Group Theory and Applications
Gruppentheorie und Anwendungen

Jürgen Bierbrauer

December 15, 2005

Contents

Part I

Introduction to Group Theory

Chapter 1

Groups and symmetries

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***), the letter e probably stands for Einheit) 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 $ee' = e = e'$). The letter e probably stands for *Einheit.* We also write the neutral element as 1. The following **cancellation laws** 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 $x = y$.*

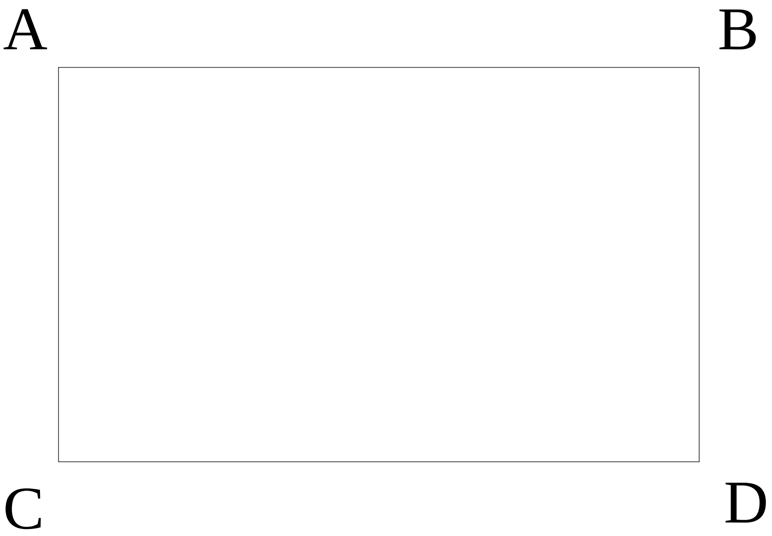


Figure 1.1: The rectangular playing card

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

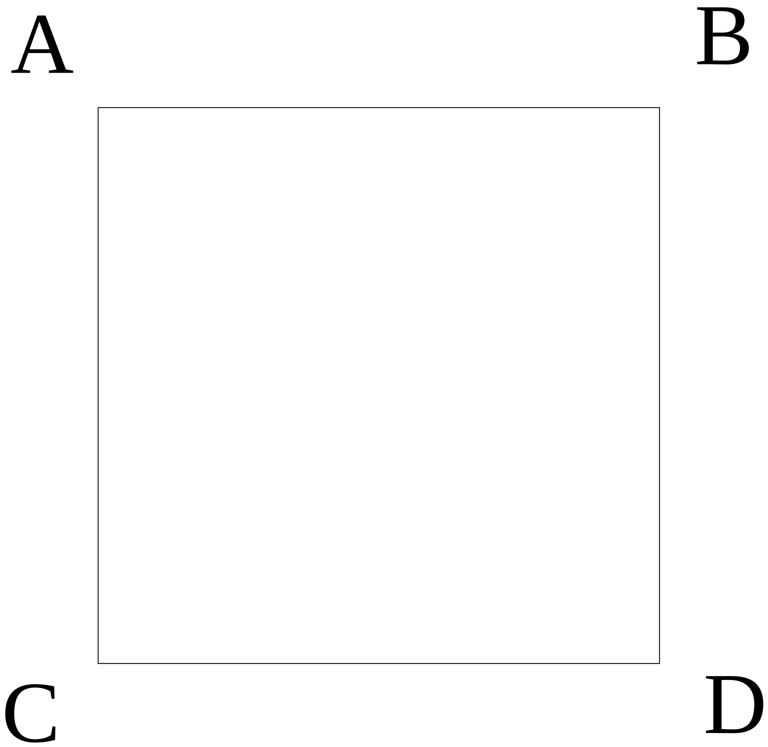


Figure 1.2: The quadratic playing card

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 $4 \times 2 = 8$ 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 :

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

The set of symmetries of any algebraic, geometric or combinatorial structure can always be expected to form a group. A symmetry is defined as a permutation of the ground set which respects the given structure. In these cases, when the elements of the group are defined as mappings, the group operation is always defined as composition of functions. This shows that associativity is satisfied. The neutral element e is the lazy permutation, and the inverse is the inverse. We see that the group axioms of Definition 1.1 are automatically satisfied. In general, when the group operation is defined in some indirect way, it may be quite laborious to check associativity.

In the case of the rectangular playing card the ground set consisted of the vertices A, B, C, D and the structure to be respected was defined on pairs of vertices (long edges, short edges, non-edges). Another example of a combinatorial structure will be given in Section 1.5.

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 simply 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 Quasigroups and latin squares

What if instead of the group axioms we demand only the cancellation laws of Theorem 1.2 to hold?

1.9 Definition. *Let G with a product operation $: G \times G \longrightarrow G.$ be defined. Then $(G,\cdot)$ is a* **quasigroup** *if the following hold for all $a, x, y \in G$:*

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

If $|G| = n$, the corresponding multiplication table (we may call it a quasigroup table) is an (n,n)-array with entries from G. The defining property of a quasigroup means that each row and each column of the matrix is a permutation: each element of G appears once in each row and once in each column. Such arrays are widely known as **Latin squares.** We see that Latin squares are equivalent with quasigroups. It is by now obvious how symmetries of quasigroups are defined:

1.10 Definition. *Let G be a quasigroup. A permutation σ of G is a symmetry of G if the following always holds:*

$$\sigma(x)\sigma(y) = \sigma(xy).$$

In words: the product (in the quasigroup) of the images under σ equals the image of the product. We convinced ourselves in Section 1.2 that in these cases the set of all symmetries forms a group, the symmetry group (also known as **automorphism group**).

As an example consider the quasigroup $G = \{e, a, b, c\}$ with table

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

which we recognize simply as the group table of the group V. What is its group of symmetries. Let σ be such a symmetry. Is e is the square of each element of G it must be fixed under σ. We leave it as an exercise to show that each permutation of $\{a, b, c\}$ is a symmetry of our "quasi"group. For example, consider $\sigma = (a, b, c)$. Reorder the rows and columns of the table accordingly:

permuted table				
	e	b	c	a
e	e	b	c	a
b	b	e	a	c
c	c	a	e	b
a	a	c	b	e

We have to check that the entries of this permuted table are precisely the images under σ of the original table. This is the case. We have seen that σ is indeed a symmetry.

Exercises

1. Prove that in any group $(ab)^{-1} = b^{-1}a^{-1}$ always holds.

2. How do you read off from the quasigroup table of G if G is commutative?

3. Consider the quasigroup $Z = \{e, z, a, b\}$ with the following table:

table of Z				
	e	z	a	b
e	e	z	a	b
z	z	e	b	a
a	a	b	z	e
b	b	a	e	z

   Determine the group of symmetries of Z.

4. Write out the group table of a non-abelian group of order 6.

Chapter 2

Subgroups and cosets

2.1 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 rather obvious.

2.1 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:

2.2 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:

2.3 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 2.3 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:

2.4 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 2.4 explains why we used the notion of **order** with apparently different meanings. We see that the order of an element as in Definition 2.3 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.

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

2.2 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.

2.6 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.

2.7 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:

2.8 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. □

2.9 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 2.8 that $o(g)$ must divide $|G|$.

2.10 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 13.1).

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.

2.11 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.*

Exercises

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 the intersection of two subgroups is a subgroup.

Chapter 3

Some basic number theory

3.1 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. The set $\mathbb{Z}$ of all integers is a group in its own right, with respect to addition as group operation. The neutral element is 0, the inverse of n is $-n$. It also illustrates that the first requirement in the definition of a subgroup (Definition 2.1) is needed: the subgroup generated by $1 \in \mathbb{Z}$ is of course all of $\mathbb{Z}$. Using only non-negative "exponents" we obtain the natural numbers (including 0). The natural numbers are closed under addition but they do not form a group.

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.

3.1 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	$\cdot$	143	+ 52
143	=	2	$\cdot$	52	+ 39
52	=	1	$\cdot$	39	+ 13
39	=	3	$\cdot$	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 $u = 3, v = -19$.

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

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

3.3 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.

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

We will obtain a group-theoretic proof of Theorem 3.4 a little later, in Section 5.2. Theorem 3.4 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:

3.5 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.

3.2 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.

3.6 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

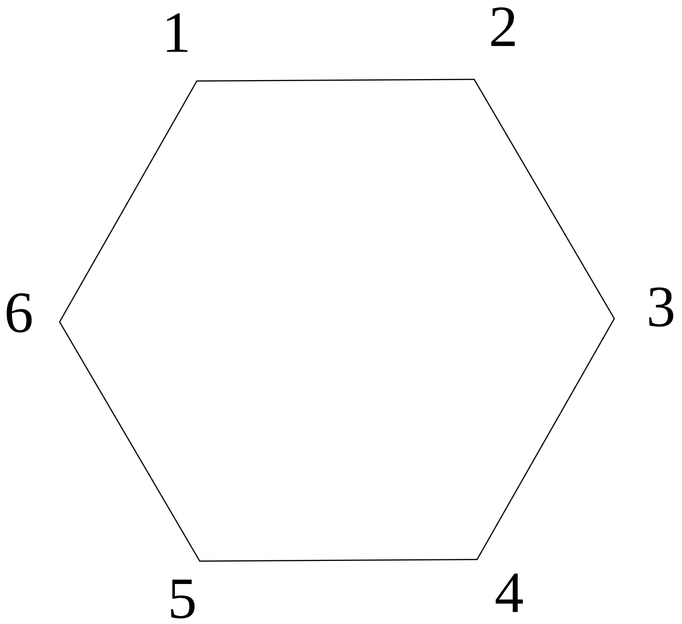


Figure 3.1: The regular hexagon

$1, 2, \ldots, n$ 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.

As an example consider the hexagon in Figure 3.2. Its group of symmetries consists of all permutations of $\{1, 2, 3, 4, 5, 6\}$ having the property that each pair of neighbouring points (joined by an edge) is mapped to a pair of neighbours. Clearly the permutation $g = (1, 2, 3, 4, 5, 6)$ is a symmetry (each edge is mapped to the next edge in clockwise direction), and so the cyclic group of order 6 generated by g is a subgroup of the symmetry group. However, reflection across the axis 14 is a symmetry as well. This is the permutation $(2, 6)(3, 5)$ and it is not contained in $\langle g \rangle$.

