4, $P \in Syl_5(G), Q \in Syl_3(G)$. We know from Sylow's theorems that $[G : \mathbb{N}(P)] \equiv 1 \pmod 5$ and $\neq 1$ because of the simplicity of G. As $[G : \mathbb{N}(P)]|12$ we see that the only possibility is $[G : \mathbb{N}(P)] = 6$. We have therefore $|\mathbb{N}(P)| = 10$. An analogous argument shows $|\mathbb{N}(Q)| = 6$. We see already that G has 24 elements of order 5 and 20 elements of order 3. The order of 15 elements of G is still in doubt. It is impossible that $\mathbb{N}(P)$ or $\mathbb{N}(Q)$ are cyclic as this would lead either to 24 elements of order 10 or to 20 elements of order 6, which is impossible. In particular G does not contain elements of orders 10 or 6. Let z be an element of order 2 (an **involution**). We have seen that $[G :\mathbb{C}(z)]$ is a multiple of 15. It follows that$\mathbb{C}(z)$ has order 4 and G has 15 involutions, which form a conjugacy class. In particular G does not contain elements of order 4. It follows that $S \cong E(4)$ and that any two different conjugates of S intersect trivially. This show that S has only 5 different conjugates, hence $[G : \mathbb{N}(S)] = 5$. Consider the representation of G by multiplication on the right cosets of $\mathbb{N}(S)$. This is a transitive permutation representation of degree 5, hence a group homomorphism $f : G \longrightarrow S_5$. We know that $Ker(f) \lhd G$. As G is simple it follows $Ker(\alpha) = \{e\}$, so that f is an isomorphism from G onto a subgroup of S_5. Assume $f(G) \neq A_5$. Then $A_5 \cap f(G)$ is a nontrivial normal subgroup of the simple group $f(G)$, contradiction. □

All the alternating groups $A_n, n \geq 5$ are simple. This will be proved in the next chapter. Likewise, the groups $PSL(n, p)$ are simple except for $PSL(2, 2)$ and $PSL(2, 3)$. This will be proved in Section 5.7.

1.33 Composition series

1.121 Definition. *A* **composition series** (K) *of* G *is a chain of subgroups*

$$G = G_0 > G_1 > G_2 > \cdots > G_r = 1,$$

where $G_i \lhd G_{i-1}$ *and* G_{i-1}/G_i *is simple. The* **composition factors** *are factor groups* $G/G_1, G_1/G_2, \ldots, G_{r-1}$, r *is the length of* (K). *Composition series* $(K_1), (K_2)$ *are* **equivalent** *if the length and the composition factors are the same (including multiplicities).*

1.122 Theorem (Jordan-Hölder). *If* G *possesses a composition series, then all composition series of* G *are equivalent (observe that finite groups do possess composition series).*

Proof. Let $(K_1) = (K)$ as in Definition 1.121 and

$$(K_2) : G = H_0 > H_1 > H_2 > \cdots > H_s = 1$$

be two composition series for G. Use induction on r (case $r = 1$ is equivalent with G being simple, and the claim is trivially true in that case). If $G_1 = H_1$, then we are done by induction. We can assume $G_1 \neq H_1$. It follows $G_1 H_1 = G$. Put $L_2 = G_1 \cap H_1$. By the second isomorphism theorem 1.110 we have $G/G_1 \cong H_1/L_2$ and $G/H_1 \cong G_1/L_2$ and both groups are simple. Let (L) be a composition series of L_2. Then (K_1) is equivalent with $G > G_1 > L_2 > (L)$, which is equivalent with $G > H_1 > L_2 > (L)$. As this composition series is equivalent with (K_2) we conclude that (K_1) and (K_2) are equivalent. $\square$

1.34 Solvable and nilpotent groups

1.123 Definition. *A group G is* **solvable** *if every composition factor has prime order.*

Recall that simple groups either have prime order or are nonabelian. The following facts are trivial: If G is solvable, then all subgroups and all factor groups of G are solvable. If $N \lhd G$ is solvable and G/N is solvable, then G is solvable. Repeated application of Theorem 1.113 shows that p-groups are solvable.

1.124 Definition. *A group G is* **nilpotent** *if it is the direct product of its Sylow subgroups, equivalently if G has exactly one (normal) Sylow-p-subgroup for every p.*

1.35 Problems

1. Write the permutation

$$g = (1, 7, 4, 5)(2, 3, 7)(1, 6)(4, 6, 5, 3)$$

in standard form, as a product of disjoint cycles, and determine the order of g.

2. Prove that $(ab)^{-1} = b^{-1}a^{-1}$.

3. Determine the number of generators of the cyclic group of order 3125.
4. Let g have order 165. Determine the order of g^{48}.
5. Write out the group table of a non-abelian group of order 6.
6. Find a normal subgroup of the group D_8.
7. Find all normal subgroups of S_4.
8. Prove that the intersection of two subgroups is a subgroup.
9. Prove that the intersection of two normal subgroups is a normal subgroup.
10. Prove that the symmetry group V from Theorem 1.3 is elementary-abelian.
11. Give an example showing that the image of a homomorphism is not in general a normal subgroup.
12. Let n be an even number and g a fixedpointfree element of order 2 in S_n. Determine the signum of g.
13. Prove the following: if $g \in G, o(g) = n$ and $h \in H, o(h) = m$, then the element $(g, h) \in G \times H$ has order $lcm(n, m)$.
14. Prove the formula $\sum_{d|n} \phi(d) = n$.
15. Prove Proposition 1.32.
16. Show that the subgroups of order 2 in S_3 are not normal.
17. Prove Proposition 1.61.
18. Show that D_{2n} is not abelian when $n > 2$.
19. Find an element of order 3 of the cube group and the corresponding symmetry of the face graph (see Section 1.19).
20. Determine the number of elements of order 3 in the cube group.
21. Let Γ be the graph on $2n$ vertices, which has n disjoint edges. Determine the order of its automorphism group.

22. Determine the center of the quaternion group Q_8.

23. Show that $Q_8 \lhd SL(2,3)$.

24. Find a group of order 8 all of whose subgroups are normal. Is this true of all groups of order 8?

25. Find the symmetry of the cube, which performs the permutation $(A,D)(B,F)(C,E)$ on the faces.

26. Show that the definition of the semidirect product really satisfies the group axioms. In particular prove associativity and determine the inverse of the element (g,a) in the semidirect product of G and A.

27. Determine the length of the conjugacy class of n-cycles in S_n.

28. Prove that $S_3 \cong D_6$.

29. Let H be a subgroup of G. Prove that H is a normal subgroup if and only if $[H,G] \subseteq H$, in words: if all commutators of elements in h and elements in G are in H.

30. Show that the relation of being a characteristic subgroup is transitive.

31. Show that $\mathbb{Z}(G)$ is a characteristic subgroup of G.

32. Determine the order of $Aut(Z_n)$.

33. Show that the elementary-abelian normal subgroup $V \lhd S_4$ is self-centralizing: $\mathbb{C}_{S_4}(V) = V$.

34. Show that there is no simple nonabelian group of order < 60.

35. Prove that all groups of order p^2 are abelian.

36. Determine the centralizer of an $n-$cycle in S_n.

37. Determine the structure of groups whose order is a product of two primes. Hint: Use the Sylow theorems, automorphism groups and the semidirect product.

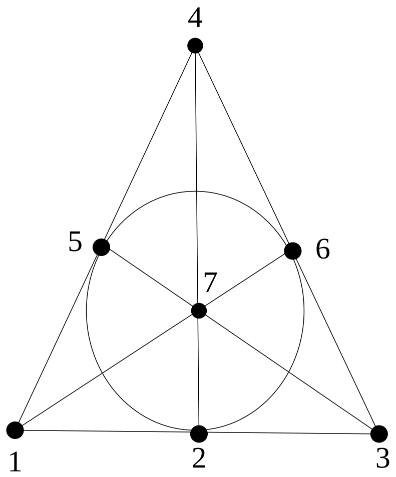


Figure 1.7: The Fano plane

38. Determine the order of the group of symmetries of the **Fano plane.** This group is the subgroup of S_7 consisting of those permutations, which map lines to lines. The lines are the seven 3-element subsets visible from the figure. Do we know that group by name already?

Chapter 2

Permutation groups

Recall the notion of similarity of permutation representations as well as Theorem 1.103, which says that transitive permutation representations can be found inside the group. They correspond simply to subgroups.

2.1 Lemma (Burnside's Lemma). *Let (G, Ω) be a permutation group. Then the following hold:*

1. *If G has t orbits on Ω, then*

$$t|G| = \sum_{g \in G} |F(g)| (\mathbf{Burnside'sLemma})$$

2. *Let G be transitive ($t = 1$) and let G_x have r orbits on Ω. Then r (the* **rank** *of (G, Ω)) is independent of the choice of $x \in \Omega$ and we have*

$$r \cdot |G| = \sum_{g \in G} |F(g)|^2.$$

Proof. 1. Count pairs (g, x), where $g \in G, x \in \Omega, xg = x$ in two ways. This yields $\sum_{x \in \Omega} |G_x| = \sum_{g \in G} |F(g)|$. If Δ is an orbit, then for every $x \in \Delta$ we have $|G_x| = |\Delta|/|\Delta|$. It follows $\sum_{x \in \Delta} |G_x| = |G|$. Claim 1. follows.
2. We know from part 1. that $r \cdot |G_x| = \sum_{g \in G_x} |F(f)|$. For $x, y \in \Omega$ we have that (G_x, Ω) and (G_y, Ω) are equivalent. In fact, pick an element $g \in G$ such that $xg = y$. The similarity (see Definition 1.98) may be defined by $\alpha : h \mapsto h^g$ and $\beta : z \mapsto zg$ (if $h \in G_x$, then $yh^g = (xg)g^{-1}hg = xhg = xg = y$). It follows that r is independent of the choice of x. We calculate $r \cdot |\Omega| \cdot r \cdot G \cdot = \sum_{x \in \Omega} \sum_{g \in G_x} |F(g)| = \sum_{g \in G} \sum_{x \in F(g)} |F(g)| = \sum_{g \in G} |F(g)|^2$. $\square$

Burnside's Lemma says that in the transitive case the average number of fixed points of a group element is 1. As the identity has more than 1 fixed point it follows in particular that there must be fixed-point-free elements.

2.2 Corollary. *If the permutation group (G, Ω) is transitive, $|\Omega| > 1$, then there exists an element $g \in G$ such that $F(g) = \emptyset$.*

2.3 Definition. (G, Ω) *is t-***transitive** *($t \geq 1$) if whenever two t-tuples $(x_1, x_2, \ldots, x_t)$ and $(y_1, y_2, \ldots, y_t)$ of different elements in Ω are given, there exists $g \in G$ such that $x_i g = y_i, i = 1, 2, \ldots, t$ (the x_i have to be pairwise different, also the y_j are pairwise different; nothing is assumed about the relation between the x_i and the y_j).*

It is clear that 1-transitivity is equivalent with transitivity and that t-transitivity implies $(t-1)$-transitivity $(t > 1)$. One may also say that (G, Ω) is t-transitive if and only if G is transitive in its implied operation on t-tuples of pairwise different elements from Ω. The proof of the following lemma is formal and trivial:

2.4 Lemma. *Let (G, Ω) be a permutation group. Then the following are equivalent:*

- *(G, Ω) is t-transitive $(t \geq 1)$.*
- *(G, Ω) is transitive and $(G_x, \Omega - \{x\})$ is $(t-1)$-transitive.*
- *(G, Ω) is $(t-1)$-transitive and for some (all) $(t-1)$-tuple $(x_1, \ldots, x_{t-1})$ we have that $(G_{(x_1,\ldots,x_{t-1})}, \Omega - \{x_1, \ldots, x_{t-1}\})$ is transitive. Here $G_{(x_1,\ldots,x_{t-1})}$ denotes $\cap_{i=1}^{t-1} G_{x_i}$.*

2.5 Corollary. *If (G, Ω) is t-transitive, $|\Omega| = n$, then*
$|G| = n(n-1) \cdot \ldots (n-t+1)|G_{(x_1,\ldots,x_t)}|$.

Proof. This follows by repeated application of the orbit length lemma. □

2.6 Definition (double cosets). *Let $H, K \leq G$. A set HgK for some $g \in G$ is called a* **double coset** *of G for H and K. Observe that HgK is a union of right cosets for H and a union of left cosets for K.*

2.7 Lemma. *Let $H, K \leq G$. The following hold:*

1. *If $x \in HgK$, then $HxK = HgK$.*

2. G is the disjoint union of its different double cosets for H and K.

3. HgK is the union of $|K|/|H^g \cap K|$ right cosets for H and of $|H|/|H^g \cap K|$ left cosets for K.

Proof. 1. $HhgkK = HgK$.
2. follows from 1.
3. $|HgK| = |g^{-1}HgK| = |H^gK| = |H^g| \cdot |K|/|H^g \cap K| = |H| \cdot |K|/|H^g \cap K|$.
The second formula follows in an analogous way. □

2.8 Lemma. *If (G, Ω) is 2-transitive, $g \notin G_x$, then $G = G_x \cup G_x g G_x$ is the union of two double cosets for G_x.*

Proof. Consider g as fixed, choose $g' \in G - G_x$. Because of double transitivity there is some $h \in G_x$ such that $G_x g' = G_x gh$. It follows $g' \in G_x g G_x$. Here we have used Theorem 1.103. □

2.9 Example. *The symmetric group S_n is clearly n-transitive. The alternating group A_n is $(n-2)$-transitive $(n \geq 3)$. For $n = 3$ this is clear. For general n it follows by induction as the stabilizer of a point in A_n is A_{n-1}.*

2.10 Definition (primitivity). *Let (G, Ω) be transitive. Let $\Delta \subset \Omega, |\Delta| > 1$. Δ is a* **region of imprimitivity** *of (G, Ω) if for every $g \in G$ either $\Delta g = \Delta$ or $\Delta g \cap \Delta = \emptyset$. Call (G, Ω)* **primitive** *if it does not contain a region of imprimitivity.*

If $\Delta \subset \Omega$ is a region of imprimitivity, $|\Omega| = n, |\Delta| = m$, then clearly $m|n$ and the number of distinct images of Δ is n/m. We view the permutation representation of G on Ω as composed out of a representation on n/m points (the images of Δ) and a representation of the stabilizer of Δ on Δ.

2.11 Theorem. *Let (G, Ω) be transitive. Then (G, Ω) is primitive if and only if the stabilizer G_x of some (any) $x \in \Omega$ is a* **maximal subgroup** *of G. Here we call $H \leq G$ a maximal subgroup if there is no subgroup L such that $H < L < G$.*

Proof. 1. Let $\Delta \subset \Omega$ be a region of imprimitivity, denote by G_Δ the stabilizer of Δ. By definition of we have for every $x \in \Delta$ that $G_x \subseteq G_\Delta$. As $|\Delta| > 1$ we have $G_x \neq G_\Delta$. As $\Delta \neq \Omega$ we have $G_\Delta \neq G$.
2. Assume $G_x < H < G$. Put $\Delta = xH$. Then Δ is a region of imprimitivity, and $|\Delta| = [H : G_x]$. □

2.12 Theorem. *If (G,Ω) is 2-transitive, then (G,Ω) is primitive.*

Proof. Let $\Delta \subset \Omega$ be a region of imprimitivity. Choose $x, y \in \Delta, x \neq y$ and $z \notin \Delta$. By definition of 2-transitivity we find $g \in G$ such that $xg = x, yg = z$. This contradicts the definition of a region of imprimitivity. $\square$

2.1 Normal subgroups and permutation representations

2.13 Theorem. *If (G,Ω) is primitive and $1 \neq N \lhd G$, then (N,Ω) is transitive.*

Proof. Let $|\Omega| = n$. We have $G_x \leq G_xN \leq G$. Because of primitivity we have either $G_xN = G$ or $G_xN = G_x$. Assume $G_xN = G_x$, equivalently $N \leq G_x$. By conjugation we see that $N \leq G_y$ for all $y \in \Omega$, hence $N = 1$, contradiction. We conclude $G_xN = G$. As

$$n = |G|/|G_x| = |N|/|G_x \cap N|,$$

we conclude that N is transitive on Ω. $\square$

2.14 Definition. (G,Ω) *is* **sharply t-transitive** *($t \geq 1$) if whenever two t-tuples $(x_1, x_2, \ldots, x_t)$ and $(y_1, y_2, \ldots, y_t)$ of different elements in Ω are given, there exists exactly one $g \in G$ such that $x_ig = y_i, i = 1, 2, \ldots, t$.*
(G,Ω) *is* **regular** *if it is sharply 1-transitive, equivalent if (G,Ω) is transitive and $|G| = |\Omega|$.*

2.15 Theorem. *Let (G,Ω) be primitive and G_x a simple group. Then one of the following holds:*

- *Either G is simple, or*
- *G contains a normal subgroup N such that (N,Ω) is regular.*

Proof. Assume G is not simple. Let $1 \neq N \lhd G$. We know from Theorem 2.13 that (N,Ω) is transitive. We have to show that $N \cap G_x = 1$. As G_x is a simple group and $N \cap G_x \trianglelefteq G_x$ the only other possibility is $N \cap G_x = G_x$, equivalently $G_x \leq N$. It follows from the orbit length lemma that $N = G$, contradiction. $\square$

So we can sometimes guarantee the existence of a normal regular subgroup. Let us study this situation more in detail.

2.16 Lemma. *Let (G, Ω) be transitive, $N \lhd G$ such that (N, Ω) is regular. Then $(G_x, \Omega - \{x\})$ is similar to the representation of G_x by conjugation on $N - \{1\}$.*

Proof. Observe that $x \in \Omega$ is fixed.

$$\beta : \Omega - \{x\} \longrightarrow N - \{1\}$$

is defined as $y\beta = n \in N$ satisfying $xn = y$. Observe that $n \neq 1$ exists and is uniquely determined as N is regular on Ω. Thus β certainly defines a bijection. We have to check the defining property of similarity. Let $h \in G_x, y \in \Omega - \{x\}$. We need to show that $(yh)\beta = h^{-1}(y\beta)h$. Put $(yh)\beta = n, y\beta = n'$. Then $xn = yh$ and $xn' = y$. It follows $x(h^{-1}n'h) = xn'h = yh$. This shows $n = h^{-1}n'h$, as claimed. We can interpret Lemma 2.16 as saying that for every choice of $x \in \Omega$ the set Ω can be given a group structure, with x in the role of the neutral element, and G_x respects this group structure. □

We obtain a first classification theorem:

2.17 Theorem. *Let (G, Ω) be t-transitive ($t \geq 2$) with a regular normal subgroup N. Then $t < 5$ and one of the following holds:*

1. *$t = 2, N \cong E(p^n)$ for some prime p.*
2. *$t = 3$ and either $N \cong Z_3$ or $N \cong E(2^n)$.*
3. *$t = 4, N \cong E(4)$.*

Proof. It follows from Lemma 2.16 that the automorphism group of N is $(t-1)$-transitive on $N - \{1\}$. Certainly $t \geq 2$. The transitivity shows that N must be elementary abelian of some prime-power order. If $t = 3$, then the double transitivity shows that either $N \cong Z_3$ or $p = 2$. If $t > 3$, then clearly $N \cong E(4)$ and $t = 4$. □

As a consequence of this theory we obtain an easy proof for the fact that the alternating groups are simple groups:

2.18 Theorem. *The alternating groups A_n are simple when $n \geq 5$.*

Proof. We have shown in Section 1.32 that A_5 is simple. Let now $n > 5$. The stabilizer of a point in A_n is A_{n-1}. By induction we can assume that A_{n-1} is a simple group. A_n is highly transitive, hence certainly primitive. If A_n is not simple, then we know from Theorem 2.15 that A_n must contain a regular normal subgroup. By Theorem 2.17 this implies $t \leq 4$, hence $n = 6$. By Theorem 2.17 we get a contradiction even in case $n = 6$. $\square$

2.2 Problems

1. Let $A, B \leq G$. Then $|AB| = |A| \cdot |B| / |A \cap B|$.

Chapter 3

The classical simple groups

We know already two classes of classical simple groups. The **alternating group** A_n has been introduced as a (normal) subgroup of the symmetric group S_n in Section 1.15. We have proved that $A_n, n \geq 5$ are simple groups.

The projective special linear group $PSL_n(q)$ is a factor group of the special linear group $SL_n(q)$. The groups $PSL(n,q), n \geq 2$ are simple except for $PSL(2,2)$ and $PSL(2,3)$. The remaining families of classical finite simple groups are related to bilinear forms (scalar products) and quadratic forms.

3.1 Scalar products

Let $V = V(n,q)$ be a vector space of dimension n over $\mathbb{F}_q$. 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** $A = ((v_i, v_j))_{i,j}$.

3.2 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.

3.2.1 Hyperbolic planes

Let $n = 2$. Choose $0 \neq x \in V$. Then $x^\perp = \langle x \rangle$ 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.**

3.2.2 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 $H = \langle x, y \rangle$ 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 $\{v_1, v_2, \dots, v_m\} \cup \{w_1, w_2, \dots, w_m\}$ such that

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

where $H_i = \langle v_i, w_i \rangle, (v_i, w_i) = 1$. 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 if 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 $H_1 = \langle v_1, w_1 \rangle, H_1' = \langle v_1', w_1' \rangle$. 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 $q^{1+3+\cdots+(2m-1)}$. As $\sum_{i=1}^m (2i+1) = m^2$ we obtain

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

Let us use coordinates: so A is the Gram matrix of a non-degenerate symplectic scalar product, with respect to a fixed basis $x_1, x_2, \dots, x_{2m}$. 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 $(x_i^g, x_j^g) =$

$(x_iT, x_jT) = (\sum_k t_{ik}x_k, \sum_l t_{jl}x_l) = \sum_{k,l} t_{ik}a_{k,l}t_{jl}$. 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:

3.2 Lemma. *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 $SP(2m, q) \subset SL(2m, q)$.

3.3 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, see Lemma 1.73). 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 $V = \langle x_1 \rangle \perp x_1^\perp$. 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:

3.3 Theorem.

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

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.

3.4 Proposition. *The number of $v \in V$ such that $(v, v) = 0$ is $q^{n-1}(q^n + (-1)^n(q-1))$. For every $0 \neq \alpha \in I\!F_q$ 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. □

3.5 Theorem. *The orders of the unitary groups are as follows:*

- $|GU(n, q^2)| = \prod_{i=1}^n q^{i-1}(q^i - (-1)^i) = q^{n(n-1)/2}(q+1)(q^2-1)\cdot\cdots\cdot(q^n - (-1)^n)$
- $|SU(n, q^2)| = \prod_{i=2}^n q^{i-1}(q^i - (-1)^i)$.
- *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 3.4. 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 $f(n,1)f(n-1,1)\dots f(1,1)$. 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 $U_3(2)$.

3.4 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 $V=\langle v,w\rangle \perp \langle v,w\rangle^\perp$ and $\langle v,w\rangle^\perp$ 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 $R=\langle u_1,u_2,\dots,u_m\rangle$. Find vectors v_i such that $\{u_i,v_i\}$ is a hyperbolic pair and $\langle U,v_1,v_2,\dots,v_m\rangle = H_1\perp\dots\perp H_m\perp U_0$ is non-degenerate. Here $H_i=\langle u_i,v_i\rangle$ 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, $U=\langle u_1,u_2,\dots,u_m\rangle$. Then $V=\langle u_1,v_1\rangle\perp\dots\perp\langle u_m,v_m\rangle\perp V_0$, 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.

3.6 Lemma. *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. $\square$

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 3.6 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 $V_0 = \langle u_1, u_2 \rangle$. By Lemma 3.6 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 $b = -c_0$.

3.7 Definition. *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 $(\mathbb{F}_q^*)^2$, more precisely*

$$D(V) = \begin{cases} +1 & \text{if } det(A) \text{ is a square,} \\ -1 & \text{if } det(A) \text{ is a nonsquare.} \end{cases}$$

As a basis transformation T leads to the transformation TAT^t of the Gram matrix, the discriminant is uniquely determined.

3.8 Lemma. *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. *$V_0 = \langle v_0 \rangle$ and $(v_0, v_0) = 1$.*

2. *$V_0 = \langle v_0 \rangle$ and $(v_0, v_0) = c_0$.*

3. *$V_0 = \langle v_1, v_2 \rangle$, 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 $-c_0 \bmod \mathbb{F}_q^2$, 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:

3.9 Theorem. *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. *$dim(V) = n = 2m+1, V = H_1 \perp \cdots \perp H_m \perp \langle v_0 \rangle$, 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 $ind(V) = m$.*

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

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

   or

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

   where V_0 is the 2-dimensional anisotropic space given in Lemma 3.8. The $(+)-$type has $ind(V) = m$, the $(-)-$type has $ind(V) = m-1$. These types have different discriminant.

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 scalar 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.

3.10 Lemma. *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 :

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

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

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

3.11 Lemma. *In the orthogonal space of odd dimension* $2m+1$ *with anisotropic complement* $V_0 = \langle v_0\rangle$, *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 $\langle v_1, w_1\rangle^\perp$ 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

$$|O^+_{2m}(q)| = q^{m(m-1)}2(q^2 - 1)(q^4 - 1) \ldots (q^{2m-2} - 1)(q^m - 1).$$

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

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

3.12 Lemma. *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 $m=1$.

3.5 Witt's theorem

3.13 Theorem (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.

3.14 Definition. *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 3.14 are obvious. Let us show that S is indeed an isometry:

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

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

3.15 Lemma. *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 $S : v \mapsto w$. $\square$

3.16 Lemma. *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 $dim(\langle v,w\rangle) = 2$. Consider first the case that $\langle v,w\rangle$ is non-degenerate. Then $V = \langle v,w\rangle \perp \langle v,w\rangle^\perp$ and we can assume without restriction that $V = \langle v,w\rangle$. Assume $(v-w)^\perp = \langle v\rangle$. Then

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

It follows $\langle v\rangle = \langle w\rangle = (v-w)^\perp$, contradicting the dimensional assumption. We have that $(v-w)^\perp$ is different from $\langle v\rangle$, and analogously also different

from $\langle w\rangle$. Let $\langle t\rangle = (v-w)^\perp$. Then $\langle v,w\rangle = \langle v,t\rangle = \langle w,t\rangle$, where $(v,t) = (w,t)$. It follows that there is an isometry fixing t and mapping $v \mapsto w$.
The last case is that $dim(\langle v,w\rangle) = 2$ and $\langle v,w\rangle$ is degenerate. The dimension of the radical can only be 1. Let $Rad(\langle v,w\rangle) = \langle u\rangle$. We can find $u' \in V$ such that $W = \langle u,u'\rangle \perp \langle v\rangle$ 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 $W = w^\perp \perp \langle w\rangle$. 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. $\square$

3.17 Lemma. *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 $V/\langle w\rangle^{perp}$. We call T a **symplectic transvection.**

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

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

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

3.18 Lemma. *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. $\square$

3.5.1 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 3.18 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:

$$U_1 \subset \langle U_1, y_1, \ldots, y_m \rangle = \langle x_1, y_1 \rangle \perp \cdots \perp \langle x_m, y_m \rangle \perp W,$$

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:

3.19 Corollary. *Under the assumptions of Theorem 3.13 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 $V = H_1 \perp \cdots \perp H_{m-1} \perp V_0$, 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 3.15 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 $g = s_1 s_2 \dots s_r$, 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 $V = H_1 \perp \cdots \perp H_m$ (of index m). Then $-I \in \Omega(V)$ if and only if either q is $1 (\mathrm{mod}\ 4)$ or m is even. In the case when $V = H_1 \perp \cdots \perp H_{m-1} \perp V_0$ (of index $m-1$) we have $-I \in \Omega(V)$ if and only if q is $3 (\mathrm{mod}\ 4)$ **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:

3.20 Lemma. *In odd characteristic the orders of the projective orthogonal groups are as follows:*

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

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

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

3.6 Symmetric scalar products in characteristic 2

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 $\langle v,w\rangle$ 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 $V = V_0 \perp \langle v\rangle$ 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: $rad(V_0)=\langle v_0\rangle$. We have $V_0 = W_0 \perp \langle v_0\rangle$, where W_0 is a non-degenerate symplectic space. It follows $V = W_0 \perp \langle v_0, v\rangle$, where $W_0 = V_0 \cap v^\perp, (v,v)=(v_0,v)=1$. The group G operates on V_0 and on $\langle v_0\rangle$. The space $V_0/\langle v_0\rangle$ 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 $V_0/\langle v_0 \rangle$. 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 $\langle v, v_0 \rangle = W_0^{\perp}$. 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.

3.7 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 either. 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:

3.21 Definition. *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 $H = \langle u, v \rangle$ 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 $(,)$.

3.22 Lemma. *Let (V, Q) be a quadratic space, $0 \neq v \in V \backslash Rad(V), Q(v) = 0$. There exists an $w \in V$ such that $Q(w) = 0, (v, w) = 1$. The space $H = \langle v, w \rangle$ 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. $\square$

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

3.23 Lemma. *Let $U = \langle u_1, \ldots, u_m \rangle$ be a maximal singular subspace of the nondegenerate quadratic space (V, Q). There exist vectors $v_1, \ldots, v_m$ such that $V = \langle u_1, v_1 \rangle \perp \cdots \perp \langle u_m, v_m \rangle \perp V_0$, where $\langle u_i, v_i \rangle$ 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 $0 \neq w \in W_0$.*

3.24 Theorem. *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 $V = \langle v_0 \rangle, Q(v_0) = 1$ 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 $w \in v^{\perp} \setminus \langle v \rangle$. 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 $V = \langle v, w \rangle$, 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, define $tr : \mathbb{F}_q \longrightarrow \mathbb{F}_2$ (the **trace**) by $tr(x) = x + x^2 + x^4 + \cdots + x^{2^{n-1}}$, where $q = 2^n$ ($tr(x)$ is the sum of all images of x under the Galois group, see Lemma 1.78). Then tr is $\mathbb{F}_2-$linear and onto. 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 Theorem 90,** see for example [12], part I, paragraph 7. The condition on $a \in \mathbb{F}_q$ as given in 2. of Theorem 3.24 is therefore equivalent to $tr(a) = 1$.

Let now $d = 1$, hence $n = 2m + 1, V = H_1 \perp \cdots \perp H_m \perp \langle v_0 \rangle$, where the $H_i = \langle u_i, v_i \rangle$ 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 $V/\langle v_0 \rangle$. 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 $V/\langle v_0 \rangle$ carries a nondegenerate symplectic scalar product it follows that G is embedded in the group $Sp_{2m}(q)$. Let now $\tilde{g} \in Sp(V/\langle v_0 \rangle)$. Then $\tilde{g}$ maps the hyperbolic plane $H_i + \langle v_0 \rangle / \langle v_0 \rangle$ onto a hyperbolic plane $\langle u_i' + \langle v_0 \rangle, v_i' + \langle v_0 \rangle \rangle$. We wish to find $\alpha, \beta \in \mathbb{F}_q$ such that $\langle u_i' + \alpha v_0, v_i' + \beta v_0 \rangle$ 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.

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

where the H_i are quadratic hyperbolic planes, or

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

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).

3.25 Theorem ('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 $O^\pm_{2m}(q)$ as in odd characteristic. The Clifford algebra allows the conctruction of a **Dickson invariant** : $O^\epsilon_{2m}(q) \longrightarrow \mathbb{F}_2$. The kernel of the Dickson invariant is denoted by $SO^\epsilon_{2m}(q)$, has index 2 in the full orthogonal group and is usually a simple group.

3.7.1 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).

3.8 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
$P\Omega_4^+(q) \cong L_2(q) \times L_2(q)$
$P\Omega_4^-(q) \cong L_2(q^2)$
$P\Omega_5(q) \cong S_4(q)$
$P\Omega_6^+(q) \cong L_4(q)$

Chapter 4

Polya's enumeration theory

Many combinatorial enumeration problems can be formulated as the determination of the number of orbits of a certain permutation group. As motivational examples let us consider the following two problems:

1. In how many essentially different ways can the six faxes of a die be colored with two colours (red and green, say) ? Here two colourings are equivalent if one can be obtained from the other by application of a rotation to the die (reflections are not allowed, and it is not allowed to change the role of the colours).

2. What is the number of essentially different graphs on five vertices? Here we consider only simple graphs (no loops, no multiple edges, no directed edges). Two graphs are equivalent if one can be obtained from the other by a permutation of the set of vertices.

At first we want to see that both problems belong to the same general family of enumeration problems, which may be described as follows:
Let G be a group acting on the set Ω. Denote by C^Ω the set of all mappings $\chi : \Omega \longrightarrow C$. Determine the number of orbits of G in its operation on C^Ω.
This needs some explanation. We may interpret the set C^Ω of all mappings $: \Omega \longrightarrow C$ as the set of all **colorings** of Ω with $|C|$ colours. Moreover it should be explained what the natural action of G on C^Ω is.

4.1 Lemma. *Let the group G act on the set Ω. The natural action of G as a group of permutations on the set C^Ω of all mappings $: \Omega \longrightarrow C$ (colorings) is defined as follows:*

$$\chi^g(x) = \chi(x^{g^{-1}}).$$

Here $\chi : \Omega \longrightarrow C, x \in \Omega, g \in G$. *This defines the image* χ^g *of the mapping* χ *under* g.