We will come back to the symmetries of an n-gon in Chapter 8.

Exercises

1. Prove the formula $\sum_{d|n} \phi(d) = n$.

2. Prove that $(2, 6)(3, 5)$ is not contained in the cyclic group generated by $(1, 2, 3, 4, 5, 6)$.

Chapter 4

Generators and isomorphisms

4.1 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 ($|S| = 1$).

4.2 Isomorphisms

We said earlier 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. A precise notion is needed to express this situation.

4.1 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 $f(g_1 g_2) = f(g_1) f(g_2)$.*

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:

4.2 Theorem. *Let $g \in G, o(g) = n$. The subgroup $\langle g \rangle$ of G as considered in Theorem 2.4 is isomorphic to the cyclic group Z_n.*

4.3 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 2.11.

Chapter 5

Direct products

5.1 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 $i = 0, 1, \dots, n-1$. 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 3.5). We conclude $j = n/gcd(i, n)$.

5.1 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 5.1 this is equivalent with $gcd(i, n) = 1$. Comparison with Definition 3.3 shows that the number of such elements is $\phi(n)$.

5.2 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 2.10). We have $o(g^i) = d$ if and only if $gcd(i, n) = n/d$ by Theorem 5.1. Write $i = \frac{n}{d} \cdot j$. The condition on j is $gcd(j, d) = 1$. We obtain the following generalization of Theorem 5.2:

5.3 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 $g^j \in \langle g^i \rangle$. □

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

We leave the proof as an exercise.

5.2 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:

5.5 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.

5.6 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 5.6 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 5.2) we see that Theorem 5.6 yields the promised group-theoretic proof of Theorem 3.4.

Exercises

1. Determine the number of generators of the cyclic group of order 3125.

2. Let g have order 165. Determine the order of g^{48}.

3. Prove that the symmetry group V from Theorem 1.3 is elementary-abelian.

4. 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 $lcm(n, m)$.

5. Prove Proposition 5.4.

Chapter 6

Factor groups and homomorphisms

6.1 Normal subgroups and factor groups

We turn to another point of our check list given in the beginning of Section 2.1, 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 2.2). 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:

6.1 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 6.1 says that for every $n \in N$ and $g \in G$ we have $g^{-1}ng \in N$.

6.2 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 6.1 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 2.9). 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.

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

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

6.4 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 3.2) 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.

6.2 Group homomorphisms

We defined group isomorphisms in Section 4.2. An important and natural generalization are homomorphisms.

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

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

The conditions in Definition 6.5 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 4.2).

6.6 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.

6.7 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, $f(g^{-1}kg) = f(g)^{-1}f(k)f(g) = f(g)^{-1}ef(g) = e$. $\square$

Theorem 6.7 often helps to prove that certain subgroups are normal. It suffices to find a group homomorphism, which has the subgroup as itskernel. The kernel determines if f is one-to-one (injective).

6.8 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.

6.9 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 6.8 that $\overline{f}$ is indeed an isomorphism. □

Exercises

1. Find a normal subgroup of the group D_8.
2. Find all normal subgroups of S_4.
3. Prove that the intersection of two normal subgroups is a normal subgroup.
4. Give an example showing that the image of a homomorphism is not in general a normal subgroup.
5. Show that the subgroups of order 2 in S_3 are not normal.

Chapter 7

Alternating groups, permutation representations

7.1 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.

7.1 Definition. *Let $\pi \in S_n$, where S_n acts on $\Omega = \{1, 2, \ldots, n\}$. 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. Observe that the number of inversions does not depend on the ordering of the symbols. This is an instance of a procedure which is often encountered in combinatorial theory: an arbitrary total ordering is imposed on the objects, but in the end the choice of this ordering turns out to be immaterial.

The essential combinatorial idea is in the following lemma:

7.2 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. $\square$

The same argument yields a stronger conclusion:

7.3 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:

7.4 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 7.3). 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.

7.5 Lemma. *We have*

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

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

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

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

In the language of Section 4.1 we would say that the transpositions are a set of generators of the symmetric group.

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.

7.7 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.

7.8 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 6.9).

7.9 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:

7.10 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:

7.11 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 9.3.

7.2 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 6.5) shows how this can be made precise:

7.12 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 6.9) 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.

7.13 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 6.7 that $V \lhd S_4$. By Theorem 6.9 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.

7.3 Orbits and the orbit lemma

7.14 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 $i \mapsto j$.*

7.15 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. $\square$

7.16 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 $Ker(\pi) = \{e\}$.*

7.17 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)

7.18 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 Exercises). The following easy theorem is extremely useful for many applications.

7.19 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 equals 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: $\pi(h) : i \mapsto i$. Conseqnently every element of the coset $G_i g$ maps i to the same element of the orbit. This shows already that the length of the orbit cannot exceed 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. $\square$

Exercises

1. Let n be an even number and g a fixedpointfree element of order 2 in S_n. Determine the signum of g.
2. Prove Proposition 7.18.

Chapter 8

Dihedral groups and graphs

8.1 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 7.19) 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 $g : 2 \longrightarrow n$. The continuation is uniquely determined: $g : 3 \longrightarrow n - 1, \ldots$. In our hexagonexample we have $g = (2, 6)(3, 5)$. Geometrically g is the reflexion across the line connecting 1 and 4. We have seen that $|H| = 2$ and conclude $|G| = 2n$.

8.1 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.**

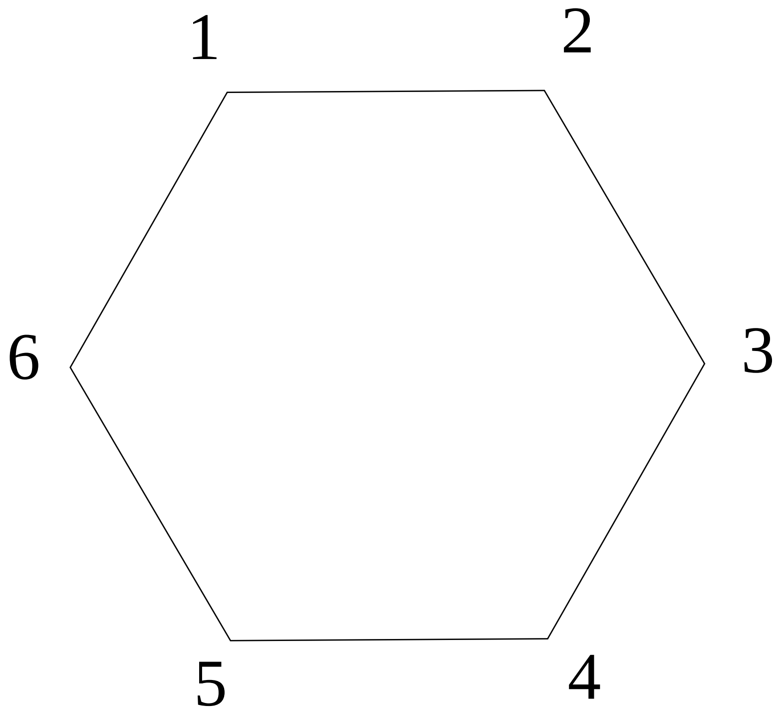


Figure 8.1: The regular hexagon

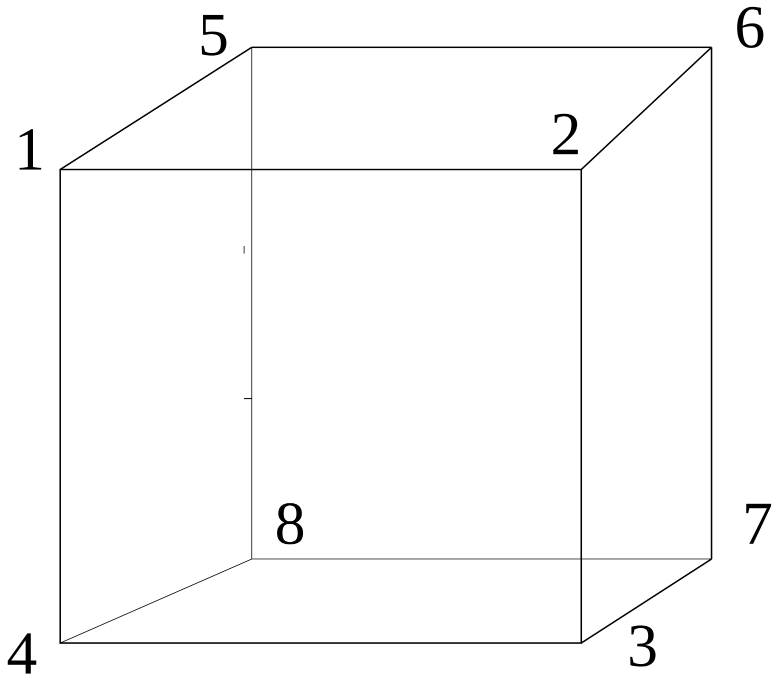


Figure 8.2: The cube

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

8.2 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.

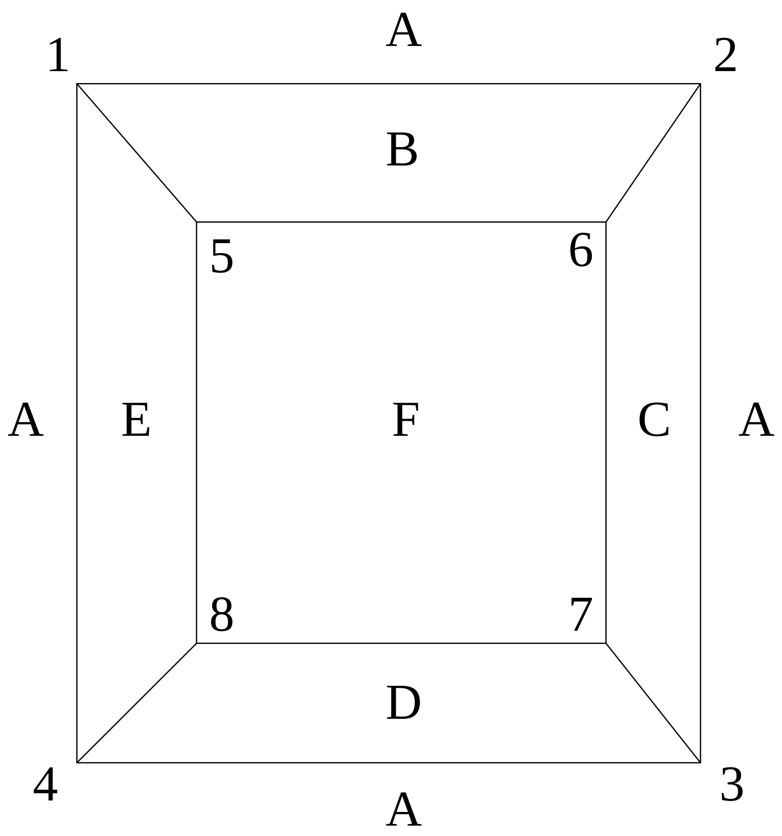


Figure 8.3: A flat version of the cube

8.2 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 7.19 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 8.1). 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 $|G| = 6 \cdot 8 = 48$. □

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 6.9 that G/K is isomorphic to a subgroup of S_4. As $|G/K| = 24 = |S_4|$ it follows $G/K \cong S_4$.

8.3 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.

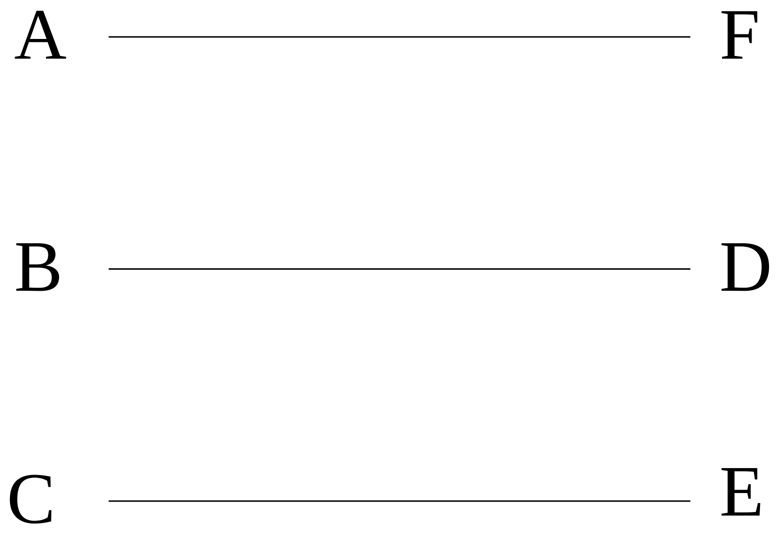


Figure 8.4: A graph related to the cube

8.4 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 8.1). 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 6.9 that the permutation representation of G on the faces yields an isomorphism between G and the automorphism group of the face-graph.

8.5 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 $(A, D, C)(B, E, F)$,

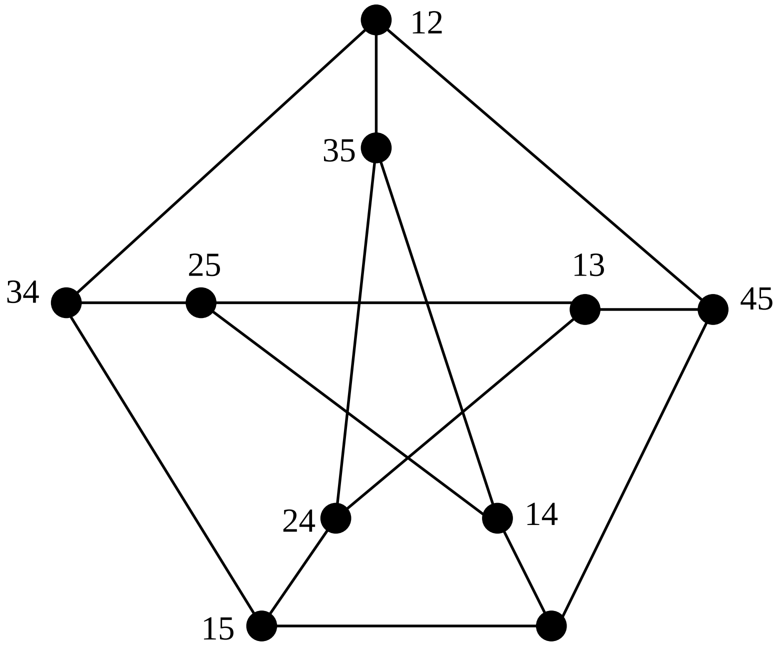


Figure 8.5: The Petersen graph

which clearly is a symmetry of the face-graph. The corresponding symmetry of the cube is $(1, 8, 6)(2, 4, 7)$.

The Petersen graph

Here is another famous graph, the Petersen graph P.

The determination of its symmetry group is greatly simplified when we recognize an algebraic structure behind it. Start from a ground set $\Omega = \{1, 2, 3, 4, 5\}$ and identify the vertices of our graph with the pairs of elements of Ω. Here we write 12 for $\{1, 2\}$, for example. A graph structure is obtained by defining two pairs ij and kl to form an edge if i, j, k, l are different. This is the Petersen graph. In the figure we have indicated such a labelling. Why does this simplify our task? Well, each permutation of Ω maps edges to edges, so S_5 certainly is a subgroup of $G = Aut(P)$. As S_5 is transitive on the 10 vertices, so is G. The same argument shows that the stabilizer of 12 induces the full S_3 on the set of its neighbours $\{34, 35, 45\}$. Also, the permutation $(1, 2)$ shows that the stabilizer of points $12, 34, 35, 45$ still acts transitively on the remaining neighbours $15, 25$ of 34. So far we know

$$|G| = 10 \times 3! \times 2 \times |K|,$$

where K is the subgroup of G consisting of the elements that fix each of $12, 34, 35, 45, 15, 25$. Now it is obvious that K is the identity group. It follows $|G| = 10 \cdot 6 \cdot 2 = 120$.

8.6 Theorem. *The automorphism group of the Petersen graph is S_5.*

Exercises

1. Show that D_{2n} is not abelian when $n > 2$.
2. Find an element of order 3 of the cube group and the corresponding symmetry of the face graph (see Section 8.2).
3. Determine the number of elements of order 3 in the cube group.
4. Let Γ be the graph on $2n$ vertices, which has n disjoint edges. Determine the order of its automorphism group.
5. Find the symmetry of the cube, which performs the permutation $(A, D)(B, F)(C, E)$ on the faces.
6. Prove that each element of the dihedral group D_{2n} outside the cyclic subgroup of order n is an involution.

Chapter 9

Finite fields and linear groups

9.1 Prime fields

9.1 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.

9.2 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 3.2 that there are integers b and w such that $ab + pw = 1$. This proves our claim. □

9.2 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.

9.3 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 $x^n = -a_{n-1}x^{n-1} - \cdots - a_1 x - a_0$, 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 3.1) 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:

9.4 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.

9.5 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 it is a consequence of the following lemma:

9.6 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: $(x+y)^p = x^p + y^p$. □

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

9.7 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:

9.8 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 $q-1$.

9.9 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 5.2 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 5.3 shows that it is impossible that our group has no elements of order $q-1$. The group is therefore cyclic. $\square$

9.10 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. $\square$

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 $\mathbb{F}_{q^n}$.

9.11 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 9.6, 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.

A standard textbook on finite fields is Lidl-Niederreiter [7].

9.3 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.

9.12 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 $det(A) \neq 0$.*

9.13 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.

9.14 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 $(q^n - 1)/(q - 1)$.

9.15 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.

9.16 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 9.9 that $Z \cong Z_{q-1}$.*

9.17 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:

9.18 Theorem.

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

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

9.19 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 5.4. $\square$

9.20 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 $GL_n(2) \cong S_3$. 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.

9.21 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.

Exercises

1. Determine the center of the quaternion group Q_8.
2. Show that $Q_8 \lhd SL(2,3)$.
3. Find a group of order 8 all of whose subgroups are normal. Is this true of all groups of order 8?

Chapter 10

Automorphisms, conjugation, characteristic subgroups

10.1 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.

10.1 Definition. *A group isomorphism $f : G \longrightarrow G$ is an* **automorphism** *of G (see also Section 4.2). 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.

10.2 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 6.1 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.

10.3 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. □

10.4 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.

10.2 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.

10.5 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 $G' \subseteq N$. $\square$

10.3 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 $g \in G$).

10.6 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:

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

In fact, conjugation by $g \in G$ maps the normal subgroup $K \trianglelefteq G$ to itself. It therefore induces an automorphism of K. However, this automorphism of K, while induced by an inner automorphism of G, need not be an inner automorphism of K. This is why we need the assumption that H be characteristic in K.

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.

Exercises

1. Show that the relation of being a characteristic subgroup is transitive.
2. Show that $\mathbb{Z}(G)$ is a characteristic subgroup of G.
3. Determine the order of $Aut(Z_n)$.

Chapter 11

Permutation representations on subsets

11.1 The semidirect product

The semidirect product is an important generalization of the direct product from Section 5.2.

11.1 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.

11.2 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 8.1. 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*

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

11.2 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:

11.3 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:

11.4 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:

11.5 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:

11.6 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 11.6:

11.7 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 10.4).

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 2.2). Finally we show that multiplication from the right is in principle sufficient to describe all transitive permutation representations.

11.8 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 7.19 that all the elements mapping $i \mapsto j$ form the coset Hg. This gives us the desired bijection. $\square$

Exercises

1. 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.

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

Chapter 12

Conjugacy classes

12.1 Conjugacy classes

12.1 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 11.7 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:

12.2 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:

12.3 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 12.3 that the m-cycles form one conjugate class.

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

We know from Section 1.4 that the cycle type is uniquely determined. Lemma 12.3 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:

12.5 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 12.3 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 $(2,2)$.

12.2 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 11.5) helps us to describe situations when AB is a subgroup.

12.6 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. $\square$

12.7 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 12.6, 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 10.1 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.