It is clear that for every $g \in G$ this defines a permutation of the colorings. If the coloring Ψ is given, the coloring χ defined by $\chi(y) = \Psi(y^g)$ satisfies $\chi^g = \Psi$. Moreover we see that the mapping $\chi \mapsto \chi^g$ defines a permutation representation of G on the set C^Ω of colorings of Ω. In fact, we have $\chi^{g_1g_2}(x) = \chi(x^{(g_1g_2)^{-1}}) = \chi(x^{g_2^{-1}g_1^{-1}})$ and $(\chi^{g_1})^{g_2}(x) = \chi^{g_1}(x^{g_2^{-1}}) = \chi(x^{g_2^{-1}g_1^{-1}})$. We obtain the same result. This shows that we have a permutation representation of G on the set of colorings.

In the first problem above choose G to be the group of all rotations in 3-space mapping the die (the cube) onto itself. We will see that G has order 24 and is isomorphic to the symmetric group S_4. We choose C to have 2 elements. The number we have to determine is the number of orbits of G on the set of colorings of the six faces of the die with 2 colours. We are talking about the permutation representation of G on the $2^6 = 64$ colorings of the faces induced by the permutation representation of G on the 6 faces, and we have to determine the number of orbits.
For the second problem above, we start from the symmetric group S_5, in its natural action on a 5-set V (the set of vertices of our graphs). Then $\Omega = \binom{F}{2}$ is the set of all unordered pairs of vertices. A graph is determined by deciding for every pair of vertices if they are joined by an edge or not. We may choose $C = \{e, n\}$, where e stands for **edge** and n for **nonedge.** There are clearly precisely $2^{10} = 1024$ such graphs. Two such graphs are equivalent if they are in the same orbit under the action of $G = S_5$. Again we have to determine the number of orbits.

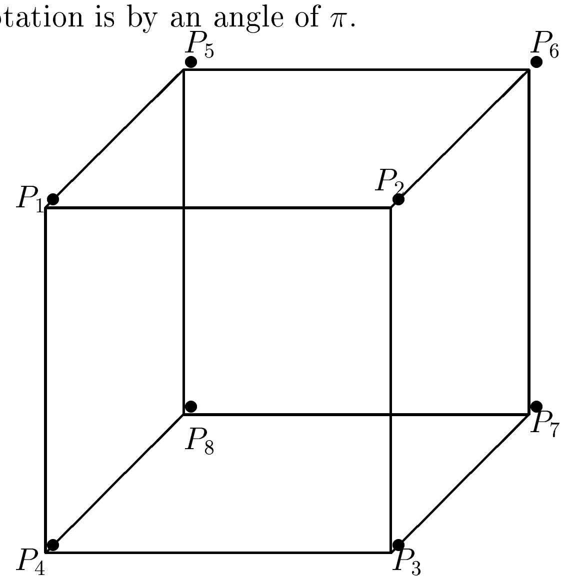
In order to be able and solve the first problem we have to determine the group G of rotations of 3-space, which map the cube to itself. We denote the vertices as $P_1, \ldots, P_8$ and the faces $F_1, \ldots, F_6$. Here we use the convention that the indices of opposite faces add up to 7 (see the figure). It is clear that G is transitive on vertices, on edges and also on faces. The stabilizer of a face is a cyclic group of order 4. For example, the stabilizer of F_1 is generated by the rotation about the axis through the centers of F_1 and F_6 by the angle $\pi/2$, hence $G_{F_1} = \langle\alpha\rangle \cong Z_4$, where

$$\alpha = (P_1, P_2, P_3, P_4)(P_5, P_6, P_7, P_8).$$

We conclude $|G| = 6 \cdot 4 = 24$. Similarly $G_{F_2} = \langle\beta\rangle \cong Z_4$, where

$$\beta = (P_1, P_5, P_8, P_4)(P_2, P_6, P_7, P_3).$$

It follows from Theorem 1.108 that the conjugacy classes of S_4 are in bijection with the partitions of the number 4. Aside of the neutral element we have eight elements of order 3, six elements of order 4, three involutions of cycle type (2,2) in the natural representation (forming the normal subgroup V together with the neutral element), and six involutions, which act as transpositions. We can see the operation of these elements on the cube: The elements of order 3 have as axis a line through two opposite vertices. They rotate by $2\pi/3$. The elements of order 4 and the three special involutions have as axis a line through the centers of two opposite faces. The remaining six involutions have as axis a line through the centers of two opposite edges. Rotation is by an angle of π.



Our main tool will be the cycle index:

4.2 Definition (cycle index). *Let G be a finite group acting on the n-set Ω. For every $g \in G$ denote by $f_i = f_i(g)$ the number of cycles of g of length i. Observe $\sum_{i=1}^n i f_i(g) = n$. The* **cycle index** *of (G, Ω) is defined as*

$$P_G(Z_1, Z_2, \ldots, Z_n) = \frac{1}{|G|} \sum_{g \in G} \prod_{i=1}^{n} Z_i^{f_i(g)}.$$

If $a_G(f_1, \ldots, f_n)$ denotes the number of elements of $g \in G$ satisfying $f_i(g) = f_i$, then we can write this equivalently as

$$P_G(Z_1, Z_2, \ldots, Z_n) = \frac{1}{|G|} \sum_{f_1, \ldots, f_n} a_G(f_1, \ldots, f_n) \prod_{i=1}^{n} Z_i^{f_i}.$$

We can now state and prove Pólya's main theorem. It is a little more general than what we have motivated above in the sense that instead of counting orbits of G in C^Ω we work with weights.

4.3 Definition (weights). *Let G be a finite group acting on the n-set Ω, with the induced action on the set C^Ω of colorings.*
Let $R \supseteq \mathbb{Q}$ be a commutative ring, w a function $w : C \longrightarrow R$. We interpret $w(c)$ as the **weight** *of colour c. Denote by $\mathcal{B}$ the set of orbits of G on the colorings. Let χ be a coloring. We define the weight of χ by*

$$w(\chi) = \prod_{x\in\Omega} w(\chi(x)).$$

As each $g \in G$ permutes the elements of Ω it is clear that w is constant on orbits. We can interpret w as a function $w : \mathcal{B} \longrightarrow R$.

4.4 Theorem (Pólya's theorem). *Let G be a finite group operating on the n-set Ω, C a finite set (the colours). Consider the induced action of G on the set C^Ω of colorings.*
Let $R \supseteq \mathbb{R}$ be a commutative ring, $w : C \longrightarrow R$. Let w also be defined on C^Ω and on the set $\mathcal{B}$ of G-orbits on C^Ω, as in Definition 4.3. Then the following holds:

$$\sum_{B\in\mathcal{B}} w(B) = P_G(\sum_{c\in C} w(c), \sum_{c\in C} w(c)^2, \dots).$$

Here P_G denotes the cycle index of G in its operation on Ω. In words: In order to obtain the sum of the weights of the orbits we have to evaluate the cycle index $P_G(Z_1, Z_2, \dots, Z_n)$ at $Z_i = \sum_{c\in C} w(c)^i$.

Proof. We will see that all we need for the proof is Lemma 2.1, the Burnside lemma. In fact, fix an orbit $B \in \mathcal{B}$ and apply the Burnside Lemma. We obtain

$$1 = \frac{1}{|G|} \sum_{g\in G} |F(g) \cap B|.$$

Here $F(g) \cap B$ is the set of colorings in the same orbit B, which are fixed under g. Multiply with $w(B)$:

$$w(B) = \frac{1}{|G|} \sum_{g\in G} \sum_{\chi\in B, \chi^g=\chi} w(\chi).$$

Sum up over $\mathcal{B}$:

$$\sum_{B\in\mathcal{B}} w(B) = \frac{1}{|G|}\sum_{g\in G}\sum_{\chi\in F(g)} w(\chi).$$

Comparison with the definition of the cycle index shows that it suffices to prove the following:
For every $g \in G$ we have

$$\sum_{\chi\in F(g)} w(\chi) = \prod_{i=1}^{n}(\sum_{c\in C} w(c)^i)^{f_i}.$$

Here the $f_i = f_i(g)$ are as in Definition 4.2. If we realize that g has f_i cycles of length i and that a coloring χ is fixed by g if and only if it is constant on cycles we see that this is really a triviality. □

Let us use this theorem to solve the two motivational problems: the cycle index of the octohedral group $G \cong S_4$ in its action on the six faces of the cube is

$$P_G = \frac{1}{24}(Z_1^6 + 3Z_1^2Z_2^2 + 6Z_1^2Z_4 + 6Z_2^3 + 8Z_3^2). \tag{4.1}$$

As we wish to count orbits we should define the weight of each of the two colours to be 1. The number of orbits of colorings of the faces of the cube with 2 colours is therefore

$$P_G(2,2,\dots) = \frac{1}{24}(2^6 + 3\cdot 16 + 6\cdot 8 + 6\cdot 8 + 8\cdot 4) = 10.$$

Let us consider the second motivational problem, the number of isomorphism classes of graphs on 5 vertices. We have listed the conjugacy classes of S_5 in its natural action on 5 points in the proof of Theorem 1.119. The operation on the 10 pairs is easily deduced from this. The corresponding cycle index (of the operation of S_5 on 10 objects) is

$$P_G = \frac{1}{120}(Z_1^{10} + 24Z_5^2 + 20Z_1Z_3^3 + 10Z_1^4Z_2^3 + 15Z_1^2Z_2^4 + 30Z_2Z_4^2 + 20Z_1Z_3Z_6). \tag{4.2}$$

As before we color with two colours and wish to compute the number of orbits. We obtain the number of isomorphism classes of simple graphs on 5 vertices as

$$P_G(2,2,\dots) = 34.$$

The **universal** way to use the weights in Pólya's theorem is to work with the polynomial ring $R = I\!R[x_c | c \in C]$ in $|C|$ variables and to define $w(c) = x_c$. All other choices of weights can be obtained by specialization. With the universal choice we get $w(f) = \prod_{c \in C} x_c^{n_c}$, where $n_c = f^{-1}(c)$. Let us apply the universal choice of weights to the operation of S_5 on the 10 points of $\binom{F}{2}$, whose cycle index has been given in equation 4.2. With weights $w(e) = x, w(n) = y$ the right side in Theorem 4.4 becomes

$$\begin{aligned} P_G(x+y, x^2+y^2, \ldots, x^6+y^6) = x^{10} + x^9y + 2x^8y^2 + 4x^7y^5 + 6x^6y^4 + \\ +6x^5y^5 + 6x^4y^6 + 4x^3y^7 + 2x^2y^8 + xy^9 + y^{10} \end{aligned}$$

The coefficients tell us that there are precisely six nonisomorphic graphs with five edges and also 6 nonisomorphic graphs with six edges, for example. The sum of all coefficients is 34, the number of isomorphism classes of graphs on five vertices, as it has to be. We see that the universal choice of weights gives us more information than the earlier specific choice.

4.1 Problems

1. The **octahedral group:** Let G be the group of rotations fixing the unit cube. With the notation introduced above show the following:

   (a) $G = \langle \alpha, \beta \rangle$.

   (b) $G \cong S_4$.

   For part 2. consider the action of G on the four pairs of opposite vertices: $A = \{P_1, P_7\}, B = \{P_2, P_8\}, C = \{P_3, P_5\}, D = \{P_4, P_6\}$.

2. Determine the number of nonisomorphic graphs on 4 vertices.

3. Determine the number of essentially different colorings of the faces of a die with m colours.

4. Consider the action of the octohedral group $G \cong S_4$ on the faces of a die. Determine the number of orbits of G on subsets of any fixed cardinality (between 1 and 6) of the set of faces.

Chapter 5

Block designs

In this chapter we use permutation groups in the construction of an important class of combinatorial objects, block designs.

5.1 Definition (t-designs). *Let Ω be a set of cardinality n and $\mathcal{B}$ a family of k-subsets of Ω. The pair $(\Omega, \mathcal{B})$ is a (***simple***) t-***design*** *if for every t-subset $T \subset \Omega$ there are exactly λ subsets $B \in \mathcal{B}$ such that $B \supseteq T$, for some natural number λ. The subsets $B \in \mathcal{B}$ are called the* **blocks** *of the design. More precisely the parameters of the design are then denoted as*

$$t-(n, k, \lambda).$$

There are many variants of this definition. We mention some of them, but as we will use mostly simple t-designs in the sequel we will not be very formal. If k-subsets are allowed to be counted more than once as a block we speak of a (not necessarily simple) $t-$design. t-designs with $\lambda = 1$ are also known as **Steiner systems.** In the case of Steiner systems we will also use the shorter notation $S(t, k, n)$ instead of $t-(n, k, 1)$. If we generalize the notion of a design in the sense that we use blocks not all of the same cardinality k one speaks of t-wise balanced designs. We obtain a trivial structure by choosing $\mathcal{B}$ to be the family of all k-subsets of Ω. This **complete design** has parameters $t-(n, k, \binom{n-t}{n-k})$. In order to exclude trivial cases we assume $t < k < n$. Consider pairs (T, B), where $|T| = t, B \in \mathcal{B}$ and $T \subset B$. Counting these pairs in two ways we arrive at the following equation:

$$\binom{n}{t} \cdot \lambda = b \cdot \binom{k}{t} \tag{5.1}$$

relating the parameters of a design $t-(n,k,\lambda)$. Here $b=|\mathcal{B}|$ denotes the number of blocks. Next we wish to show that a t-design is also $(t-1)$-design (if $t\geq 2$). It follows by induction that any t-design is an i-design for all $i\leq t$. If the value of t is in doubt we write λ_t instead of λ. The $\lambda-$parameter when the same design is considered as an i-design is then denoted by λ_i.

5.2 Lemma. *Let $\mathcal{D}$ be a design $t-(n,k,\lambda)$. Then $\mathcal{D}$ is also a $(t-1)$-design, where*

$$\lambda_{t-1}=\lambda\cdot(n-t+1)/(k-t+1).$$

Proof. Fix a $(t-1)$-subset $T'\subset\Omega$. The number of blocks containing T' is $\lambda_{t-1}=(n-t+1)\lambda/(k-t+1)$. Not clear yet? Count pairs (x,B), where $x\notin T', B\supset T'\cup\{x\}$. Counting in two ways we get $(n-t+1)\lambda=\lambda_{t-1}(k-t+1)$. □

By induction we arrive at the following formula for λ_i :

$$\lambda_i=\lambda\cdot\frac{\binom{n-i}{t-i}}{\binom{k-i}{t-i}} \tag{5.2}$$

We describe briefly some straightforward constructions.

5.3 Lemma. *Let $\mathcal{D}=(\Omega,\mathcal{B})$ be a simple design with parameters $t-(n,k,\lambda)$.*

1. *Choose as blocks all the k-sets which are not blocks of $\mathcal{D}$. Comparison with the complete design shows that this yields a design $t-(n,k,\binom{n-t}{n-k}-\lambda)$, the* **complementary design.**

2. *Fix a set I of i points, where $i<t$ and use as blocks the $B-I$, where B varies through the blocks of $\mathcal{D}$, which contain I. We obtain a design $(t-i)-(n-i,k-i,\lambda)$, a* **derived design.**

3. *Let the blocks of $\mathcal{D}'$, the* **supplementary design,** *be the complements of the blocks of $\mathcal{D}$. This yields a t-design with block-size $k'=n-k$. In order to determine its $\lambda-$value we can compare equation 5.1 with the corresponding expression for $\mathcal{D}'$. Observe that the number b of blocks is the same for both designs. By division we obtain the parameters of $\mathcal{D}'$ as*

$$t-(n,n-k,\lambda\cdot\frac{\binom{n-k}{t}}{\binom{k}{t}}).$$

4. *Fix a point P and choose as blocks of the* **residual design** $\mathcal{D}'$ *all the blocks of* $\mathcal{D}$ *avoiding P. It is clear that we obtain a $(t-1)$-design on $n-1$ points. In fact, the $\lambda-$value of $\mathcal{D}'$ is $\lambda' = \lambda_{t-1} - \lambda = \lambda \cdot (\frac{n-t+1}{k-t+1} - 1) = \lambda \cdot \frac{n-k}{k-t+1}$. We conclude that $\mathcal{D}'$ has parameters $(t-1)-(n-1, k, \lambda \cdot \frac{n-k}{k-t+1})$.*

5.4 Definition. *Let $\mathcal{D} = (\Omega, \mathcal{B})$ and $\mathcal{D}' = (\Omega', \mathcal{B}')$ be designs. An* **isomorphism** *from $\mathcal{D}$ to $\mathcal{D}'$ is a bijective mapping $: \Omega \longrightarrow \Omega'$, which induces a bijection between the blocks. An* **automorphism** *of $\mathcal{D}$ is an isomorphism from $\mathcal{D}$ to itself. The automorphism group $Aut(\mathcal{D})$ is the group of all automorphisms of $\mathcal{D}$. Observe that $Aut(\mathcal{D})$ is by definition a subgroup of the symmetric group on Ω.*

5.1 Some easy direct constructions

Let $E \cong E(2^n)$ be an elementary abelian group, equivalently the additive group of a vector space of dimension n over $\mathbb{F}_2$. We will in fact use additive notation. We define a 4-set $B = \{a, b, c, d\} \subset E$ to be a block if $a+b+c+d = 0$. This gives us a Steiner 3-design $S(3, 4, 2^n)$. In fact, let $T = \{a, b, c\}$ be a 3-set. There can be at most one block containing T, given by $d = a + b + c$. The only thing that could conceivably go wrong is that $d \in T$. In that case T would not be contained in a block at all. Assume without restriction $d = a$. We see that this cannot happen as it would follow $b = c$, contradiction. We have proved the following:

5.5 Theorem. *The 4-subsets of an elementary abelian 2-group, whose elements sum to zero, form the blocks of a Steiner 3-design*

$$S(3, 4, 2^n), \textit{ for all } n \geq 4.$$

Next we define projective planes: Let $V = V(3, q)$ be a 3-dimensional vector space over the field $\mathbb{F}_q$. As points choose the $(q^3 - 1)/(q - 1) = q^2+q+1$ subspaces of dimension 1. As blocks (lines) choose the 2-dimensional subspaces, with the natural inclusion relation. We see that the number of lines equals the number of points: $b = n = q^2 + q + 1$. Each line has $(q^2 - 1)/(q-1)$ points, each point is on $q+1$ lines, any pair of points is on precisely one line and any two lines have precisely one point in common. In particular we have an $S(2, q + 1, q^2 + q + 1)$.