12.8 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 10.3). 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. $\square$

Consider the group $V \triangleleft S_4$. As V is (elementary) abelian, it has no inner automorphisms. Apply Theorem 12.8. 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 7.13 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.

Exercises

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

2. Prove that $S_3 \cong D_6$.

3. 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.

Chapter 13

The Sylow theorems

13.1 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 2.8): 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.

13.1 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.

13.2 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 11.7), 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. $\square$

13.3 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 13.2 (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. □

13.4 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:

13.5 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 $g \in \mathbb{N}_G(P)N = N\mathbb{N}_G(P)$. □

13.2 Proof of the Sylow theorems

13.6 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 $q = p^m, \Omega = \{(x_1, x_2, \ldots, x_q) | x_i \in G, x_1 x_2 \cdot \ldots x_q = e\}$. We have $|\Omega| = |G|^{q-1}$. If $x_1 x_2 \cdot \ldots x_q = e$ then also $x_2 x_3 \cdot \ldots x_q x_1 = e$. It follows that the cyclic permutation $(x_1, x_2, \ldots, x_q) \mapsto (x_2, \ldots, x_q, x_1)$ generates a p-group of permutations of Ω. The fixed points under this group are precisely the q-tupels $(a, a, \ldots, a)$, 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 13.3 that we are done. $\square$

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 $P \leq \mathbb{N}(Q)$. It follows from Theorem 12.6 that PQ is a group. As $PQ/Q \cong P/(P \cap Q)$ by Theorem 12.7 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 13.3 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 $[G : P] = [G : \mathbb{N}_G(P)][\mathbb{N}_G(P) : P]$. 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 $|\mathbb{N}_G(P)/P|$ is divisible by p. By Cauchy's theorem we can find a group of order p in $\mathbb{N}_G(P)/P$. 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.

Chapter 14

Simple groups, composition series

14.1 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.

14.1 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. Also, it follows from Theorem 13.2 that a p-group of order $> p$ cannot be simple.

In order to give a first glimpse of the Sylow theorems let us show that groups of orders 6 or 30 cannot be simple.

Let G be simple, $|G| = 6$. Choose $P \in Syl_3(G)$. If $\mathbb{N}_G(P) = G$, then P is a normal subgroup, contradiction. It follows $\mathbb{N}_G(P) = P$ and there are $6/3 = 2$ different Sylow-3-subgroups. It follows that G has 4 elements of order 3. It follows that G has precisely one involution, meaning that the Sylow-2-subgroups is normal subgroup, contradiction.

Let now $|G| = 30$ and $P \in Syl_5(G)$. As $|Syl_5(G)|$ is a divisor of 2×3 and also $\equiv 1 \pmod 5$, this cardinality must be 1 or 6. The former is excluded as P would be a normal subgroup. It follows that G has 6 Sylow-5-subgroups and $6 \times 4 = 24$ elements of order 5. The same argument applied to a Sylow-3-subgroup Q shows $\mathbb{N}_G(Q) = Q$. It follows that G has $10 \times 2 = 20$ elements of order 3. We have counted far more than 30 elements already, contradiction.

Are there any non-abelian simple groups?

14.2 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 12.5). 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 $\mathbb{C}(g) \nsubseteq A_5$, 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 $\in N$ and $|N|$ must divide 60. This is impossible. ☐

We can prove more:

14.3 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 Chapter 15. Likewise, the groups $PSL_n(q)$ are simple except for $PSL_2(2)$ and $PSL_2(3)$.

14.2 Composition series

14.4 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).*

14.5 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 14.4 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 12.7 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. □

14.3 Solvable and nilpotent groups

14.6 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 13.2 shows that p-groups are solvable.

14.7 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.*

Exercises

1. Show that there is no simple nonabelian group of order < 60.
2. Prove that all groups of order p^2 are abelian.
3. Determine the centralizer of an $n-$cycle in S_n.
4. Determine the structure of groups whose order is a product of two primes. Hint: Use the Sylow theorems, automorphism groups and the semidirect product.

Chapter 15

Permutation groups

Recall the notion of similarity of permutation representations as well as Theorem 11.8, which says that transitive permutation representations can be found inside the group. They correspond simply to subgroups.

15.1 Lemma. *Let (G, Ω) be a permutation group. Then the following hold:*

1. *If G has t orbits on Ω, then*

$$t|G| = \sum_{g \in G} |F(g)| \quad (\textbf{Burnside's Lemma})$$

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 $|G_x| = |G|/|\Delta|$. It follows $\sum_{x \in \Delta} |G_x| = |G|$. Claim 1. follows.
2. We know from part 1. that $r \cdot |G_x| = \sum_{g \in G_x} |F(g)|$. 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 11.3) 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.

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

15.3 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:

15.4 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 $\cap_{i=1}^{t-1} G_{x_i}$.*

15.5 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. □

15.6 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.*

15.7 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. □

15.8 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 11.8. □

15.9 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}.*

15.10 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.

15.11 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 $|\Delta| = [H : G_x]$. □

15.12 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. □

15.1 Normal subgroups and permutation representations

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

Proof. Let $|\Omega| = n$. We have $G_x \leq G_x N \leq G$. Because of primitivity we have either $G_x N = G$ or $G_x N = G_x$. Assume $G_x N = G_x$, 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 $G_x N = G$. As

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

we conclude that N is transitive on Ω. □

15.14 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 $x_i g = y_i, i = 1, 2, \ldots, t$.*
(G, Ω) *is* **regular** *if it is sharply 1-transitive, equivalent if (G, Ω) is transitive and $|G| = |\Omega|$.*

15.15 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 15.13 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. □

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

15.16 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 15.16 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:

15.17 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 15.16 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:

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

Proof. We have shown in Section 14.1 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 15.15 that A_n must contain a regular normal subgroup. By Theorem 15.17 this implies $t \leq 4$, hence $n = 6$. By Theorem 15.17 we get a contradiction even in case $n = 6$. $\square$

Exercises

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

Part II

Designs and Codes

Chapter 16

Block designs

16.1 Definition of designs

Block designs have their origin in statistics. The name is derived from the design of experiments. The most demanding variant is the following:

16.1 Definition (Steiner systems). *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* **Steiner t-design** *(or Steiner system) $S(t, k, n)$ if every t-subset $T \subset \Omega$ is contained in precisely one element of $\mathcal{B}$.*

The elements of $\mathcal{B}$ are known as the **blocks** of the design. In case $t = 2$ one speaks of **lines** instead of blocks, in case $t = 3$ it is natural to call the blocks **circles** for obvious reasons: the central axiom is that any 3 points determine exactly one circle. One speaks of circle geometries in this case. Here is an example, Figure 16.1. It depicts an $S(2, 3, 7)$, which is known as the **Fano plane.**

The labelling indicates how it can be constructed: start from a 3-dimensional vector space, the space $\mathbb{F}_2^3$ of triples, over $\mathbb{F}_2$. As points (elements of Ω) choose the set of 1-dimensional subspaces, as lines the 2-dimensional subspaces. Each 2-dimensional subspace has 3 points (so $k = 3$) and any two 1-dimensional subspace are contained in precisely one 2-dimensional subspace. We have indeed an $S(2, 3, 7)$.

There is an obvious relation between the number b of blocks and the number n of points in an $S(t, k, n)$: count the pairs (T, B) where T is a t-set, B is a block and $T \subset B$. Counting from left to tight we obtain $\binom{n}{t} \cdot 1$, starting

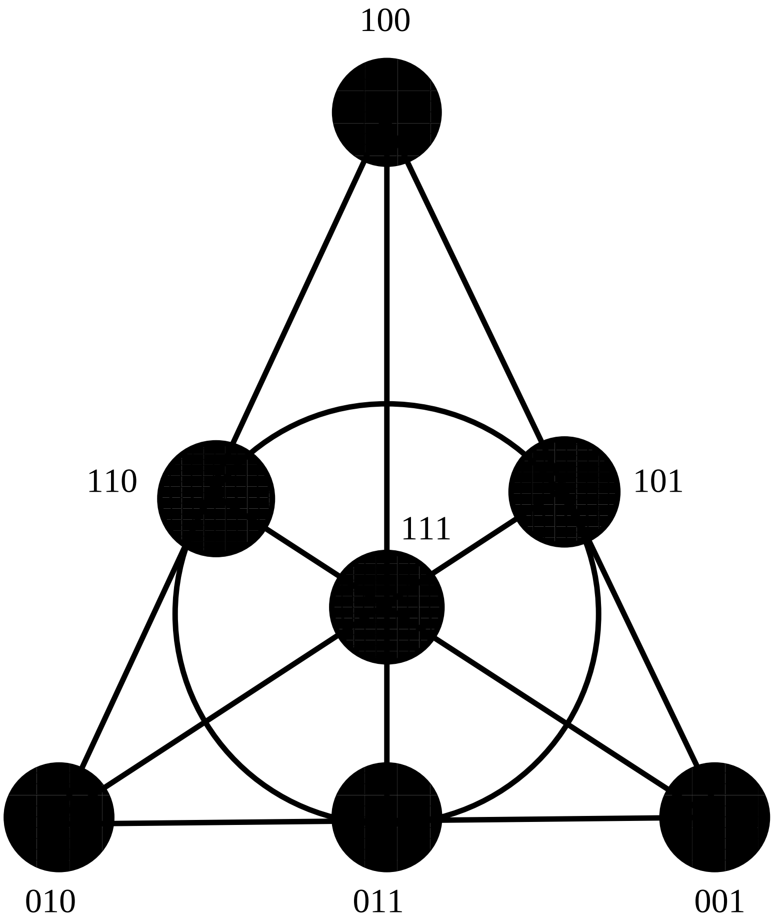


Figure 16.1: The Fano plane

from the right we count $b \cdot \binom{k}{t}$. This yields

$$b = \binom{n}{t} / \binom{k}{t}$$

for the number of blocks of an $S(t, k, n)$.