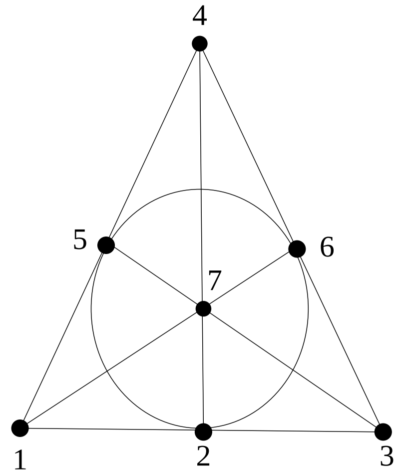


Figure 5.1: The Fano plane

5.6 Definition. *Let q be a prime-power.*
The 1-dimensional and 2-dimensional subspaces of a 3-dimensional vector space over $\mathbb{F}_q$ form the points and lines (blocks) of the (classical) **projective plane** *of order q. This is a Steiner system $S(2, q+1, q^2+q+1)$. It has the property that any pair of lines intersects in precisely one point.*
Fix a line l, consider only the points off l (the **affine points***). The structure induced is a Steiner system $S(2, q, q^2)$ (the (classical)* **affine plane** *of order q.) In general $S(2, n+1, n^2+n+1)$ are called* **projective planes** *of order n and $S(2, n, n^2)$ are* **affine planes** *of order n.*

It is an open problem if projective planes of nonprimepower orders exist.

Designs $S(2, 3, n)$ are also known as **Steiner triple systems,** $S(3, 4, n)$ are **Steiner quadruple systems.** We have seen that the projective plane of order 2 is a Steiner triple system $S(2, 3, 7)$. This design is uniquely determined by its parameters and is also known as the **Fano plane.** We have seen a picture in the Problems section of Chapter 1. Here it is again:

Symmetric designs are by definition 2-designs with equally many blocks as points. Symmetric designs with $\lambda = 2$ are also known as **biplanes.** Here is an easily constructed biplane:

5.7 Theorem. *Order 16 points in a square. Each point P defines a block B_P in the following way: the points of B_P consist all the points in the same row and all the points in the same column of P, but not P. This defines a design $2-(16, 6, 2)$.*

5.2 Steiner triple systems

In this section we use a construction of Richard Wilson [23] to show that Steiner triple systems $S(2,3,n)$ exist for all conceivable n. What are these conceivable n? Fix a point. As all remaining points occur in pairs n must be odd. Equation 5.1 yields $b = n(n-1)/6$. It follows that n must be 0 or 1 mod 3. We have seen that necessarily $n \equiv 1, 3 \pmod 6$.

It remains to show that an $S(2,3,n)$ exists whenever this condition is satisfied. Let $m = n-2$. Then $m \equiv \pm 1 \pmod 6$, in words: m is odd and not divisible by 3. Let G be an abelian group of order m. Write G additively. Denote by Δ the family of triples $\{x, y, z\} \subset G - \{0\}$ satisfying $x+y+z = 0$. Define a graph Γ with $G - \{0\}$ as set of vertices by joining x, y by and edge if $\{x, y\}$ is not contained in any triple from Δ. We will have to study the structure of this graph for a while.

5.8 Definition. *A* **1-factor** *of a graph is a collection of edges, which partition the vertices. A* **1-factorization** *of a graph is a partitioning of the edge set in 1-factors.*

Clearly 1-factors can only exist when the number of vertices is even.
It is obvious that the edges $\{x, -x\}$ form a 1-factor of Γ. Assume $\{x, y\}$ is an edge of Γ and $y \neq -x$. Then either $-(x+y) = x$ (and $y = -2x$) or $-(x+y) = y$ (and $y = -\frac{1}{2}x$). Observe that each vertex x really has three different neighbours (if $-\frac{1}{2}x = -2x$, then $3x = 0$, which is impossible as m is not divisible by 3). Graphs with valency 3 are also known as **cubic graphs.**

5.9 Lemma. *The graph* Γ *possesses a 1-factorization.*

Such a 1-factorization necessarily consists of three 1-factors. It suffices to prove that each connected component of Γ has a 1-factorization. Consider the graph Γ' at first, which arises out of Γ by omitting the edges $\{x, -x\}$. As Γ' is regular of degree two, it is a union of cycles. Consider the cycle C of Γ' containing vertex x. The vertices in C are $x, -2x, 4x, -8x, 16x, \ldots$. Observe that the mapping $x \mapsto -2x$ is an automorphism of the group G as G is abelian of odd order. We distinguish two cases:
Assume $-x \in C$. Then C has even length and for every $y \in C$ we have that $-y$ is opposite to y in C. In particular C is a connected component of Γ.
Assume $-x \notin C$. Then $-C$ has the same length as C and the connected

component of Γ containing x is $C \cup (-C)$.
We can now prove the lemma: in the first case the connected component is a cycle of even length, with opposite vertices joined. It is rather obvious how a 1-factorization can be constructed. In the second case the connected component is the union of two cycles of the same length, with corresponding vertices joined. A construction of a 1-factorization is a little trickier in this case, but not hard. We leave this as an exercise.

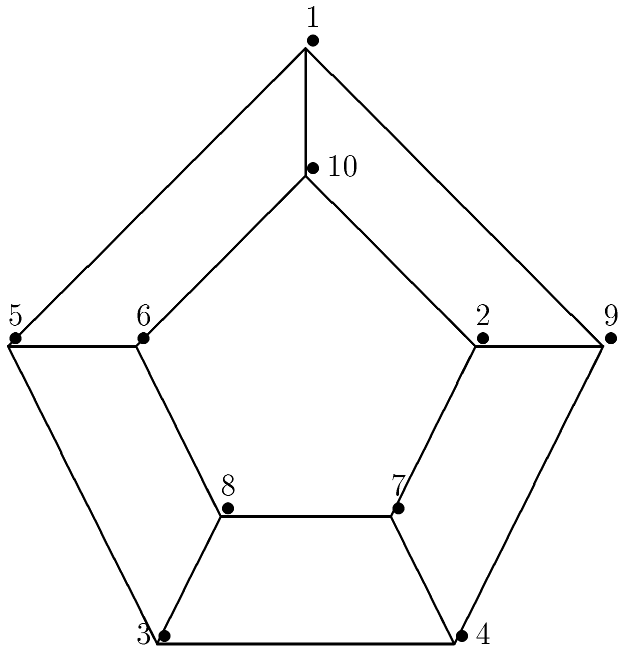
Let now F_1, F_2, F_3 the 1-factors of a 1-factorization of Γ. Let $\Omega = (G - \{0\}) \cup \{a_1, a_2, a_3\}$. We define the blocks of a Steiner triple system on Ω :
If x, y, z are different elements of $G - \{0\}$ such that $x + y + z = 0$, then $\{x, y, z\}$ is a block of type I.
If $\{x, y\}$ is an edge of Γ, then it belongs to one of our 1-factors, say F_i. Define $\{x, y, a_i\}$ to be a block (type II).
Finally, $\{a_1, a_2, a_3\}$ is the only block of type 0. It is now easy to check that we have constructed a Steiner triple system. We have proved the following:

5.10 Theorem. *A Steiner triple system $S(2, 3, n)$ exists if and only if* $n \equiv 1, 3$ *(mod* $6), n \geq 3$.

We know $S(2, 3, 3)$ (trivial), $S(2, 3, 7)$ (the Fano plane) and $S(2, 3, 9)$ (the affine plane of order three). Let us carry through Wilson's construction to find an $S(2, 3, 13)$: The group is $G = \mathbb{Z}/11\mathbb{Z}$, the cyclic group of order 11. We have $\Omega = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, a_1, a_2, a_3\}$. The number of blocks is $b = n(n - 1)/6 = 26$. Blocks of type I are the triples of nonzero residues mod 11 with vanishing sum. This gives us the complete list of blocks of types 0 and I:

a_1	a_2	a_3
1	2	8
1	3	7
1	4	6
2	3	6
2	4	5
3	9	10
4	8	10
5	7	10
5	8	9
6	7	9

Graph Γ looks as follows:



Here is a 1-factorization:

F_1 :	1,9	3,4	2,10	7,8	5,6
F_2 :	1,5	4,9	6,10	2,7	3,8
F_3	3,5	6,8	1,10	2,9	4,7

This gives us the fifteen remaining blocks:

a_1	1	9
a_1	3	4
a_1	2	10
a_1	7	8
a_1	5	6
a_2	1	5
a_2	4	9
a_2	6	10
a_2	2	7
a_2	3	8
a_3	3	5
a_3	6	8
a_3	1	10
a_3	2	9
a_3	4	7

5.3 Some easy recursive constructions

5.11 Theorem (Moore). *If an $S(2, q, a)$ and an $S(2, q, b)$ exist, where q is a prime-power, then an $S(2, q, a \cdot b)$ exists.*

Proof. Arrange the points in an (a, b)-rectangle. Define the structure of an $S(2, q, a)$ on the set of rows (the row system) and the structure of an $S(2, q, b)$ on the set of columns (the column system). Moreover impose the structure of an $S(2, q, b)$ on each row and the structure of an $S(2, q, a)$ on each column. We use all these as blocks and call these blocks of type I. The remaining blocks will be of a different type: Consider the (q, q)-rectangles consisting of the points whose first coordinates form a block of the row system and whose last coordinates form a block of the column system. Impose the structure of an affine plane A of order q on these q^2 points in such a way that the rows and columns are blocks. Observe that this can be arranged. As blocks of type II we choose all the blocks of A aside of the rows and columns. It is now an elementary task to check that we obtain an $S(2, q, a \cdot b)$. $\square$

As an illustration the reader should check how this construction, when applied to two copies of the trivial system $S(2, 3, 3)$ yields an $S(2, 3, 9)$, which latter is the affine plane of order 3 (see the Problems section). In fact, we obtain the 9 points arranged in a square and the 12 lines are the following:

the rows, the columns and the sets of three points whose first and second coordinates are different.

5.12 Theorem (Skolem). *If an $S(2, q+1, n)$ exists, where q is a prime-power, then an $S(2, q+1, q \cdot n+1)$ exists.*

Proof. Write the point set as $X \cup \{\infty\}$, where the $q \cdot n$ points in X are arranged in a rectangle. The blocks will be of three kinds:

- The union of a column and ∞ is a block (type I).
- Impose the structure of an $S(2, q+1, n)$ on each row. Use all these blocks (type II).
- Impose the structure of an $S(2, q+1, n)$ on the set of columns. Consider the $(q, q+1)$-rectangles R whose second coordinates form a block. Impose the structure of a projective plane of order q on each such set $R \cup \{\infty\}$ in such a way, that the unions of ∞ and the columns of R are lines. Take as blocks (type III) all the lines of these projective planes not passing through ∞.

□

5.13 Theorem (Witt). *If $S(3,4,a)$ and $S(3,4,b)$ exist, then $S(3,4,a \cdot b)$ can be constructed*

Proof. Write the point set as an (a, b)-rectangle. The blocks will be the following 4-subsets:

- Impose the structure of an $S(3,4,b)$ on each row, proceed analogously for columns. Use all these sets as blocks (type I).
- Take all quadrangles as blocks. More precisely these are point sets of the form $\{(a_i, b_j) | i = 1,2; j = 1,2\}$ (type II).
- Take all points sets of the form $\{(a_1, b_1), (a_1, b_2), (a_2, b_3), (a_2, b_4)\}$, where the b_j are different (point sets on two different rows, two from each row, all from different columns). Do the analogous thing for columns. This yields the blocks of type III.

- Impose the structure of an $S(3,4,b)$ on the set of rows, analogously for the columns. Consider the $(4,4)$-rectangles A of points whose first and second coordinates form blocks of these row system and column system, respectively. Choose as blocks of type IV all 4-sets from such rectangles A with different row coordinates and different column coordinates.

$\square$

5.4 A link to permutation groups

We describe a straightforward connection between permutation groups and block designs.

5.14 Definition. *A permutation group (G,Ω) is t-homogeneous if G is transitive in its operation on the unordered t-subsets of Ω.*

It is clear that t-transitive permutation groups are t-homogeneous (see Definition 2.3).

5.15 Theorem. *Let the permutation group (G,Ω) be t-homogeneous, where $|\Omega| = n$. Choose a k-subset $B \subset \Omega$, where $t < k < n$. Let $\mathcal{B} = B^G$ be the orbit of B under the action of G. Then $(\Omega,\mathcal{B})$ is a t-design.*

This is in fact trivial. Let us calculate the $\lambda-$parameter. Equation 5.1 simplifies as we can calculate b. In fact, it follows from the orbit length lemma that $b = |G|/|G_B|$. Here $G_B = \{g|g \in G, Bg = B\}$ is the **set-stabilizer** of B. It follows

$$\lambda = \frac{|G|\binom{k}{t}}{|G_B|\binom{n}{t}} \tag{5.3}$$

5.5 The groups $PGL_2(q)$

We have introduced the general linear groups in Section 1.22. In particular $GL_2(q)$ has order $(q^2-1)(q^2-q)$. The center Z of $GL_2(q)$ consists of the scalar matrices and is therefore a cyclic group of order $q-1$ (see the Problems section). The factor group $PGL_2(q) = GL_2(q)/\mathbb{Z}(GL_2(q))$ has order $(q+1)q(q-1)$. The determinant is a group homomorphism $det : GL_2(q) \longrightarrow \mathbb{F}_q^*$,

which is of course surjective. The kernel of det is $SL_2(q)$, the **special linear group.** We know that $SL_2(q) \lhd GL_2(q)$ and $GL_2(q)/SL_2(q) \cong Z_{q-1}$. In particular $SL_2(q)$ and $PGL_2(q)$ have the same order $(q+1)q(q-1)$. Clearly $Z \cap SL_2(q) \lhd SL_2(q)$. Let $d = |Z \cap SL_2(q)|$. A scalar matrix $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$ belongs to $SL_2(q)$ if and only if $\lambda^2 = 1$. It follows that $d = 1$ if q is even whereas $d = 2$ if q is odd. We can also say that $Z \cap SL_2(q)$ is generated by the matrix $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ but in characteristic 2 we have $-1 = 1$. The factor group $PSL_2(q) = SL_2(q)/(Z \cap SL_2(q))$ is the **projective special linear group.** Its order is $(q+1)q(q-1)/d$. Consider the canonical mapping $\pi : SL_2(q) \longrightarrow PGL_2(q)$. The kernel of π is $Z \cap SL_2(q)$. It follows that π induces an injective mapping : $PSL_2(q) \longrightarrow PGL_2(q)$. We may see $PSL_2(q)$ as a normal subgroup of $PGL_2(q)$. Its index is d. In particular we have $PGL_2(q) = PSL_2(q)$ when q is a power of 2.
Clearly $GL_2(q)$ acts as a transitive permutation group on the $q^2 - 1$ nonzero vectors of the underlying vector space V. It also acts on the $(q^2-1)/(q-1) = q+1$ one-dimensional subspaces of V. However, the elements of Z (the scalar matrices) belong to the kernel of this permutation representation. We leave it as an exercise to show that the kernel is precisely Z. It follows that $PGL_2(q)$ acts as a permutation group on the set of one-dimensional subspaces of V. This set is known as the **projective line.**

5.16 Definition. *The projective line $PG(1, q)$ is the set of all one-dimensional subspaces of some two-dimensional vector space over the field $\mathbb{F}_q$.*

It is easier to calculate with the action of $PGL_2(q)$ on the projective line when coordinates are introduced. So let $V = \mathbb{F}_q^2$. Represent the subspace generated by $(\tau, 1)$ as $\tau \in \mathbb{F}_q$ and the subspace generated by $(1, 0)$ by the symbol ∞. With this identification we can write

$$PG(1, q) = \mathbb{F}_q \cup \{\infty\}.$$

Let $g \in PGL_2(q)$ be represented by the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. We compute

$$(\tau, 1) \begin{pmatrix} a & b \\ c & d \end{pmatrix} = (a\tau + c, b\tau + d).$$

It follows that $\tau g = (a\tau + c)/(b\tau + d)$ if $b\tau + d \neq 0$. If $b\tau + d = 0$, then $\tau g = \infty$. An analogous computation shows that $\infty g = \infty$ if and only if

$b = 0$, and $\infty g = a/b$ otherwise. We conclude that the action of $PGL_2(q)$ on the projective line is described as $\tau \longrightarrow \dfrac{a\tau + c}{b\tau + d}$ for $ad - bc \neq 0$. Here $\tau \in PG(1, q) = \mathbb{F}_q \cup \{\infty\}$ and the usual rules for calculation with ∞ have to be observed.