The difficulty of constructing Steiner t-designs grows with t. In fact, each $S(t, k, n)$ implies an $S(t-1, k-1, n-1)$ (see the Problems section). Steiner t-designs are hard to come by for $t > 3$. It is a sad fact that not a single Steiner t-design is known for $t > 5$. It is natural to relax the uniformity conditions in Definition 16.1 in the following way:

16.2 Definition (t-designs). *Let Ω be a set of cardinality n and $\mathcal{B}$ a family of k-subsets of Ω (blocks). The pair $(\Omega, \mathcal{B})$ is a (**simple**) t-**design** if every t-subset $T \subset \Omega$ is in exactly λ blocks. The parameters are denoted as*

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

The Steiner systems correspond to case $\lambda = 1$. The same argument as above shows that the number of blocks is

$$b = \lambda \binom{n}{t} / \binom{k}{t}. \tag{16.1}$$

A trivial structure is obtained 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 $t < k < n$.

The existence of non-complete simple t-designs for $t > 6$ has long been an open problem. The first 6-designs were found by Magliveras-Leavitt [8] in 1983. Teirlinck proved the existence of simple t-designs for all t [11, 12]. A general survey on designs and related structures is the *Handbook of Combinatorial Designs* [5].

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

16.3 Example. *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 $2 - (16, 6, 2)$.*

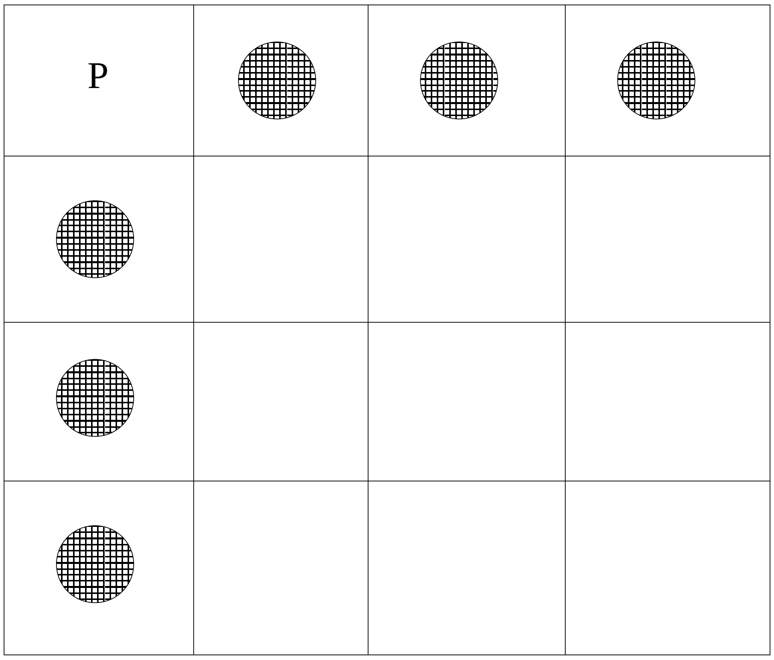


Figure 16.2: The biplane $2-(16,6,2)$

See Figure 16.1 where we depict the block corresponding to the point P in the Northeast corner.

A basic construction idea for groups were groups of symmetry. We agreed that the set of symmetries will always forma group, no matter which structure we start from. What is the automorphism group of a block design? This is clear by now.

16.4 Definition. *The automorphism group of a design $t-(n,k,\lambda)$ is the set of all permutations of points which map each block to a block.*

One of the exercises is to prove that $GL(3,2)$ is the full automorphism group of the Fano plane.

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:

16.5 Theorem. *The* 4*-subsets of an elementary abelian* 2*-group, whose elements sum to* 0 *form the blocks of a Steiner* 3*-design*

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

The smallest member $S(3, 4, 8)$ of this family implies $S(2, 3, 7)$, as we know. This is another construction of the Fano plane. Designs $S(3, 4, n)$ are known as **Steiner quadruple systems,** the $S(2, 3, n)$ are **Steiner triple systems.**

16.2 Projective geometries

Our original construction of the Fano plane generalizes in a natural way: start from an arbitrary finite field $\mathbb{F}_q$. Consider the space $V = \mathbb{F}_q^3$, a 3-dimensional space. Define

- **points:** the one-dimensional subspaces of V,
- **lines:** the two-dimensional subspaces of V.

As V has $q^3 - 1$ nonzero vector, and each 1-dimensional space has $q - 1$ nonzero vectors, the total number of points is $(q^3 - 1)/(q - 1) = q^2 + q + 1$. The same counting method shows that each line has $(q^2 - 1)/(q - 1) = q + 1$ points.

The most important property of this geometry is the following: any two different points are on precisely one common line. This fact is clear as any two 1-dimensional spaces generate a 2-dimensional space. We conclude that $PG(2, q)$, the classical projective plane of order q, is a Steiner design $S(2, q+1, q^2 + q + 1)$.

In general a design $S(2, n+1, n^2+n+1)$ is known as a **projective plane** of **order** n. The classical projective plane $PG(2, q)$ has order q. It is a famous problem to decide if projective planes of non-prime power orders exist. No example is known.

There is no reason to limit ourselves to 3-dimensional vector spaces: Let $V = V(k, q) = \mathbb{F}_q^k$ the space of k-tuples, a k-dimensional vector space over

$\mathbb{F}_q$. It makes sense, intuitively, to view the 1-dimensional subspaces of V as **points** and the 2-dimensional subspaces as **lines.** The main reason is the following: any two points are on precisely one common line. This is clear (two different 1-dimensional subspaces generate a 2-dimensional subspace) and it is a familiar axiom in geometry. In fact, this is the whole point: we give geometric names to the subspaces of the vector space V and use geometric intuition.

Observe the shift in dimension: we view 1-dimensional subspaces as points (0-dimensional geometric objects), 2-dimensional subspaces as lines (1-dimensional geometric objects) and so forth. Consequently the geometry derived from $V(k, q)$ is considered to be $(k-1)$-dimensional: $PG(k-1, q)$, the $(k-1)$-dimensional **projective geometry.** It has $k-1$ types of objects, from points (1-dimensional subspaces) to **hyperplanes** ($(k-1)$-dimensional vector subspaces). The most frequently used objects are points, lines, planes (3-dimensional subspaces) and hyperplanes.

A "geometric" reason why the number of points of $PG(2, q)$ must be $q^2 + q + 1$ is the following: fix a point P. It is on $q + 1$ lines. Each line contains q points different from P. In the resulting picture each point of $PG(2, q)$ shows up exactly once. We count $1 + (q + 1)q$ points.

The lowest-dimensional case of interest is the projective line $PG(1, q)$. It has $q + 1$ points (why? the number of 1-dimensional subspaces of a 2-dimensional space is $(q^2 - 1)/(q - 1) = q + 1$).

We wish to get some familiarity with $PG(k-1, q)$ in general. The enumeration of objects is just as easy as in the case of the projective plane. For example, the number of points is

$$(q^k - 1)/(q - 1) = q^{k-1} + q^{k-2} + \cdots + q + 1,$$

equal to the number of hyperplanes (there are $q^k - 1$ nonzero vectors in $V(k, q)$. Each such vector determines a point, but each point contains $q - 1$ nonzero vectors).

As an example consider $PG(3, 2)$. It has $2^4 - 1 = 15$ points and therefore also 15 planes. It is somewhat more interesting to count lines. As any two points determine a line we count 15×14 (the number of ordered pairs of different points), which counts each line 3×2 times (as a line has 3 points). The number of lines in $PG(3, 2)$ is therefore $15 \times 14/6 = 35$.

In the same manner the number of lines of $PG(3,q)$ can be determined. As there are $(q^4-1)/(q-1) = q^3+q^2+q+1$ points, the number of lines is

$$\frac{(q^3+q^2+q+1)\times(q^3+q^2+q)}{(q+1)q} = (q^2+1)(q^2+q+1).$$

Another way to count the lines of $PG(3,q)$ is the following: there are q^3+q^2+q+1 planes, each containing q^2+q+1 lines. The product $(q^3+q^2+q+1)(q^2+q+1)$ counts each line x times, where x is the number of planes through a given line. We have that x is the number of 3-dimensional subspaces of a 4-dimensional vector space, which contain a fixed 2-dimensional subspace. This is the same as the number of points on a line: $x = q+1$. The number of lines of $PG(3,q)$ is therefore $(q^3+q^2+q+1)(q^2+q+1)/(q+1) = (q^2+1)(q^2+q+1)$.

Fix a hyperplane H in $PG(k-1,q)$. The points of $PG(k-1,q)$ outside H are called **affine points** (with respect to H). They form the $(k-1)$-dimensional **affine geometry** $AG(k-1,q)$. The number of points in $AG(k-1,q)$ is q^{k-1}.

We are now confident it should be possible to solve each counting problem of this type whenever this is required.

We know that $GL(k,q)$ is a transitive permutation group on the nonzero vectors of V. It induces a 2-transitive permutation group on the 1-dimensional subspaces, the points of $PG(k-1,q)$. In 9.16 we saw that the kernel of this representation representation is precisely the group Z of scalar matrices. It follows that the projective general linear group $PGL(k,q)$ is an automorphism group of the projective space $PG(k-1,q)$. It is 2-transitive on the points.

16.3 Steiner triple systems

In this section we use a construction of Richard Wilson [16] 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 16.1 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 an 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.

16.6 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.**

16.7 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 $x,-2x,4x,-8x,16x,\dots$. 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

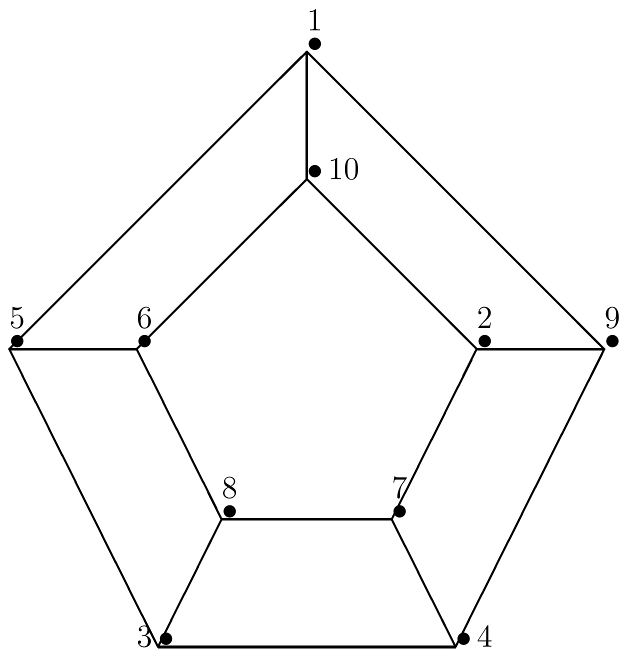
$\{x, y, a_i\}$ to be a block (type II).
Finally, $\{a_1, a_2, a_3\}$ is the only block of type 0. It is now easy to check that we have constructed a Steiner triple system. We have proved the following:

16.8 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 15 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

16.4 $PGL_2(q)$ and the projective line

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

16.9 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 15.3).

16.10 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 16.1 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

$$\lambda = \frac{|G|\binom{k}{t}}{|G_B|\binom{n}{t}} \tag{16.2}$$

The linear groups have been introduced in Section 9.3. Here we concentrate on $PGL(2,q)$. Its order is $(q+1)q(q-1)$. The order d of $Z \cap SL(2,q)$ is $gcd(2,q-1)$. It follows $PGL(2,q) = PSL(2,q)$ in characteristic 2 whereas $|PSL(2,q)| = (q+1)q(q-1)/2$ if q is odd. The canonical mapping $\pi : SL(2,q) \longrightarrow PGL(2,q)$ has $Z \cap SL(2,q)$ as kernel. It follows that we can view $PSL_2(q)$ as a normal subgroup of $PGL_2(q)$.

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.

16.11 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).*

Circle geometries

Next we construct a class of Steiner 3-designs on the projective line. We use Theorem 16.10 and in particular equation 16.2. So let $B \subset PG(1,q), |B| = k$. It follows from equation 16.2 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:

16.12 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 16.12 that the set-stabilizer of B in $PGL_2(Q)$ must be $PGL_2(q)$. We obtain a 3-design on $Q+1$ with $\lambda = \dfrac{k(k-1)(k-2)}{(q+1)q(q-1)} = 1$.

16.13 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 an $S(3,q+1,q^f+1)$. In particular we conclude that designs with these parameters exist for all prime-powers q and all natural numbers f.*

A class of 4-designs

We will use the groups $PGL_2(q)$ in characteristic 2 to construct families of 4-designs. As $PGL_2(q)$ is not 4-homogeneous on the projective line the simple method from Theorem 16.10 cannot be used. Our family 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 We collect some more information:

16.14 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. □

16.15 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 5. □

Let $S \subset PG(1, q)$ be a 4-subset. It follows from Corollary 16.12 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 $a \in \mathbb{F}_q \setminus \mathbb{F}_2$. The elements $\tau \longrightarrow a/\tau$ and $\tau \longrightarrow (\tau + a)/(\tau + 1)$ are involutions. They commute and stabilize S.

16.16 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 16.12 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.

16.17 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:

16.18 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 [2], where a simple construction is given of designs $4 - (2^f + 1, 6, 10)$ for f odd.

Exercises

1. Show that the $S(2, 3, 7)$ is essentially uniquely determined.
2. Determine the order of the group $GL(3, 2)$.
3. Show that $GL(3, 2)$ is a group of automorphisms of the Fano plane.
4. Show that $GL(3, 2)$ is the full automorphism group of the Fano plane.

5. Describe an $S(2,4,13)$.

6. Prove the following: any two different lines of a projective plane of order n have precisely one point in common.

7. Prove the following: removing a line and all its points in a projective plane of order n produces a design $S(2,n,n^2)$. Those designs are known as **affine planes** of order n.

8. Prove that the existence of $S(t,k,n)$ implies the existence of $S(t-1,k-1,n-1)$.

9. Find a large subgroup of the automorphism group of the biplane $2-(16,6,2)$.

Chapter 17

Error-correcting codes

17.1 Basic concepts

The object of Coding Theory is the transmission of messages over noisy channels. Below is the standard picture visualizing the situation.

At first we need to understand what the elements of this picture mean: what is a **message,** a **channel,** what is **noise**?

If there are 8 possible messages to be sent, say, then we can represent each message as a bitstring of length 3, like 000 or 011 or 110. We will generally assume this has been done and define a **message** to be a bitstring.

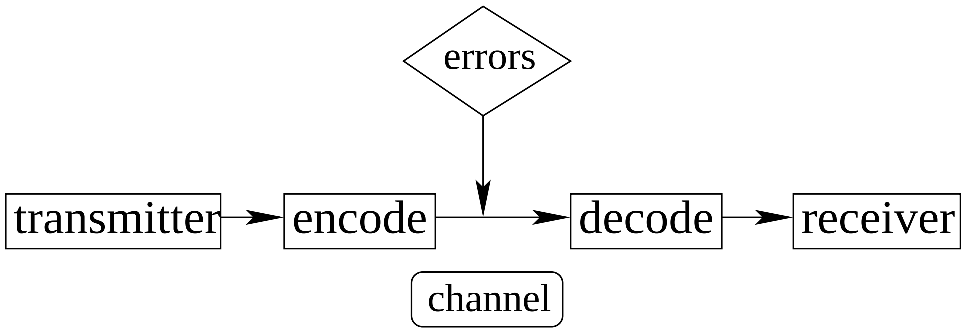


Figure 17.1: Information transmission over a noisy channel

Transmitting pictures from space

Assume we wish to transmit a photograph from outer space, like one of the pictures of Saturn taken by the Voyager spacecrafts in the early 1980s (*Viger* for Star Trek buffs). The picture is divided into 800×800 pixels, each pixel is assigned one of $256 = 2^8$ degrees of brightness. The brightness of a pixel is thus represented by a bitstring of length 8 and the total black and white picture consists of $800 \times 800 \times 8$ bits. As the picture really is in color, the same photo is transmitted three times, each time through a different color filter. The full color picture will thus be represented by a bitstring of length $3 \times 800 \times 800 \times 8 = 15,360,000$. This is our message. The channel is determined by the properties of space between the spacecraft and the receiver on Earth, above all by the Earth's atmosphere. A certain number of bits will be destroyed. Here we only consider errors of the type that 0 is transmitted and 1 is received or vice versa.

Back to the general model

Assume we wish to send one of 8 possible messages (the bitstrings of length 3), for example message 011. If it should happen along the way (in the channel) that the second bit is flipped (the second coordinate is in error), then 001 will be received.

In general the number of errors occurring in the channel is the number of coordinates where the message differs from what is received. This motivates the following definition:

17.1 Definition. *Let* $x = (x_1, x_2, \ldots, x_n)$ *and* $y = (y_1, y_2, \ldots, y_n)$ *in* $\mathbb{F}_q^n$. *The* **distance** *(or* **Hamming distance***) between* x *and* y *is*

$$d(x, y) = \text{number of coordinates } i \text{ where } x_i \neq y_i.$$

Expressed in the context of messages and errors $d(x, y)$ is the minimum number of errors transforming x into y. In fact, consider the second example above: $x = 00110$ and $y = 00101$ differ in the last two coordinates: $d(x, y) = 2$ and $x + 00011 = y$.

Things get even easier when we use the weight.

17.2 Definition. *The* **weight** $wt(x)$ *of* $x \in \mathbb{F}_q^n$ *is the number of nonzero coordinates in* x.

The weight of a string is its distance from the all-0 vector. If the all-0 string is sent and w errors occur during transmission, then the received message has weight w. If x is sent, e is the error vector and $y = x + e$ is received, then $d(x, y) = wt(e)$.

It is easy to see that the Hamming distance is a metric.

The basic idea is the following: instead of using all possible strings from $\mathbb{F}_q^n$ we restrict to a subset (the **codewords**) which has the property that any two have a relatively large Hamming weight. Another way of saying this is: any two codewords which are different are very different. If for example the distance between any two codewords is ≥ 3 then it needs 3 transmission errors to transform one into the other. Better yet: if the received vector y has distance 1 from some codeword x, then it is most likely that x was sent (an error in one coordinate being more probable than multiple errors). This principle of decoding (mapping received tuples to codewords) will therefore correct individual errors. It is known as **maximum likelihood decoding.** The selection of codewords is the **code.** Here is an example:

Let us send bitstrings of length 6. Instead of using all elements of $\mathbb{F}_2^6$ as (encoded) messages, we use only the following subset:

000000	001011
100110	101101
010101	011110
110011	111000

Any two different codewords are at distance ≥ 3. We say that 3 is the **minimum distance** of the code. Please check for yourself that this is true.

The next step is to restrict to codes which are linear subspaces, like in the example. This leads to the following fundamental definition:

17.3 Definition. *A (linear) $[n, k, d]_q$-code is a k-dimensional subspace of Hamming space $\mathbb{F}_q^n$ each of whose nonzero elements (codewords) has weight $\geq d$.*

The idea of error correction

Transmitter and receiver agree on the code to be used. Only codewords will be sent. If only one error occurs in the channel, then the received word will be in a ball of radius 1 around a codeword (in the Hamming metric). Assume

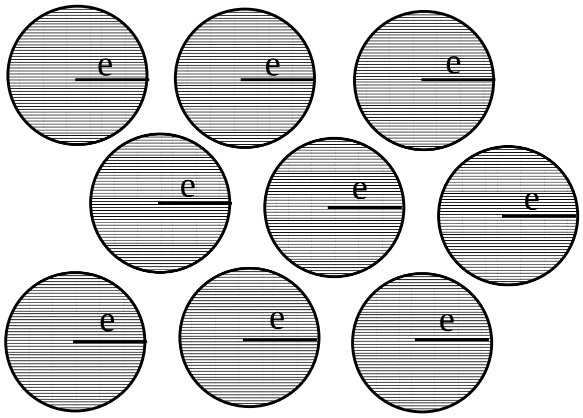


Figure 17.2: Non-overlapping balls centered at codewords

the code has been chosen such that any two codewords are at distance at least 3. Then the balls of radius 1 do not overlap: if a bitstring has distance 1 from some codeword, then it has larger distance from any other codeword. In other words, the receiver will decode any vector at distance ≤ 1 from some codeword as that codeword.