It is obvious that $G = PGL_2(q)$ is transitive on $PG(1, q)$. The stabilizer G_∞ consists precisely of the $q(q-1)$ mappings $\tau \longrightarrow a\tau + b$, where $a \neq 0$. If $x \in \mathbb{F}_q$ is given then $\tau \longrightarrow \tau + x$ affords the operation $0 \mapsto x$. We conclude that G is 2-transitive. The stabilizer $G_{(\infty,0)}$ consists of the mappings $\tau \longrightarrow a\tau$, where $a \in \mathbb{F}_q^*$. If $y \in \mathbb{F}_q^*$, then the unique element in $G_{(\infty,0)}$ affording the operation $1 \mapsto y$ is $\tau \longrightarrow y\tau$. We conclude that G is 3-transitive on the projective line.

5.17 Theorem. *The group $PGL_2(q)$ of order $(q+1)q(q-1)$ is 3-transitive in its action on the projective line $PG(1, q)$. Given two ordered triples of different points from $PG(1, q)$ there is* **precisely one** *element $g \in PGL_2(q)$ mapping one triple onto the other ($PGL_2(q)$ is* **sharply** *3-transitive on the projective line).*

5.5.1 Circle geometries

Next we construct a class of Steiner 3-designs on the projective line. We use Theorem 5.15 and in particular equation 5.3. So let $B \subset PG(1, q), |B| = k$. It follows from equation 5.3 that the design whose blocks are the images of B under $PGL_2(q)$ has parameters $3 - (q + 1, k, \lambda)$, where $\lambda = k(k-1)(k-2)/|G_B|$. As λ cannot be smaller that 1 we obtain the following corollary:

5.18 Corollary. *Let $B \subset PG(1, q), |B| = k$. Then the order of the set-stabilizer of B in $PGL_2(q)$ divides $k(k-1)(k-2)$.*

Let us work in $PGL_2(Q)$, where $Q = q^f$ and choose $B = \mathbb{F}_q \cup \{\infty\}$, in particular $k = q + 1$. It is clear that $PGL_2(q) < PGL_2(Q)$ and that $PGL_2(q)$ stabilizes B. It follows from Corollary 5.18 that the set-stabilizer of B in $PGL_2(Q)$ must be $PGL_2(q)$. We obtain a 3-design on $Q + 1$ with $\lambda = \dfrac{k(k-1)(k-2)}{(q+1)q(q-1)} = 1$.

5.19 Theorem. *Let $\Omega = PG(1, q^f)$. Choose as blocks the orbit containing $\mathbb{F}_q \cup \{\infty\}$ under the 3-transitive action of $PGL_2(q^f)$. This yields a design*

$$3 - (q^f + 1, q + 1, 1) \text{ (a Steiner 3-design).}$$

In particular we conclude that designs with these parameters exist for all prime-powers q and all natural numbers f.

Steiner 3-designs are also called **circle geometries,** for obvious reasons.

5.5.2 A class of 4-designs

We will use the groups $PGL_2(q)$ in characteristic two to construct families of 4-designs. As $PGL_2(q)$ is not 4-homogeneous on the projective line the simple method from Theorem 5.15 cannot be used. Our familiy will have block-size 5. We start by studying the operation of $PGL_2(q)$ in a little more detail.

So let $q = 2^f$ and assume that f is odd (equivalently $\mathbb{F}_4$ is not a subfield of $\mathbb{F}_q$). Let $G = PGL_2(q) = PSL_2(q)$. The sharp triple transitivity of G gives a lot of information on the action of G. An immediate consequence is that the stabilizer of a 3-subset is precisely S_3 (see the Problems section). We collect some more information:

5.20 Lemma. *Let $q = 2^f$, $G = PGL_2(q)$ in its action on the projective line. Then the following hold:*

1. *An element $1 \neq g \in G$ has at most two fixed points.*
2. *Sylow-2-subgroups are elementary abelian*

Proof. It follows from sharp triple transitivity that an element with three fixed points is the identity. A Sylow-2-subgroup is given by the elements $\tau \longrightarrow \tau + x$, where $x \in \mathbb{F}_q$. This is clearly elementary abelian. □

5.21 Lemma. *Let $q = 2^f, f$ odd, and $G = PGL_2(q)$ in its operation of the projective line. Then the following hold:*

1. *Involutions have precisely one fixed point.*
2. *Elements of order 3 are fixed-point-free.*
3. *$|G|$ is not divisible by 5.*

Proof. Involutions certainly have at least one fixed point. If more, then they would have at least three fixed points, contradiction. As f is odd we have that $q+1$ is a multiple of three. As elements of order three cannot have three fixed points, they must be fixed-point-free. As f is odd we have that q is ± 2 (mod 5). It follows that $(q + 1)q(q - 1)$ is not divisible by five. □

Let $S \subset PG(1,q)$ be a 4-subset. It follows from Corollary 5.18 that $|G_S|$ divides $8 \cdot 3$. An element of order 3 operating on a 4-set would have a fixed point. This cannot be the case. Moreover it is impossible that $|G_S| = 8$ as G_S would then have to be isomorphic to a Sylow-2-subgroup of S_4, which is a non-abelian group. We conclude that $|G_S|$ divides 4. In order to show equality it suffices to find a subgroup of order 4 of the stabilizer of S. To that end we can replace S by another 4-set from the same orbit. Because of the triple transitivity we can choose $S = \{\infty, 0, 1, a\}$ for some $a \in \mathbb{F}_q - \mathbb{F}_2$. The elements $\tau \longrightarrow a/\tau$ and $\tau \longrightarrow (\tau + a)/(\tau + 1)$ are involutions. They commute and stabilize S.

5.22 Lemma. *Let $q = 2^f, f$ odd, and $G = PGL_2(q)$ in its action on the projective line. Then the set-stabilizer G_S of a 4-set S is an elementary abelian group of order 4, with precisely one fixed point.*

In fact, G_S must have at least one fixed point, and cannot have three fixed points.

Let $F \subset PG(1,q)$ be a 5-subset. As $|G|$ is not divisible by 5 and elements of order 3 are fixed-point-free we conclude from Corollary 5.18 that $|G(F)|$ divides 4. It is clear that only two cases can occur: either G_F is trivial or G_F is a four-group.

5.23 Lemma. *Let $q = 2^f, f$ odd, and $G = PGL_2(q)$ in its action on the projective line. Then the set-stabilizer G_F of a 5-set F is either trivial or an elementary abelian group of order 4, with precisely one fixed point.*

Define a design $\mathcal{D}$ on $PG(1,q)$ with block set $\mathcal{B}$ consisting of the 5-sets with a nontrivial stabilizer. As each such 5-set can be written in a unique way as the union of a 4-set S and the fixed point of G_S we see that the number of blocks is $b = \binom{q+1}{4}$. We claim that the parameters are $4-(q+1,5,5)$. Indeed, let $S = \{a,b,c,d\}$ be given. We have to count the elements $x \in PG(1,q) \setminus S$ such that the 5-set $F = S \cup \{x\}$ has a nontrivial stabilizer. This stabilizer is then a four-group V. We see that the fixed point of V must be an element of F. If the fixed point is x, then $V = G_S$ and x is the fixed point of V. So assume the fixed point of V is in S. As G_S is transitive on S we may assume a is this fixed point. Then V must contain an element σ achieving the following operation: $\sigma(a) = a, \sigma : b \longleftrightarrow c, d \longleftrightarrow x$. Because of the sharp triple transitivity of G we see that an involution σ is uniquely determined by the first three operations. This shows that x is uniquely determined as image of d under σ. We see that the number of blocks containing S is indeed $\lambda = 1 + 4 \cdot 1 = 5$. We have proved the following:

5.24 Theorem (Alltop's designs). *Let $q = 2^f, f$ odd, and $G = PGL_2(q)$ in its action on the projective line. Let a 5-set $F \subset PG(1,q)$ be a block if and only if its stabilizer in G is nontrivial. This defines a simple design with parameters*

$$4 - (2^f + 1, 5, 5) \text{ for } f \text{ odd.}$$

Variants of this idea can be used to construct several families of 4-designs. See [4], where a simple construction is given of designs $4 - (2^f + 1, 6, 10)$ for f odd.

5.6 The projective linear groups

The linear groups $GL_n(q)$ had been introduced in Section 1.22. In Section 5.5 we studied the projective linear groups in dimension $n = 2$. In this section we collect some facts about the structure of these groups in the general case. The natural geometrical object on which $PGL_n(q)$ operates is the projective $(n-1)$-dimensional geometry $PG(n-1,q)$. We have introduced the special case of the projective line $PG(1,q)$ in Definition 5.16.

5.25 Definition (projective space). *Let $V = V(n,q)$ be an n-dimensional vector space over $\mathbb{F}_q$. The projective $(n-1)$-dimensional geometry $PG(n-1,q)$ has as objects the subspaces of dimensions between 1 and $n-1$. Here 1-dimensional subspaces are called* **points**, *2-dimensional subspaces are* **lines**, *and so on. The $(n-1)$-dimensional subspaces are* **hyperplanes.** *Incidence between objects is defined by inclusion. As the scalar matrices fix every subspace, we have a natural operation of $PGL_n(q)$ on the objects of $PG(n-1,q)$.*

Observe that the operation of $PGL_n(q)$ preserves incidence If for instance P is a point, l is a line and $\sigma \in PGL_n(q)$, then $P \in L$ if and only if $p\sigma \in l\sigma$.

5.26 Lemma. *$PSL_n(q)$ is 2-transitive on the points of $PG(n-1,q)$.*

Proof. It is easier to consider the action of $SL_n(q)$. Let P_1, P_2 be two different points. Adapting the basis we see that the stabilizer of P_1 and P_2 in $SL_n(q)$ consists precisely of the matrices

$\begin{pmatrix} \lambda & 0 & 0 \\ 0 & \mu & 0 \\ * & * & A \end{pmatrix}$, where $\lambda, \mu \in \mathbb{F}_q^*$, $*$ denote arbitrary matrices and A is an $(n-2, n-2)$-matrix of determinant $\frac{1}{\lambda\mu}$. It follows that the order of the stabilizer is $(q-1)^2 q^{2(n-2)}|SL_{n-2}(q)| = \frac{q(q^n-1)(q^{n-1}-1)}{(q-1)^2}$. As this is the same as the number $\frac{q^n-1}{q-1}(\frac{q^n-1}{q-1}-1)$ of pairs of points, we are done. □

5.27 Theorem. *$PGL_n(q)$ acts regularly on the ordered sets of $n+1$ points* **in general position** *of $PG(n-1, q)$. Here a set of points is in general position if any n of them generate the whole space.*

Proof. Sets of n points in general position correspond to a basis of the underlying vector space. It is clear that $PGL_n(q)$ permutes these transitively. So let $\{v_1, v_2, \ldots, v_n\}$ be a basis of $V = V(n, q)$. The stabilizer of the corresponding points $P_i = \mathbb{F}_q v_i$ in $GL_n(q)$ consists precisely of the diagonal matrices. A point $P = \mathbb{F}_q v$ complements the P_i to a set of points in general position if and only $v = \sum_{i=1}^n \lambda_i v_i$, where $\lambda_i \neq 0$ for all i. It is obvious that the scalar matrices are transitive on these vectors. The number of such $(n+1)-$tuples is

$$\frac{q^n-1}{q-1} \cdot \frac{q^n-q}{q-1} \cdot \ldots \cdot \frac{q^n-q^{n-1}}{q-1} \cdot \frac{(q-1)^n}{q-1} = |PGL_n(q)|.$$

□

5.7 The simplicity of $PSL_n(q)$.

5.28 Definition (transvections). *An element $\tau \in SL_n(q)$ is called a* **transvection** *if one of the following equivalent conditions is satisfied:*

1. *$rank(\tau - I) = 1$ and τ acts trivially on the image of $\tau - I$, (here I denotes the unit matrix).*

2. *There is a basis of V such that τ is represented by the matrix $\begin{pmatrix} I & 0 \\ C & 1 \end{pmatrix}$, where I is the $(n-1, n-1)$ unit matrix, 0 is a 0-column, C is an arbitrary nonzero $(1, n-1)-$ row and 1 is 1.*

3. *There is a hyperplane $H \subset V$, a vector $0 \neq d \in H$ and a nonzero linear functional $\chi : V \longrightarrow \mathbb{F}_q$ with kernel H such that $v\tau = v + (v\chi)d$. We write then $\tau = \tau_{u,d}$ (and d is the* **direction** *of τ).*

The matrix representation shows that the transvections with respect to the same hyperplane H form a subgroup, that this subgroup is abelian and that every transvections has order p, where p is the prime a power of which is q.

5.29 Theorem. *The transvections form a conjugacy class of elements of order p in $GL_n(q)$.*

Proof. We know that each transvection has order p. As $GL_n(q)$ is transitive on hyperplanes it suffices to show that the transvections belonging to a fixed hyperplane H are conjugate. This is shown by the following calculation:

$$\begin{pmatrix} G^{-1} & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} I & 0 \\ C & 1 \end{pmatrix} \cdot \begin{pmatrix} G & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} I & 0 \\ CG & 1 \end{pmatrix}.$$

□

5.30 Theorem. *Let $0 \neq d \in V = V(n,q)$. Let $T(d)$ consist of all transvections with direction d and the neutral element. Then $T(d)$ is a normal subgroup of the stabilizer of d in $GL_n(q)$. The group $T(d)$ is elementary abelian of order q^{n-1} and the stabilizer $GL_n(q)$ is a semidirect product of $T(d)$ and a group $GL_{n-1}(q)$.*

Proof. As $d \in H$ we have that every transvection with direction d fixes d. Let $\tau_i = \tau_{u_i,d}$, where $\tau_i : V \longrightarrow I\!F_q$ is a linear functional with kernel H_i and $d \in H_i$. We have $v\tau_1\tau_2 = (v + u_1(v)d)\tau_2 = v + u_1(v)d + u_2(v + u_1(d))d = v + (u_1(v) + u_2(v))d$. We see that $T(d)$ is an elementary abelian group. As there are precisely q^{n-1} functionals $: V \longrightarrow I\!F_q$ with d in their kernel we also obtain the order of $T(d)$.
Choosing d as first element of a basis we see that the stabilizer $GL_n(q)_d$ consists of the matrices of the form $\begin{pmatrix} 1 & 0 \\ C & A \end{pmatrix}$, where $A \in GL_{n-1}(q)$ and C is arbitrary. We can write $GL_n(q)_d$ as a semidirect product of $T(d)$ and of the complement consisting of the $\begin{pmatrix} 1 & 0 \\ 0 & A \end{pmatrix}$. □

5.31 Theorem. *If either $n \geq 3$ or the characteristic is 2, then the transvections form a conjugacy class in $SL_n(q)$.*

Proof. We know that the transvections are contained in $SL_n(q)$ and that they form a conjugacy class in $GL_n(q)$. Fix a transvection τ As the index of

$SL_n(q)$ in $GL_n(q)$ is $q-1$ we have to show that under the conditions above for every $\alpha \in \mathbb{F}_q^*$ there is an element of $GL_n(q)$ commuting with τ, whose determinant is α. In fact, choose $\begin{pmatrix} I & 0 \\ C & 1 \end{pmatrix}$, where $C = (1, 0, 0, \ldots, 0)$. Put $\rho = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & A & 0 \\ 0 & 0 & \lambda \end{pmatrix}$, where $\lambda \in \mathbb{F}_q^*$ and A is a regular $(n-2, n-2)-$matrix. Then $\rho\tau = \tau\rho$. If $n \geq 3$, then $det(A)$ attains any given value in $\mathbb{F}_q^*$. If $n = 2$, then λ^2 varies over all elements of $\mathbb{F}_q^*$, in characteristic 2. □

5.32 Theorem. *The transvections generate $SL_n(q)$.*

Proof. Let T be the set of transvections, $N = \langle T \rangle$ the subgroup of $SL_n(q)$ generated by the transvections. Then $1 \neq N \trianglelefteq SL_n(q)$. We have to show that $N = SL_n(q)$. As $SL_n(q)$ is 2-transitive on the nonzero vectors (this follows from Lemma 5.26) we conclude from Theorem 2.13 that N is transitive on the nonzero vectors. Let d be a nonzero vector. It suffices to show that N contains the stabilizer $SL_n(q)_d$. As $SL_n(q)_d$ is a semidirect product of $T(d)$ and the group consisting of the matrices of the form $\begin{pmatrix} 1 & 0 \\ C & A \end{pmatrix}$, where $A \in SL_{n-1}(q)$, we are in an inductive situation, (for the basis $n = 2$ see the Problems section). We can assume that $n \geq 3$ and that $SL_{n-1}(q)$ is generated by transvections. It is clear that these yield transvections of our complement. We have shown that $SL_n(q)_d$ is generated by transvections and are done. □

5.33 Lemma. *We have $SL_n(q)' = SL_n(q)$, unless $(n, q) = (2, 2)$ or $(n, q) = (2, 3)$.*

Proof. Because of the preceding Theorem 5.32 it suffices to show that each transvection is a commutator.
Let $n \geq 3, \tau \in T(d)$. From the description of $T(d)$ and $SL_n(q)_d$ we see that we can choose $\sigma \in T(d)$ and $g \in SL_n(q)_d$ such that $\sigma^g = \tau\sigma$. It follows $\tau = [\sigma, g]$.
In case $n = 2$ we calculate the following commutator in $SL_2(q)$:

$$\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} \cdot \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \alpha^{-1} & 0 \\ 0 & \alpha \end{pmatrix} \cdot \begin{pmatrix} 1 & -\beta \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \beta(\alpha^2 - 1) \\ 0 & 1 \end{pmatrix}.$$

We have represented a transvection as a commutator in $SL_2(q)$ if we can find $\alpha \neq 0$ such that $\alpha^2 \neq 1$. This is always possible, with the exceptions of $q = 2$ and $q = 3$. □

5.34 Theorem. *$PSL_n(q)$ is a simple group, unless $(n,q)=(2,2)$ or $(n,q)=(2,3)$.*

Proof. Assume N is a nontrivial normal subgroup of $G=PSL_n(q)$. It follows from Theorem 2.13 that N is transitive on the points of $PG(n-1,q)$. Let $0\neq d\in V$, put $P=\mathbb{F}_q d$. As the stabilizer of d in $GL_n(q)$ is a semidirect product with $T(d)$ as normal subgroup we conclude that $G_P=TH$, where $T\lhd G_P$ is the image of $T(d)$ mod Z (precisely $T=T(d)Z/Z$). In particular T is abelian. Consider the subgroup TN of G (see Theorem 1.109). As it contains T and N is transitive on the points of $PG(n-1,q)$, we see that NT contains the images mod Z of all transvections. As the transvections generate $SL_n(q)$ we conclude $G=TN$. By the second isomorphism theorem (Theorem 1.110) $G/N\cong T/(T\cap N)$. As T is abelian, G/N is abelian. Assume now we are not in one of the two exceptional situations. We have proved in Lemma 5.33 that $G=G'$. This means that G does not have any nontrivial abelian factorgroup. We conclude $G=N$. $\square$

5.8 Quadrics and ovals

Projective geometries are important mainly because roots of homogeneous polynomials live in them. We illustrate this point by using the quadratic polynomial Y^2-XZ in three variables, whose coefficients we consider as elements of $\mathbb{F}_q$. If (x,y,z) is a solution vector, then also every scalar multiple $(\mu x,\mu y,\mu y)$ is, where $0\neq\mu\in\mathbb{F}_q$. We can therefore view the set of roots to consist of points of $PG(2,q)$. This works for every homogeneous polynomial $p(X,Y,Z)$. Denote the set of its roots in $PG(2,q)$ by $V(p(X,Y,Z))$. Here the letter V stands for "variety". In general a **quadric** is the set of roots of a quadratic homogeneous polynomial. If the polynomial has n variables, then the quadric is a point set in the $(n-1)$-dimensional projective geometry.
It is easy to check that $V(Y^2-XZ)$ consists of $q+1$ points, more precisely $V(Z^2-XY)=\{(0:0:1)\}\cup\{P_\alpha|\alpha\in\mathbb{F}_q\}$, where $P_\alpha=(1:\alpha:\alpha^2)$. We claim that no line contains more than two points of $V(Z^2-XY)$. Equivalently we have to prove the following: if we write the vectors generating the points of $V(Z^2-XY)$ as columns of a $(3,q+1)-$matrix, then any three columns are linearly independent. Such sets of three columns are of one of the following two types, either $\begin{pmatrix}0&1&1\\0&\alpha&\beta\\1&\alpha^2&\beta^2\end{pmatrix}$ or $\begin{pmatrix}1&1&1\\\alpha&\beta&\gamma\\\alpha^2&\beta^2&\gamma^2\end{pmatrix}$. We leave it to the

reader to check that these matrices have nonzero determinant.

5.35 Lemma. *Let X be a point set in $PG(2,q)$ such that no line contains more than two points of X. Then $|X| \leq q+2$.*

Proof. This follows from the fact that there are precisely $q+1$ lines through each point. $\square$

5.36 Definition ((hyper)ovals). *Let X be a point set in $\mathcal{P}_2(q)$ such that no line contains more than two points of X. If $|X| = q+1$, then X is an* **oval.** *If $|X| = q+2$, then X is a* **hyperoval.**

5.37 Theorem. *$PG(2,q)$ contains ovals.*

Proof. We have seen that $V(Y^2 - XZ)$ is an oval. $\square$

5.38 Lemma. *If q is odd, then there are no hyperovals in $PG(2,q)$. If q is even, then every oval is embedded in a unique hyperoval.*

Proof. Let X be a hyperoval, P a point not in X. The points of X occur in pairs on lines through P. This shows that $q+2$. must be even. It follows that q is even.
Let new q be even, X an oval. We observe that every point of X is on precisely one tangent to X, the remaining q linea through the point passing through two points of X. As $q+1$ is odd we see that every point not in X is on at least one tangent to X. Let $N \notin X$ be a point, where two tangents to X intersect. Assume N is on a secant to X. Then N must also be on a line h missing X. As each point $\neq N$ on h is on some tangent, we see that the number of tangents is $> q+1$, contradiction. We conclude that all tangents intersect in the same point N (the **nucleus** of X), and $X \cup \{N\}$ is the unique hyperoval containing X. $\square$

5.9 The large Witt designs

Our main aim in this section is the construction of a design $S(5,8,24)$, the **large Witt design.** If we fix three points of a hypothetical $S(5,8,24)$ and consider the blocks containing these three points we obtain a design $S(2,5,21)$ on the remaining points (see Lemma 5.3). These are the parameters of a projective plane of order 4. We have seen in Definition 5.6 that the 2-dimensional projective geometry $PG(2,4)$ is an $S(2,5,21)$. We leave it as a (relatively difficult) problem to show that this is the only $S(2,5,21)$ (see the Problems section).

Let Π be the point set of $PG(2,4)$. We use $\Omega = \Pi \cup \{a_1, a_2, a_3\}$ as set of points of the $S(5,8,24)$. We can use the sets $l \cup \{a_1, a_2, a_3\}$, where l runs through the 21 lines of $PG(2,4)$, as the family of blocks containing $\{a_1, a_2, a_3\}$. In order to be able and construct our design while also proving its uniqueness we need to know more about substructures of $PG(2,4)$ and the action of $G = PGL_3(4)$ and $G_0 = PSL_3(4)$.

We collect a few basic data: G_0 is a simple group of order $2^6 \cdot 9 \cdot 5 \cdot 7$ and a normal subgroup of index 3 in G. Clearly $PG(2,4)$ contains Fano planes (just consider the points corresponding to vectors all of whose entries are in the subfield $\mathbb{F}_2$). Each Fano plane is generated by each of its quadrangles (sets of four points in general position). Here we say that a point set X generates a projective subplane A if A is the smallest projective plane containing X. As G is transitive on quadrangles we conclude that G is transitive on the set of Fano planes contained in $PG(2,4)$. Clearly the stabilizer of a Fano plane in G is $GL_3(2)$. We conclude from the orbit length lemma that the number of Fano subplanes of $PG(2,4)$ is $|G|/168 = 360$. As $GL_3(2)$ is a simple group we see that it is contained in G_0. It follows again from the orbit length lemma that G_0 has three orbits of Fano planes, each of length 120.
We know that the number of (unordered) quadrangles is $|G|/4! = 7 \cdot 360$. The stabilizer of a quadrangle is S_4. As this group is generated by involutions, we conclude that the stabilizer of a quadrangle is contained in G_0. It follows that G_0 has three orbits of quadrangles, each of size $7 \cdot 120$.

5.39 Lemma. *Each quadrangle of $PG(2,4)$ is contained in precisely one hyperoval. There are 168 hyperovals in $PG(2,4)$. The group G is transitive on hyperovals, while G_0 has three orbits of hyperovals, each of length 56.*

Proof. The first statement is best read off from a picture of the Fano plane. Let Q be a quadrangle and E the Fano plane containing Q. There is precisely one line in the Fano plane avoiding Q. This line has five points, three in E and two outside E. These two points are the only ones that complement Q to a hyperoval. We conclude that G is transitive on hyperovals. As there are $7 \cdot 360$ quadrangles, and each hyperoval contains 15 quadrangles, we count $7 \cdot 360/15 = 168$ hyperovals. The order of the stabilizer of a hyperoval in G is therefore $|G|/168 = 6!/2$. As this stabilizer is a subgroup of S_6 and A_6 is a simple group we conclude that the stabilizer of a hyperoval is A_6. By a by now familiar argument we conclude from the simplicity of A_6 that G_0 has three orbits on hyperovals. □

5.40 Lemma. *Each triangle in $PG(2,4)$ is in precisely three hyperovals, one from each G_0-orbit.*

Proof. It is clear that G_0 is transitive on triangles. The rest follows from a familiar counting argument. □

We note that this suffices to construct $S(3,6,22)$: take as point set $\Pi \cup \{\infty\}$ and as blocks the lines of $PG(2,4)$, including ∞, as well as the hyperovals from one G_0-orbit. As we aim higher we have to work a little more.

5.41 Lemma. *The* **block intersection numbers** *of a design are the cardinalities of the intersections of two different blocks. For the designs involved here the possible block intersection numbers are:*

design	*block intersection numbers*
$S(2,5,21)$	*1*
$S(3,6,22)$	*0,2*
$S(4,7,23)$	*1,3*
$S(5,8,24)$	*0,2,4*

Proof. $S(2,5,21)$ is a projective plane. It follows that two blocks intersect in one point. The statement on $S(3,6,22)$ follows. Proceeding like this we see that the only thing that remains to be proved is that block intersection number 0 cannot occur in $S(4,7,23)$. This follows from the usual counting arguments: in fact, fix a block B. As $\lambda_3 = 5$, we see that each of the 35 triples in B is contained in four blocks $\neq B$. It follows that $35 \cdot 4 = 140$ points intersect B in three points. Fix $P \in B$. As $\lambda_1 = 77$ and P is on 15 triples contained in B, we see that $77 - 1 - 15 \cdot 4 = 16$ blocks intersect B precisely in P. It follows that $16 \cdot 7 = 112$ blocks intersect B in cardinality 1. As $1 + 140 + 112 = 253$ happens to be the number of blocks of the design, we have proved that no two blocks intersect trivially. □

5.42 Lemma. *Let B be a block of our putative design $S(5,8,24)$. Put $A = \{a_1, a_2, a_3\}$. Then the following hold:*

- *If $B \supset A$, then $B \cap \Pi$ is a line of $PG(2,4)$.*

- *If* $|B \cap A| = 2$, *then* $B \cap \Pi$ *is a hyperoval.*
- *If* $|B \cap A| = 1$, *then* $B \cap \Pi$ *is a Fano plane.*
- *If* $B \cap A = \emptyset$, *then* $B \cap \Pi$ *is a* **double line** *(union of two lines, with the point of intersection omitted).*

Proof. The first case is clear. Let $|B \cap A| = 2$. It follows from the block intersection numbers that each line meets the 6-set $B \cap \Pi$ in 0 or 2 points. It follows that $B \cap \Pi$ is a hyperoval.
Let $|B \cap A| = 1$. The block intersection numbers show that each line meets the 7-set $E = B \cap \Pi$ in 1 or 3 points. It follows that the incidence structure induced by the lines on E is an $S(2, 3, 7)$, a Fano plane. Let finally $B \subset \Pi$. We see that every point $P \in B$ is on exactly one line meeting B in four points. □

This limits the number of 8-sets from which to choose the blocks of our design. In fact, the number of candidates is $21 + 168 + 360 + \binom{21}{2} = 759$. As this happens to be the number of blocks of an $S(5, 8, 24)$ we do not have much choice.

5.43 Definition. *Label the* G_0-*orbits* $\mathcal{Q}_i$ *of quadrangles,* $\mathcal{X}_i$ *of hyperovals and* $\mathcal{E}_i$ *of Fano planes such that the following hold:*

- *If* $Q \in \mathcal{Q}_i, Q \subset E, E$ *a Fano plane, then* $E \in \mathcal{E}_i$.
- *If* $Q \in \mathcal{Q}_i, Q \subset X, X$ *a hyperoval, then* $X \in \mathcal{X}_i$.

We define blocks to be all the 8-sets as follows:

1. $A \cup l$, *where* l *is a line of* $\mathcal{P}_2(4)$.
2. $\{a_i, a_j\} \cup X$, *where* X *is a hyperoval from* $\mathcal{X}_k$ *and* $\{i, j, k\} = \{1, 2, 3\}$.
3. $\{a_i\} \cup E$, *where* E *is a Fano plane from from* $\mathcal{E}_i$.
4. *All 210 double lines*

5.44 Theorem. *The design constructed in Definition 5.43 is an* $S(5, 8, 24)$.

Proof. As we have used the right number 759 of blocks it suffices to prove that any 5-set $Y \subset \Omega = A \cup \Pi$ is in at least one block.
If $Y \supset A$, then Y is on a block of the first type. Let $Y \cap A = \{a_1, a_2\}$. We can assume that the points from $Y \cap \Pi$ form a triangle. By Lemma 5.40 a triangle is contained in (exactly one) hyperoval from orbit $\mathcal{X}_3$.
Let $Y \cap A = \{a_1\}$. We are done if the four points of $Y \cap \Pi$ are either collinear or from a quadrangle. The only other possibility is that they form what we may call a **double triangle:** three points on a line l, the fourth point off l. The usual type of double counting argument shows that G_0 is regular on double triangles and that each double triangle is in eactly three Fano planes, one from each orbit.
Remains the case $Y \subset \Pi$. We are done if some four points are collinear (= on a line) or if no three points are collinear (the hyperoval case). So let P, Q, R be collinear on line l, and S, T the two remaining points. If line ST intersects l in P, Q or R, then Y is contained in a Fano plane. If not, then Y is in a double line. □

This theorem, together with the block intersection numbers of Lemma 5.41, gives us additional information on the structure of $PG(2, 4)$:

5.45 Lemma.

- *Two hyperovals are in the same G_0-orbit if and only they they intersect in even cardinality (0 or 2).*
- *Two Fano planes are in the same G_0-orbit if and only if they intersect in odd cardinality (1 or 3).*
- *A hyperoval and a Fano plane have quadrangles from the same G_0-orbit if and only they intersect in even cardinality (0,2 or 4).*

We conclude that $S(5, 8, 24)$ is uniquely determined up to isomorphism. In fact, the derived design of an $S(5, 8, 24)$ with respect to three points is an $S(2, 5, 21)$ or projective plane of order 4, which is is uniquely determined (see the Problems section). We know from Lemma 5.42 the intersections $B \cap \Pi$ of all the blocks. Lemma 5.45 shows that B is always uniquely determined by $B \cap \Pi$, up to a permutation of A.