In the picture: the whole ball (or call it a disc) of radius 1 is decoded as the center of the ball, or: the received tuple is decoded as the codeword which it resembles most closely. If not more than 1 error occurred, then this error will be corrected. Observe that Figure 17.2 serves only as an illustration.

The metric in the Euclidean plane is used to illustrate the situation in a rather different metric, the Hamming metric.

17.2 The sphere-packing bound

A basic problem of coding theory is to find for which values of q, n (the length), k (the dimension) and d (minimum distance) a linear $[n, k, d]_q$-code exists. For q, n, d fixed we wish to maximize k. As all mathematical optimization problems, this splits in two parts: we have to construct good codes (with high k), and we have to prove upper bounds showing that a higher value of k is impossible. Here is an obvious bound:

Given a vector $x \in \mathbb{F}_q^n$, how many vectors are there at distance $\leq i$ from x? We call this set of vectors the **ball of radius** i with center x.

17.4 Definition. *The number of vectors at distance $\leq i$ from a given vector in $\mathbb{F}_q^n$ is denoted $V_q(i,n)$. We call $V_q(i,n)$ the* **volume** *of a ball of radius i.*

Clearly

$$V_q(i,n) = \sum_{j=0}^{i} \binom{n}{j} (q-1)^j.$$

Let $\mathcal{C}$ be a an $[n,k,d]_q$-code. Let $e = \lfloor (d-1)/2 \rfloor$ (the largest integer less or equal $(d-1)/2$). We have chosen e such that $2e+1 < d$. Our standard argument shows that the balls of radius e centered at the codewords must be disjoint. As each such ball has $V_q(e,n)$ vectors, we must have $q^k V_q(e,n) \leq q^n$ (counting all vectors in these balls we cannot get more vectors than the whole space contains).

17.5 Theorem (sphere packing bound). *Each $[n,k,d]_q$-code satisfies*

$$q^{n-k} \geq V_q(e,n).$$

Here $e = \lfloor (d-1)/2 \rfloor$.

Codes for which equality holds in Theorem 17.5 are known as **perfect codes.** The parameters of perfect codes have all been classified.

Here is a nice parameter situation: consider a possible code $[11,6,5]_3$. We have $e = 2$ and $V_3(2,11) = 1 + 11 \cdot 2 + \binom{11}{2} \cdot 4 = 1 + 22 + 220 = 243 = 3^5$ (quite a coincidence). We see that these parameters are extremal. If such a code exists, then it is perfect. A perfect $[11,6,5]_3$-code does indeed exist. It is uniquely determined by its parameters and known as the **ternary Golay code,** named after the Swiss engineer who described it in 1949 (see Golay [6], reprinted in Berlekamp [1]).

17.3 Geometric description of codes

Let $\mathcal{C}$ be a linear $[n,k,d]_q$-code. A **generator matrix** is a (k,n)-matrix G whose rows form a basis of the code. Let G have entry a_{ij} in row i and column j. The idea is to consider the columns of G as generators of points in $PG(k-1,q)$. So let P_j be the point generated by $(a_{1j}, a_{2j}, \ldots, a_{kj})$, where $j = 1,2,\ldots,n$. Here we assume that there is no 0-column in G (if it were, the corresponding coordinate would be superfluous as we could puncture with respect to this coordinate and obtain an $[n-1, k, d]_q$-code). Consider the set $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$ of points in $PG(k-1, q)$. In fact $\mathcal{P}$ is not necessarily a set but rather a multiset of points as it can happen that more than one column of G yields the same point (different columns of G can be identical or scalar multiples of each other). As a multiset, each point P counted with its multiplicity $w(P)$, the number of columns of G that generate point P, $\mathcal{P}$ has cardinality n. These are two ways of expressing the same concept. Either we speak of a multiset of n points in $PG(k-1, q)$ or of a mapping w assigning a non-negative integer weight $w(P)$ to each point $P \in PG(k-1, q)$, such that $\sum\limits_P w(P) = n$.

It is the idea of the geometric description to read off the code parameters from the multiset $\mathcal{P}$ of points in $PG(k-1, q)$. The main theorem shows how to determine the weight distribution.

The codewords of $\mathcal{C}$ are the linear combinations of rows of the generator matrix G. Let the rows of G be $v_i = (a_{i1}, a_{i2}, \ldots, a_{in})$. Each codeword has the form $x = c_1v_1 + c_2v_2 + \cdots + c_kv_k$ and is uniquely determined by the tuple $c = (c_1, c_2, \ldots, c_k)$ of coefficients. Fix a coordinate j, indexed by point P_j. What does it mean that x has entry 0 in coordinate j? It means that

$$c_1a_{1j} + c_2a_{2j} + \cdots + c_ja_{kj} = 0.$$

However, this linear relation with the c_i as coefficients defines a hyperplane. In other words, we have $x_j = 0$ if and only if point P_j is contained in that hyperplane. It follows that $wt(x)$ equals the number of points from $\mathcal{P}$ which are **not** in this hyperplane. This is already the main theorem.

17.6 Theorem. *Let $\mathcal{C}$ be a linear $[n, k]_q$ code and $G = (a_{ij})$ a generator matrix, with notation as in the paragraph above and such that G has no 0-column. For each point $P \in PG(k-1, q)$ let $w(P)$ be the number of columns of G which define P ($\sum_P w(P) = n$).*

For each nonzero tuple $c = (c_1, c_2, \ldots, c_k) \in \mathbb{F}_q^k$ let $c^\perp$ be the hyperplane of $PG(k-1, q)$, which consists of all $y = (y_1, y_2, \ldots, y_k)$ such that $c \cdot y = 0$.

Then the weight of $x = c_1v_1 + c_2v_2 + \cdots + c_kv_k$ is

$$wt(x) = \sum_{P \notin c^\perp} w(P).$$

The v_i are the rows of G. In particular the minimum weight d is the minimal number of points from $\mathcal{P}$ outside a hyperplane (in the multiset sense).

It is harder to write down this theorem than to prove it. Even case $d = 0$ makes sense. This will be the case when all points from $\mathcal{P}$ are contained in a hyperplane, which is equivalent to the dimension of $\mathcal{C}$ being $< k$.

Observe that each linear code $\mathcal{C}$ can be described by point sets in many different ways. Each step of Gauß elimination (row operations) will produce a different point set without changing the code. The multiset $\mathcal{P}$ of points is unchanged not only under permutations of coordinates but also when columns are multiplied by nonzero scalars.

It is the charm of the geometric description of linear codes that it gives a completely different angle under which to view the construction problem. What we need are sets (or multisets) of points in projective geometry which are in some sense uniformly distributed: no hyperplane contains very many of our points, in other words: outside every hyperplane we always need to find sufficiently many points.

17.4 The ternary Golay code

It has been mentioned that a perfect code $[11, 6, 5]_3$ exists. Even better, there is a $[12, 6, 6]_3$-code (these parameters imply $[11, 6, 5]_3$, see the exercises). We illustrate the geometric method by starting from parameters $[12, 6, 6]_3$ and arriving at a construction for the code. Along the way we will find useful information about the code and its automorphism group.

Let $\mathcal{C}$ be a $[12, 6, 6]_3$-code and $\mathcal{Q}$ a corresponding multiset of 12 points in $PG(5, 3)$ which has the property that it intersects each hyperplane $PG(4, 3)$ in at most 6 points. Denote subspaces $PG(3, 3)$ as **solids.** An i-hyperplane is a hyperplane intersecting $\mathcal{Q}$ precisely in cardinality i.

17.7 Lemma. *Each solid intersects $\mathcal{Q}$ in at most 4 points. In the case of equality each hyperplane containing the solid is a 6-hyperplane.*

Proof. Let S be a solid. If it intersects $\mathcal{Q}$ in cardinality 6, we can find a hyperplane with a higher intersection cardinality (always in the multiset sense). Assume $|S \cap \mathcal{Q}| = 5$. As S is contained in four hyperplanes, the cardinality of $\mathcal{Q}$ is bounded by $5 + 4 = 9$, contradiction. The same counting argument shows that in the case of intersection cardinality 4 each hyperplane containing S must have 6 points of $\mathcal{Q}$. $\square$

Assume Q is not a set. A point of weight ≥ 2 is contained in a line of intersection cardinality ≥ 3 and so forth until we reach a solid with intersection cardinality ≥ 5, which is impossible by Lemma 17.7. So $\mathcal{Q}$ is a **set** of 12 points.

The same elementary counting argument shows that any 3 points of $\mathcal{Q}$ generate a plane, any 4 points generate a solid and any 5 points generate a hyperplane. In other words any 5 points of $\mathcal{Q}$ are in general position, meaning that vectors representing those points are linearly independent.

By Lemma 17.7 there are no 5-hyperplanes. Each hyperplane containing 5 points of $\mathcal{Q}$ meets $\mathcal{Q}$ in precisely 6 points. There are therefore precisely $\binom{12}{5}/6 = 132$ such 6-hyperplanes.

The situation can be expressed in terms of designs. If we use the intersections with 6-hyperplanes as blocks, a Steiner system $S(5,6,12)$ is obtained (see Definition 16.1). This design is known as the **small Witt design** (maybe we should wait until we know that the underlying code exists). Once the code is constructed we will at last have an example of a Steiner 5-design. This is about as good as it gets. No Steiner 6-design is known.

Write a generator matrix in the form $G = (I|P)$, where I is the $(6,6)$-unit matrix and P is a $(6,6)$-matrix. The points in $\mathcal{Q}$ are those generated by the columns of G.

It is helpful to use duality: consider the dot product (or Euclidean product) $x \cdot y = \sum_{i=1}^{12} x_i y_i$ on $\mathbb{F}_2^{12}$. Call vectors x, y **orthogonal** if $x \cdot y = 0$. As $\mathcal{C}$ has dimension 6, its dual $\mathcal{C}^\perp$ (consisting of all vectors which are orthogonal on all vectors of $\mathcal{C}$) has dimension $12 - 6 = 6$. The hyperplane defined by $x_1 = 0$ contains 5 of the points from the unit matrix. It follows that the intersection is $6:$ there is precisely one 0 in the second half of the first row. The same argument holds for all rows of G. In other words, each row of G has weight 6. Let $v_1, \ldots, v_6$ be the rows of G. We saw $v_i \cdot v_i = 6 = 0:$ each row of G is orthogonal to itself. Can we have two of the zeroes in P in the same column? The location of those zeroes defines a solid (given by two linear equations) which would contain 4 of the columns of the unit matrix plus another point. We know from Lemma 17.7 that this is impossible: the 6 zeroes in P are in different rows and in different columns. It follows that we can arrange the columns of P such that P has zeroes in the main diagonal, and all entries off the main diagonal are nonzero.