5.46 Theorem. *There is up to isomorphism exactly one design $S(5, 8, 24)$, the* **large Witt design.**

The situation is so tight that we can determine the automorphism group of this design. Denote by M_{24} the automorphism group of the large Witt design and by M_{24-i} the pointwise stabilizer of i points, $i = 1, 2, 3, 4, 5$. The construction shows that M_{24} is 3-transitive. As by construction $M_{21} \geq G_0 = PSL_3(4)$ we see that M_{21} is still 2-transitive on the remaining 21 points. It follows that M_{24} is 5-transitive and $|M_{24}| = 24 \cdot 23 \cdot 22 \cdot |M_{21}| \geq 24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 48$. Fix a set A of three points. Let H be the set-stabilizer of A in M_{24}. It follows $|M_{24}| = \frac{24 \cdot 23 \cdot 22}{6} |H|$. On the other hand $H \leq Aut(PG(2,4))$. We know the group $G = PGL_3(4) \leq Aut(PG(2,4))$, which is transitive on hyperovals and induces A_6 on a hyperoval. As the stabilizer of a hyperoval in $Aut(\mathcal{P}_2(4))$ must clearly by faithfully represented on the hyperoval and can therefore be at most S_6 we conclude that $Aut(\mathcal{P}_2(4))$ can be at most double as big as G. It follows $|M_{24}| \leq 24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 48$. We must have equality.

5.47 Theorem. *The full automorphism group of the $S(5, 8, 24)$ is a 5-transitive group M_{24} (the* **large Mathieu group***) of order*

$$|M_{24}| = 24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 48.$$

The stabilizer of three points is the simple group $PSL_3(4)$.

As a corollary we see that the full automorphism group of $PG(2,4)$ has order $2^7 \cdot 3^3 \cdot 5 \cdot 7$ and induces the full symmetric group S_6 on each hyperoval.

5.48 Theorem. $M_{24}, M_{23}, M_{22}, M_{21}$ *are simple groups*

Proof. We know that $M_{21} \cong PSL_3(4)$ is simple (Theorem 5.34). Let us show that M_{22} is simple. If this is not the case, then by Theorem 2.15 M_{22} contains a regular normal subgroup N (of order 22). Let $H \cong M_{21}$ be the stabilizer of a point. Then $M_{22} = HN$. Let H act on N by conjugation. As $Aut(N)$ is solvable and H is simple, we conclude that H must induce the identity group on N. It follows $[H, N] = 1$ and $H \triangleleft M_{22}$. Conjugation under N shows that H fixes every point, hence $H = 1$, contradiction. We have proved that M_{22} is a simple group.
The same argument proves that M_{23} and M_{24} are simple. □

5.10 The binary Golay code and the small Witt designs

5.49 Definition (codes). *A* **linear code** *over $\mathbb{F}_q$ is a subspace $\mathcal{C}$ of the vector space $\mathbb{F}_q^n$ of n-tuples. Its* **minimum distance** *d is the largest number* *such that any two different elements of $\mathcal{C}$ differ in at least d coordinates. The* **(Hamming) weight** *$wt(v)$ is the number of coordinates, where v has nonzero entry. The parameters of such a code are recorded as*

$$[n, k, d]_q$$

(n is the **length**, *k the dimension). For $x, y \in \mathbb{F}_q^n$ consider the scalar product $x \cdot y = \sum_{i+1}^n x_i y_i$. As this is nondegenerate the* **dual code** *$\mathcal{C}^\perp = \{y | x \cdot y = 0$ for all $x \in \mathcal{C}\}$ has dimension $n - k$.*

5.50 Definition (binary Golay code). *Identify the set Ω of points of $S(5, 8, 24)$ with a basis of $\mathbb{F}_2^{24}$ and identify each vector with its support. The code $\mathcal{G}$ generated by the blocks of $S(5, 8, 24)$ is the* **binary Golay code.** *The 759 vectors corresponding to blocks will be called* **octads.**

The blocks of the Witt design constitute 759 vectors of weight 8. We ask what the dimension d and minimum distance k of $\mathcal{G}$ are. As all the block intersections are even (Lemma 5.41) we conclude that $\mathcal{G} \subseteq \mathcal{G}^\perp$. In particular $k \leq 12$. As every point $P \in \Omega$ is in precisely 253 blocks we see that the sum over all octads is the all-1-vector $\mathbf{1} = (1, 1, 1, \dots)$. Consider the factor space $\mathcal{G}/\langle \mathbf{1} \rangle$, of dimension $k - 1$. The group M_{24} in its operation as a permutation group of the coordinates operates as a group of linear mappings on this space. As M_{24} is simple we see that $M_{24} \leq GL_{k-1}(2)$. We know that 23 divides the order of M_{24} and we can compare with the orders of the linear groups. As 23 does not divide $2^i - 1$ for any $0 \leq i < 11$ we conclude that $k - 1 \geq 11$ and hence $k = 12$. It follows $\mathcal{G} = \mathcal{G}^\perp$.

5.51 Definition. *Let $\mathcal{C}$ be a code $[n, k, d]_q$. Denote by A_i the number of vectors $v \in \mathcal{C}$ having weight i.*

Clearly $A_0 = 1$ and $A_i = 0$ for $0 < i < d$. Also $\sum_i A_i = |\mathcal{C}| = q^k$.
Back to the binary Golay code. We know that all weights are multiples of 4 (see the Problems section). The presence of the all-1 vector shows not only $A_{24} = 1$ but also $A_{24-i} = A_i$ for all i. We claim that $A_4 = 0$. In fact, let $Q \subset \Omega$ be a subset of cardinality 4, which is in $\mathcal{G}$. Choose a block (octad) intersecting Q in precisely three points. This contradicts the fact that $\mathcal{G}$ is self-dual. In the same spirit it is easy to see that the blocks are the only vectors of weight 8. In fact, let $X \subset \Omega$ be of cardinality eight and contained in $\mathcal{G}$. Choose a block meeting X in at least 5 (hence in at least 6) points. Because of linearity $X + B$ also is a code-word. As its weight is ≤ 4, it is the 0-word,

thus $X = B$. We have proved $A_4 = A_20 = 0, A_8 = A_{16} = 759, A_0 = A_{24} = 1$. As $\sum_i A_i = 2^{12}$, we see that A_{12} is uniquely determined as well.

5.52 Theorem. *The binary Golay code $\mathcal{G}$ has parameters* $[24, 12, 8]$. *It is self-dual ($\mathcal{G} = \mathcal{G}^{\perp}$) and has weight distribution*

$$A_0 = A_{24} = 1, A_8 = A_{16} = 759, A_{12} = 2576.$$

The codewords of weight 12 of the binary Golay code (or their supports) are called **dodecads.** Let D be a dodecad, $T \subset D$ a 5-set, $B \supset T$ the unique block containing it. As B must meet D in even cardinality and cannot be contained in D ($B + D$ would have weight 4 otherwise), we conclude $|B \cap D| = 6$. This shows that we obtain a Steiner system $S(5, 6, 12)$.

5.53 Theorem (small Witt design). *Let D be a dodecad (word of weight 12) of the binary Golay code. The family of 6-subsets of D, which are contained in octads, form the block of a design $S(5, 6, 12)$.*

We see that the binary Golay code contains 2576 copies of design, which have the parameters of the small Witt design.

5.11 Problems

1. Show that every projective plane has the property that any two different lines have precisely one point in common.

2. Show that affine planes have the following property: If l is a line and P a point not on l, then there is precisely one line h through P, which intersects l trivially (is **parallel** to l).

3. Show that an affine plane of order n exists if and only if a projective plane of order n exists.

4. Show that the classical affine plane of order 3 as defined in Definition 5.6 is the only $S(2, 3, 9)$.

5. Construct a 1-factorization for the cubic graph on $2u$ vertices, whose vertices are elements of $\mathbb{Z}/2u\mathbb{Z}$, edges are the $\{i, i+1\}$ and the $\{i, i+u\}$.

6. Construct a 1-factorization for the cubic graph on $2u$ vertices, whose vertices are the elements of $(\mathbb{Z}/u\mathbb{Z}) \times \{0,1\}$ with edges $\{(i,0),(i+1,0)\}, \{(i,1),(i+1,1)\}$ and $\{(i,0),(i,1)\}$.

7. Use a variant of the construction in Theorem 5.13 to prove the following:
If an $S(3,4,n)$ exists, then an $S(3,4,2n)$ exists.

8. Show that the center Z of $GL_2(q)$ consists of the scalar matrices and is therefore a cyclic group of order $q-1$.

9. Prove that the kernel of $GL_2(q)$ in its permutation representation on the $q+1$ one-dimensional subspaces of V is precisely the center Z.

10. Show that $PGL_2(q)$ is not 4-homogeneous on the projective line.

11. Let $S = \{\infty, 0, 1\}$. Describe all the elements of the stabilizer $PGL_2(q)_S$.

12. Show that $SL_2(q)$ is generated by transvections.

13. Determine the structure of the groups $GL_2(2)$ and $GL_2(3)$. Show in particular that they are solvable.

14. Show that there is up to isomorphism only one $S(2,5,21)$ (= projective plane of order 4).

15. Show that there is up to isomorphism only one $S(2,3,7)$ and that its full automorphism group is the simple group $GL_3(2) = PGL_3(2) = PSL_3(2)$ of order 168.

16. Prove the following: If x, y are binary vectors of the same length, both of weight divisible by four and with even intersection (the number of coordinates where both x and y has entry 1 is even), then $x+y$ has weight divisible by four.

Appendix A

Transfer and fusion

A.1 Definition (fusion). *Let $H \leq G$ and $A, B \subseteq H$. Write $A \sim_H B$ if there exists $h \in H$ such that $A^h = B$. We call A and B* **fusioned** *in G if $A \not\sim_H B$ but $A \sim_G B$.*

Transfer is an important means to prove fusion theorems. We start with some easy cases without using transfer. Remember that elements of order 2 are called **involutions**.

A.2 Theorem (Thompson). *Assume G does not contain a (normal) subgroup of index 2. Let M be a maximal subgroup of $S \in Syl_2(G)$. Then every involution in G is conjugate to some involution in M.*

Proof. We have $[G : M] = 2u$, where u is odd. Consider the permutation representation of G on the right cosets of M. Let $z^2 = 1$, assume z is not conjugate under G to some element of M. Then z does not fix any coset of M as otherwise $Mg = Mgz$ for some g, which leads to the contradiction $gzg^{-1} \in M$. It follows that z is the product of u transpositions, hence $z \notin A_{2u}$. Consequently $G \cap A_{2u}$ is a subgroup of index 2 in G, contradiction. □

A.3 Theorem (Burnside). *Let $P \in Syl_p(G)$ and A, B normal subsets (= unions of conjugacy classes) of P. Then the following holds:*

$$A \sim_G B \text{ if and only if } A \sim_{N_G(P)} B.$$

Proof. Let $A^g = B$. Then $N = I\!N(B)$ contains P and P^g. By Sylow's theorem, applied to N, we see that there is some $h \in N$ such that $P = P^{gh}$, hence $gh \in I\!N_G(P)$ and $A^{gh} = B^h = B$. □

A.4 Definition (transversals). *Let $H \leq G, [G:H] = n$. A* **right transversal** *is a set $T = \{t_1, t_2, \ldots, t_n\}$ of representatives of the distinct right cosets of H in G. A* **left transversal** *is defined analogously. Let T be a right transversal, $t \in T, x \in G$. Then $Htx = Ht'$ for some $t' \in T$. In particular $tx = ht'$, where $h \in H$ and $t' \in T$ are uniquely determined. We define functions*

$$\alpha_x^T : T \longrightarrow H, \phi_x^T : T \longrightarrow T$$

by $tx = (t\alpha_x^T)(t\phi_x^T)$.

A.5 Definition (transfer). *Let $H \leq G, [G:H] = n < \infty, T$ a right transversal of H in G and $H' \leq K \leq H$. The* **transfer** *$V = V_{G \longrightarrow H/K} : G \longrightarrow H/K$ is defined by*

$$xV = K \prod_{t \in T} (t\alpha_x^T).$$

A.6 Lemma. *Let $H \leq G, T$ a right transversal and $V = V_{G \longrightarrow H/K}$ the transfer. Then V is independent of the choice of right transversal and V is a homomorphism $V : G \longrightarrow H/K$.*

Proof. As the image of V is contained in the abelian group H/K we can reorder at our ease. At first we prove the independence. So let S be an arbitrary right transversal, $s = h_t t \in S$, where $h_t \in H$. We have $sx = (h_t t)x = h_t(t\alpha_x^T)(t\phi_x^T) = h_t(t\alpha_x^T)h_{t\phi_x^T}^{-1} s'$ where $s' \in S$. It follows $s\alpha_x^S = h_t(t\alpha_x^T)h_{t\phi_x^T}^{-1}$. Clearly ϕ_x^T is a permutation of T. In the product, taken mod K, the h-factors cancel.
Fix T now. We wish to show that V is a group homomorphism. We have $txy = (t\alpha_{xy})(t\phi_{xy}) = (tx)y = (t\alpha_x)(t\phi_x)y = (t\alpha_x)(t\phi_x\alpha_y)(t\phi_x\phi_y)$. We conclude

$$t\alpha_{xy} = (t\alpha_x)(t\phi_x\alpha_y) \tag{A.1}$$
$$t\phi_{xy} = t\phi_x\phi_y \tag{A.2}$$

It follows $xyV = K\prod_{t \in T}(t\alpha_x(t\phi_x)\alpha_y$. As ϕ_x affords a permutation of T it follows that $xyV = (xV)(yV)$. Inverses are treated in an analogous way. $\square$

Given $x \in G$ we can choose a transversal adapted to x. Assume the action of x on G/H has cycle type $(r_1, r_2, \ldots, r_t)$. Let $x_i \in G, i = 1, 2, \ldots t$

be a representative of a right coset belonging to the i-th orbit. Choose as transversal

$$T = \cup_{i=1}^{t}\{x_i = t_{i,0}, x_i x = t_{i,1}, \ldots, x_i x^{r_i-1} = t_{i,r_i-1}\}.$$

In particular $t_{i,j}\alpha_x = 1$ when $j < r_i-1$. Further $t_{i,r_i-1}x = x_i x^{r_i} = (x_i x^{r_i} x_i^{-1})x_i$. It follows

$$t_{i,r_i-1}\alpha_x = x_i x^{r_i} x_i^{-1} \in H$$

and $t_{i,r_i-1}\phi_x = x_i$. This leads us to the following theorem:

A.7 Theorem. *Let $H \leq G, [G:H] = n < \infty$ and $x \in G$. Let the cycle type of x in its multiplication operation on the right cosets of H be $(r_1, r_2, \ldots, r_t)$ (in particular $\sum_{i=1}^{t} r_i = n$). Then there are elements $x_i \in G, i = 1, 2, \ldots, t$ such that $x_i x^{r_i} x_i^{-1} \in H$ and*

$$xV_{G\longrightarrow H/K} = \prod_{i=1}^{t} x_i x^{r_i} x_i^{-1}.$$

We see that this is related to fusion: the r_i-th power of x is conjugate under G to some element of H.

A.8 Definition (D.G. Higman). *Let $H \leq G, [G:H] < \infty$. The* **focal subgroup** *is defined as*

$$Foc_G(H) = H_G^* = H^* = \langle h^{-1}h^g = [h,g] | h \in H, g \in G, h^g \in H\rangle.$$

Clearly we have $H' \leq Foc_G(H) \leq H$. In particular we may use $K = Foc_G(H)$ in the definition of the transfer. The case when $H = P \in Syl_p(G)$ and $K = P^*$ is the focal subgroup is of particular interest.

A.9 Lemma. *Let $[G:H] = n, V = V_{G\longrightarrow H/K}$, where $H^* \leq K \leq H$. Then the following hold:*

- *If $h \in H$, then $hV = Kh^n$.*
- *If $gcd([H:K], n) = 1$, then the restriction of V is surjective and $H \cap ker(V) = K$.*

Proof. By definition of $H^* = Foc_G(H)$ we have $Kh = Kh^g$ whenever $h \in H, g \in G, h^g \in H$. By Theorem A.7 we have $hV = K\prod_{i=1}^{t} h^{r_i} = Kh^n$. The rest is clear as raising to the n-th power is a group isomorphism in an abelian group whose order is coprime to n. □

A.10 Theorem (D.G. Higman). *Let $P \in Syl_p(G), P^* = Foc_G(P)$. Denote by $G'(p)$ the smallest normal subgroup with abelian $p-$factorgroup. The following hold:*

- $P^* = P \cap G'$.
- $G/G'(p) \cong P/P^*$.

Proof. By definition of $G'(p)$ we have $G = PG'(p)$. It follows from the second isomorphism theorem that $G/G'(p) \cong P/(P \cap G'(p))$. It follows from the Definition that $P^* \leq P \cap G'$. Lemma A.9 shows that $V : G \longrightarrow P/P^*$ is surjective and that $ker(V) \cap P = P^*$. As $G/ker(V) \cong P/P^*$ is an abelian p-group we have $ker(V) \geq G'(p) \geq G'$. We get $P^* \leq P \cap G' \leq P \cap G'(p) \leq P \cap ker(V) = P^*$. We have equality all the way. The claims follow. □

Harmless as it looks this theorem is an important insight. It says that the factor group $G/G'(p)$ is determined by the following data:

1. The isomorphism type of $P \in Syl_p(G)$, and
2. the fusion of elements in P under G.

As a corollary we obtain an important result of Burnside's:

A.11 Theorem (Burnside). *Let $P \in Syl_p(G)$. Assume$\mathbb{C}_G(P) = \mathbb{N}_G(P)$. Then G has a* **normal p-complement.** *This is a normal subgroup $N \lhd G$ such that $N \cap P = 1$ and $NP = G$.*

Proof. It follows from the assumption that P is abelian. It follows from Theorem A.3 that fusion in P is controlled by $\mathbb{N}_G(P)$. The assumption says that there is no such fusion, or equivalently $Foc_G(P) = 1$. It follows from Theorem A.10 that $G/G'(p) \cong P$. The kernel of the transfer map is a normal p-complement. □

A.12 Corollary. *Let G be a group of even order, $S \in Syl_2(G)$. If S is cyclic, then G has a normal 2-complement.*

Proof. Let S be cyclic of order 2^a. We have $|Aut(S)| = \phi(2^a) = 2^{a-1}$ (see the Problems section). Moreover we know that $\mathbb{N}_G(S)/\mathbb{C}_G(S)$ is isomorphic with a subgroup of $Aut(S)$ (see Theorem 1.111). As this is a group of odd order, we conclude $\mathbb{N}_G(S) = \mathbb{C}_G(S)$. Use Theorem A.11. □

Appendix B

Transitive extensions and the small Mathieu groups

Let (G, Ω) be a transitive permutation group. We have studied the corresponding operation $(G_x, \Omega \setminus \{x\})$ of the stabilizer. We ask under which conditions this process can be reversed. So let (H, Ω) be given. Can we find $(G, \Omega \cup \{*\})$ such that $G_* = H$? If (H, Ω) is t-transitive, then necessarily $(G, \Omega \cup \{*\})$ will be $(t+1)$-transitive. We study the case when $t \geq 2$. Let $x, y \in \Omega, x \neq y$. Pick a permutation g of $\Omega \cup \{*\}$ affording the operation $g : * \longleftrightarrow x, y \longleftrightarrow y$ and $h \in H$ such that $h : x \longleftrightarrow y$. Let $f \in H_x$. Then gfg fixes $*$ and x. It follows $gH_xg = H_x$. We will see that these conditions suffice to define a transitive extension.

B.1 Theorem (transitive extension). *Let (H, Ω) be t-transitive for some $t \geq 2$. Put $\Omega^* = \Omega \cup \{*\}$. Assume we can find a permutation g of Ω^* and an element $h \in H$ such that the following hold:*

1. $g : * \longleftrightarrow x, h : x \longleftrightarrow y, yg = y$.
2. *g^2 and $(hg)^3$ are in H.*
3. $gH_xg = H_x$.

Then $G = \langle H, g\rangle = H \cup H \cdot g \cdot H$ is $(t+1)$-transitive on Ω^* and $G_* = H$.

Proof. By assumption we have h and the new permutation g operating on the set $\{*, x, y\}$. Observe that it suffices to prove that the union $H \cup HgH$ is a group. The remaining claims follow automatically (for example this group operates on Ω^*, the element $*$ is not fixed and H is the stabilizer of $*$. As H is t-transitive, it follows that G must be $(t+1)$-transitive). Let us prove this fact. As H is a group it suffices to show that $gHg \subseteq H \cup HgH$. We use the 2-transitivity of H. By Lemma 2.8 $H = H_x \cup H_x h H_x$. It is one of our assumptions that $gH_x g = H_x$. Remains to show that $gH_x h H_x g \subseteq HgH$. This is the case: $(gH_x)h(H_x g) = (H_x g)h(gH_x) \subseteq H_x(hgh)HH_x \subseteq HgH$. Here we have used the assumptions, in particular that $(hg)^3 \in H$. □

We are going to construct some particularly interesting permutation groups, the small Mathieu groups:
Let $Z = \{a, b, c, d, e, f\}$ be a 6-set and G the group of permutations of Z. The order of G is $6! = 10 \cdot 9 \cdot 8$. The group G also operates on the $\binom{6}{3}/2$ complementary pairs of 3-subsets of Z. These form our set $\Omega = \{0, 1, \ldots, 9\}$, where

$0 = (abc\|def)$	$1 = (abd\|cef)$
$2 = (abe\|cdf)$	$3 = (abf\|cde)$
$4 = (acd\|bef)$	$5 = (ace\|bdf)$
$6 = (acf\|bde)$	$7 = (ade\|bcf)$
$8 = (adf\|bce)$	$9 = (aef\|bcd)$

We see G as a subgroup of the symmetric group on 10 objects now, without changing notation (the correct approach would be to speak of an embedding of S_6 into S_{10} and use a different symbol for the image of this embedding). Clearly G is faithful and transitive on 10 objects. Let $\phi_1 = (abc), \phi_2 = (bcd)$. These are permutations of order 3. Both stabilize object 0. In the operation on 10 points we have

$$\phi_1 = (1, 9, 4)(2, 8, 5)(3, 7, 6), \phi_2 = (1, 2, 3)(4, 5, 6)(7, 9, 8).$$

It is checked right away that ϕ_1, ϕ_2 commute. In particular we have that $E = \langle \phi_1, \phi_2 \rangle$ is elementary abelian of order 9. We also see that E is transitive on $\Omega - \{0\}$. As $|G| = 10 \cdot 9 \cdot 8$ it follows that the stabilizer $G_{0,1}$ of two points has order 8. It is now clear that $G_{0,1} = \langle (a, b), (e, f), (a, e)(b, f)(c, d) \rangle$. As this group has orbits $\{2, 3, 4, 9\}$ and $\{5, 6, 7, 8\}$ we see in particular that G is not 3-transitive on Ω.

Consider the normal subgroup $H < G$, where H is the alternate group on 6 objects. It is clear that H is transitive on 10 points. As $E < H$ it follows that H is 2-transitive on 10 points. It follows that $H_{0,1}$ has order 4. We see that $H_{0,1} = \langle\theta\rangle$ is cyclic of order 4, where

$$\theta = (a, f, b, e)(c, d) = (2, 9, 3, 4)(5, 8, 7, 6).$$

It follows that $H_0 = \langle\phi_1, \phi_2, \theta\rangle$ (of order 36). Put $\psi = (a, b)(c, d) = (01)(49)(56)(78)$. Then $H = \langle\phi_1, \phi_2, \theta, \psi\rangle$.

Our next aim is to embed H in a group, which is double as large as H (contains H as a subgroup of index 2) and is 3-transitive on 10 points. To this end consider the permutation

$$\lambda = (2735)(4698).$$

Clearly λ is not in H, as it would have to be a power of θ otherwise. We have $\lambda^2 = \theta^2 \in H$. It is easy to check that λ normalizes H. If we denote conjugation by $\alpha^\beta = \beta^{-1}\alpha\beta$, then we have in fact

$$\phi_1^\lambda = \phi_1\phi_2,\ \phi_2^\lambda = \phi_1\phi_2^{-1},\ \theta^\lambda = \theta^{-1},\ \psi^\lambda = \psi\theta.$$

Put $M_{10} = \langle H, \lambda\rangle$. We know that M_{10} contains H as a subgroup of index 2, hence has the same order $6! = 10 \cdot 9 \cdot 8$ as S_6. The operation of λ shows that M_{10} is 3-transitive, hence sharply 3-transitive. Next we construct a transitive extension of M_{10} : put $\Omega^* = \Omega \cup \{T\}$ and consider the permutation $g = (0, T)(4, 7)(5, 9)(6, 8)$. Then $g : T \longleftrightarrow 0, 1 \longleftrightarrow 1$ and $\psi : 0 \longleftrightarrow 1$. In order to be able and apply Theorem B.1 we have to check that $g(M_{10})_0 g = (M_{10})_0$. As g is an involution this is equivalent to saying that g normalizes $(M_{10})_0$. As $(M_{10})_0$ contains H_0 and has order $9 \cdot 8$ it is clear that $(M_{10})_0 = \langle\phi_1, \phi_2, \theta, \lambda\rangle$. By the way, E is a normal subgroup of $(M_{10})_0$ and a Sylow-2-subgroup is $\langle\theta, \lambda\rangle$. It is easily checked that this latter group is a quaternion group.

It is now clear that the conditions of Theorem B.1 are satisfied. The group $M_{11} = \langle M_{10}, g\rangle$ is sharply 4-transitive, of order $11 \cdot 10 \cdot 9 \cdot 8$. A Sylow-2-subgroup is $\langle\theta, \lambda, g\rangle = \langle g\theta, g\rangle$. Here $g\theta = (T, 0)(2, 9, 8, 5, 3, 4, 6, 7)$ has order 8, g is an involution and $(g\theta)^g = (g\theta)^3$. This group is known as **semidihedral group** (of order 16).

B.2 Lemma. *M_{11} is a simple group.*

Proof. Assume N is a nontrivial normal subgroup of $G = M_{11}$. It follows from Theorem 2.13 that N operates transitively. As a group of order 11 on 11 points has a normalizer of order 110 in S_{11}, it follows that $|N| > 11$. In particular $N \cap M_{10}$ is a nontrivial normal subgroup of M_{10}. Remember that M_{10} was constructed as an extension of the simple group A_6 by a nontrivial automorphism. It follows that M_{10} has the group H (isomorphic with A_6) as only nontrivial normal subgroup. If $N \supset M_{10}$, then $N = M_{11}$, contradiction. It follows $N \cap M_{10} = H$. We conclude that N has index 2 in M_{11}. The Sylow theorem will give a contradiction: let P be a Sylow-11-subgroup of N (and of M_{11}). The Sylow theorem states that all Sylow-11-subgroups are conjugate and their number (= index of the stabilizer) is $\equiv 1 \pmod{11}$. We apply this to N and to M_{11}. This leads to a contradiction. $\square$

Here is another transitive extension: let $\Omega^{**} = \Omega \cup \{T, E\}$. Let $g' = (E,T)(2,9)(3,4)(5,7)$. We can choose g as its partner in M_{11} and see that $M_{12} = \langle M_{11}, g' \rangle$ is sharply 5-transitive, of order $12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$, of course.

B.3 Lemma. *M_{12} is a simple group.*

Proof. If M_{12} is not simple, then by Theorem 2.15 it must contain a regular normal subgroup N. The number of elements of order 3 in N is certainly < 11 then. Consider the operation of the simple group M_{11} by conjugation. It will have to operate trivially. In particular we find an element of order 3, which centralizes a group M_{11}. This is impossible. $\square$

Appendix C

The small Witt design

In Appendix B we constructed the simple Mathieu group $G = M_{12}$ of order $12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$ in its sharply 5-transitive action on 12 points. We wish to use Theorem 5.15 to construct a 5-design with $k = 6$ on 12 points. We use the notation and results of Appendix B. Put $\Omega = \{E, T, 0, 1, \dots, 9\}$. Blocks are defined in the following way: Let I be the conjugacy class of involutions having four fixed points. As the pointwise stabilizer of 4 points is a quaternion group of order 8 and as Q_8 has precisely one involution we see that $|I| = \binom{12}{4}$. Each $g \in I$ yields four blocks: the unions of the four fixed points of g and two more points in the same transposition of g. So, if $g = (a)(b)(c)(d)(e,f)(g,h)(i,j)(k,l)$, then $\{a,b,c,d,e,f\}$ and $\{a,b,c,d,g,h\} \dots$ are blocks. How many blocks does this define and what is the stabilizer of a block?

We claim that each block is described precisely $\binom{6}{4} = 15$ times in this way. Concretely this claim says that if the involution g_1 fixing c,d,e,f has (a,b) as a transposition, then necessarily for every pair $\{x,y\} \subset B = \{a,b,c,d,e,f\}$ the involution g_2 with $B \setminus \{x,y\}$ as set of fixed points maps $x \longleftrightarrow y$. As the symmetric groups are generated by transpositions this is equivalent with the statement that the set stabilizer of a block is as big as possible: $G_B \cong S_6$. As $(c,d) = (a,c)^{(a,d)}$ it suffices to show that all operations of type $(a,c)(b)(d)(e)(f)$ are induced by involutions in G. So let τ be the involution with b,d,e,f as fixed points. We have to show that the $a\tau = c$. Observe that all this happens in the stabilizer of three points (d,e,f). We see that we can work in the group $(M_{10})_0$ of order $9 \cdot 8$. We have seen that $(M_{10})_0$ is the semidirect product of the normal subgroup $E = \langle \phi_1, \phi_2 \rangle \cong E(9)$ and the quaternion group $Q = \langle \theta, \lambda \rangle$. Moreover Q is the stabilizer of a point. As

$(M_{10})_0$ is sharply 2-transitive, stabilizers of different points intersect only in the identity. This shows that there are $9 \cdot 7 = 63$ nonidentity elements fixing one point each. Thus E consists of the identity and the eight fixed-point-free elements. These are of order three. Let $\sigma \in (M_{10})_0$ be the involution fixing a and let σ afford the operation $(a)(b,c)$. Let $\tau \in (M_{10})_0$ be the involution fixing b. We have to show that τ affords the operation $(b)(a,c)$. Assume this is not the case, so that τ maps $\tau = (b)(a,d)\dots$. Choose e such that $\sigma = (a)(b,c)(d,e)\dots$ As the factor group $(M_{10})_0/E$ has only one involution we conclude that $\sigma\tau \in E$. It follows that $\sigma\tau$ is fixed-point-free of order three. As $\sigma\tau$ affords the operation $e \mapsto a \mapsto d$ it follows that $d \mapsto e$. This shows that τ must fix e. This is impossible as τ has only one fixed point.
We have proved our claim. It follows that for any block B the length of its orbit under the action of M_{12} is $|M_{12}|/6! = 132$. The total number of blocks is $\binom{12}{4} \cdot 4/15 = 132$. We conclude that M_{12} is transitive on the blocks. It follows from Theorem 5.15 that this defines a 5-design with $\lambda = 1$. We have seen the following:

C.1 Theorem (small Witt design). *Consider the sharply 5-transitive action of M_{12} on the 12-set Ω. Define a 6-set B to be a block if there is an involution in M_{12}, which stabilizes B as a set and has four fixed points in B. There are 132 blocks. The set-stabilizer is $(M_{12})_B \cong S_6$. Further M_{12} is transitive on the blocks and these blocks define a Steiner 5-design $S(5,6,12)$.*

Bibliography

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

[2] W.O.Alltop: *An infinite class of 4-designs,* Journal of Combinatorial *Theory* **6** (1969),320-322.

[3] T.Beth, D.Jungnickel and H.Lenz, *Design Theory,* Cambridge Univ. Press 1986, ^{2}2000.

[4] J.Bierbrauer, *A new family of 4-designs,* Graphs and Combinatorics **11** (1995),209-211.

[5] N.L. Biggs, White, *Permutation groups and combinatorial structures,* Cambridge University Press 1979.

[6] N.G. de Bruijn, *Pólyas Abzähl-Theorie: Muster für Graphen und chemische Verbindungen,* Selecta Mathematica *III* 1-26 (K. Jakobs, ed), Springer 1971.

[7] J.Dieudonné, *La géométrie des groupes classiques,* Springer 1963.

[8] *The CRC Handbook of Combinatorial Designs (C.J.Colbourn and J.H.Dinitz,eds),* CRC Press 1996.

[9] B.Huppert, *Endliche Gruppen I,* Springer 1967.

[10] B.Huppert and N.Blackburn, *Finite Groups II* and *Finite Groups III,* Springer 1982.

[11] D. Hughes, F. Piper, *Design Theory,* Cambridge University Press 1985.

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

[13] A. Kerber, Bayreuther Mathematische Schriften **12**(1983),**15** (1983),**21**(1986).

[14] A. Kerber, *Algebraic Combinatorics via Finite Group Actions,* BI Mannheim.

[15] Moore, *Tactical Memoranda, American Journal of Mathematics* **18** (1896), 268-275.

[16] Netto, *Lehrbuch der Kombinatorik*, ^{2}1927, with notes by Skolem in the appendix.

[17] D.S.Passman, *Permutation Groups,* Benjamin 1968.

[18] G. Pólya, *Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen, Acta Mathematika* **68** (1937), 145-254.

[19] M.Suzuki, *Group Theory I,* Springer 1982.

[20] M.Suzuki, *Group Theory II,* Springer 1986.

[21] H.Wielandt, *Finite Permutation Groups,* Academic Press 1964.

[22] E. Witt, *Über Steinersche Systeme, Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg* **12**(1938),265-275.

[23] Richard M. Wilson, *Some partitions of all triples into Steiner triple systems,* Proceedings of the Hypergraph Seminar, Ohio State University 1972, *Lecture Notes in Mathematics* **411** (C. Berge, Ray-Chaudhury, eds) 1974, 267-277.