Write $v_i = (e_i|w_i)$, where w_i is the i-th row of P. The only way how $v_i + v_j$ as well as $v_i - v_j$ can have weight ≥ 6 is that both have weight $= 6$, equivalently: w_i and w_j agree in precisely 2 coordinates. Of the 4 coordinates where both w_i and w_j are nonzero, in two coordinates the entries are equal, in two they are different. This shows $w_i \cdot w_j = 0 = v_i \cdot v_j$. As we also have $v_i \cdot v_i = 0$, it follows that all words of $\mathcal{C}$ are orthogonal to one another: $\mathcal{C} \subseteq \mathcal{C}^\perp$. For dimensional reasons $\mathcal{C} = \mathcal{C}^\perp$: our code is self-dual. Different rows of P are orthogonal to each other, whereas $w_i \cdot w_i = 2$. This shows in particular that P is a non-singular matrix: $det(P) \neq 0$, equivalently: the rows of P are linearly independent.

We show now that P can be brought in a special form when we use the following operations on G :

- Row operations on G (change of basis of $\mathcal{C}$),
- permutations of columns of G,
- multiplication of columns by constants ± 1.

The justification is that those operations are guaranteed not to change the properties of the code we are looking for. Row operations do not change the code at all. The others form a group, the **monomial group,** of order $2^{12}12!$ As columns of P are determined only up to scalar multiples we can choose $w_1 = (0, 1, 1, 1, 1, 1)$. By changing the sign of one or several rows of P we can make sure the first column of P is $(0, 1, 1, 1, 1, 1)^t$. This will change some of the entries 1 on the diagonal of I into 2, but we can correct that by multiplying the corresponding columns by 2. So far we have

$$P = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & \pm 1 & \pm 1 & \pm 1 & \pm 1 \\ 1 & \pm 1 & 0 & \pm 1 & \pm 1 & \pm 1 \\ 1 & \pm 1 & \pm 1 & 0 & \pm 1 & \pm 1 \\ 1 & \pm 1 & \pm 1 & \pm 1 & 0 & \pm 1 \\ 1 & \pm 1 & \pm 1 & \pm 1 & \pm 1 & 0 \end{pmatrix}.$$

Because of orthogonality, w_2 has two entries 1 and two entries 2 in the last four coordinates. We can choose $w_2 = (1, 0, 1, 1, 2, 2)$ (eventually the last 4 columns have to be suitably permuted. This moves the 0 entries of those columns into undesired positions, which can be corrected by a suitable permutation of rows. The resulting permutation of the entries 1 in the first 6 columns can be corrected by another column permutation). Observe that each $w_i, i > 1$ has two entries 1 and two entries 2 in the last 5 coordinates. This suffices to show that the entries in column 2 of P are uniquely determined. We have $P = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 2 & 2 \\ 1 & 1 & 0 & \pm1 & \pm1 & \pm1 \\ 1 & 1 & \pm1 & 0 & \pm1 & \pm1 \\ 1 & 2 & \pm1 & \pm1 & 0 & \pm1 \\ 1 & 2 & \pm1 & \pm1 & \pm1 & 0 \end{pmatrix}$. The entries in the $(2,2)$-squares in the center and in the Southeast are uniquely determined as well: $P = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 2 & 2 \\ 1 & 1 & 0 & 2 & \pm1 & \pm1 \\ 1 & 1 & 2 & 0 & \pm1 & \pm1 \\ 1 & 2 & \pm1 & \pm1 & 0 & 1 \\ 1 & 2 & \pm1 & \pm1 & 1 & 0 \end{pmatrix}$.

Up to making the two last columns change places (and following the above procedure) we can choose $p_{35} = 1, p_{36} = 2$. The remaining entries of P are uniquely determined. We have

$$P = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 2 & 2 \\ 1 & 1 & 0 & 2 & 1 & 2 \\ 1 & 1 & 2 & 0 & 2 & 1 \\ 1 & 2 & 1 & 2 & 0 & 1 \\ 1 & 2 & 2 & 1 & 1 & 0 \end{pmatrix}.$$

Observe that matrix P is symmetric. The generator matrix is

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 2 & 2 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 2 & 1 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 2 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 1 & 2 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 2 & 2 & 1 & 1 & 0 \end{pmatrix}$$

Starting from matrix G it is easy to check that it generates a self-dual $[12,6,6]_3$-code. In fact, because of self-duality all weights are divisible by 3, so it suffices to exclude weight 3. Linear combinations involving more than 3 rows of G present no danger. As the rows of P are linearly independent, linear combinations with exactly 3 nonzero coefficients have weight > 3 as well. As the rows of G have weight 6 it suffices to show that $w_i + w_j$ and

$w_i - w_j$ have weight > 1 for $i \neq j$, which of course is true. It follows that G is a generator matrix of a self-dual $[12,6,6]_3$-code, the ternary Golay code $\mathcal{G}_{12}$.

The automorphism group of $\mathcal{G}_{12}$.

The discussion in the preceding subsection shows that there is up to monomial equivalence exactly one $[12,6,6]_3$-code. We can in fact determine its automorphism group. Recall that the notion of an automorphism group is always contingent upon the action of some larger group. In our case the larger group is the monomial group of order $2^{12}12!$ The reason is that it is the largest group we can think of having the property that the image of a code with the properties we are looking for will have those same properties. We saw that up to the action of this group the code is uniquely determined: the $[12,6,6]_3$-subcodes of $\mathbb{F}_3^{12}$ form one orbit under the monomial group. The automorphism group $Aut(\mathcal{G}_{12})$ is defined as the stabilizer of our code $\mathcal{G}_{12}$ under the action of the monomial group.

We need some more practice with monomial operations. Each element of the monomial group will be written $g = \pi m$, where π is a permutation of $\{1,2,\dots,12\}$ and $m = m(1,2,\dots,12) = (m_1,m_2,\dots,m_{12}) \in \{1,2\}^{12}$. Element g acts by at first permuting the columns of G according to π and then multiplying column i by m_i, for all i. An element g belongs to $Aut(\mathcal{G}_{12})$ if it stabilizes the ternary Golay code $\mathcal{G}_{12} = \langle v_1,v_2,v_3,v_4,v_5,v_6\rangle$, in other words if the image of v_i under g is contained in $\mathcal{G}_{12}$, for all $i = 1,\dots,6$.

What happens if π is the identity permutation? We leave it to the reader to verify that $m = (m_1,\dots,m_{12}) \in Aut(\mathcal{G}_{12})$ if and only if either all $m_i = 1$ or all $m_i = 2$. Denote the latter element by -1.

The columns of the generator matrix G generate the point set $\mathcal{Q} = \{Q_1,Q_2,\dots,Q_{12}\} \subset PG(5,3)$. Each element $g \in Aut(\mathcal{G}_{12})$ induces a permutation of $\mathcal{Q}$. This permutation is of course π, where $g = \pi m$.

17.8 Definition. *Let $Aut(\mathcal{G}_{12})$ be the stabilizer of the ternary Golay code $\mathcal{G}_{12}$ in the monomial group. Write $g = \pi m$ as above. Let*

$$M_{12} = \{\pi | g = \pi m \in Aut(\mathcal{G}_{12}) \text{ for some } m\}$$

the permutation group on $\{1,\dots,12\}$ (which we identify with the set $\mathcal{Q}$ of points in $PG(5,3)$ describing the columns of the generator matrix G) determined by $Aut(\mathcal{G}_{12})$. This subgroup $M_{12} \subset S_{12}$ of the symmetric group on 12 objects is known as the **Mathieu group** *on 12 symbols.*

As mentioned above, whenever $g = \pi m \in Aut(\mathcal{G}_{12})$ then $-g = \pi(-m)$ is the only other element of $Aut(\mathcal{G}_{12})$ with permutation π. The **orders,** the number of elements of these groups, are therefore related by $|Aut(\mathcal{G}_{12})| = 2 \times |M_{12}|$. In practice we can concentrate on the permutation part π and adapt m by setting $m_1 = 1$.

We already have a lot of information about these groups. Consider subsets of 6 coordinates. The 132 blocks of the Witt design $S(5, 6, 12)$ correspond to the 6-hyperplanes and to $(6, 6)$-submatrices of G which have rank 5 (hence determinant 0). The remaining $\binom{12}{6} - 132 = 12 \times 11 \times 6$ sets of 6 columns correspond to regular $(6, 6)$-submatrices of G, **information sets** of coordinates. Examples of such information sets are the first 6 and the last 6 coordinates. We have shown above that the generator matrix can be given a special form starting from any information set. This shows that M_{12} is transitive on information sets. By a basic principle of permutation groups we have that the order of M_{12} is $|M_{12}| = 12 \times 11 \times 6 \times |H|$, where H is the subgroup of M_{12} consisting of those elements that map the set $\{1, 2, 3, 4, 5, 6\}$ of coordinates into itself. In order to determine the order of M_{12} it suffices to determine the order of H.

We have $h \in H$ if H permutes the points corresponding to the first 6 columns and also the points corresponding to the last 6 columns. The zeroes along the main diagonal of P show that the action of π on the last 6 coordinates is the same as on the first 6 : if $\pi : i \mapsto j$ where $i, j \leq 6$, then $\pi : 6 + i \mapsto 6 + j$. The elements $h_1 = (2, 3, 5, 6, 4)(8, 9, 11, 12, 10)$, and $h_2 = (2, 3)(4, 5)(8, 9)(10, 11)$ are both in H. The group $\langle h_1, h_2\rangle$ generated by h_1, h_2 has order 10. Another element of H fixing 1 is

$$h_3 = (3, 5, 4, 6)(9, 11, 10, 12)m(1, 2, 2, 2, 2, 2, 2, 1, 1, 1, 1, 1).$$

The group $\langle h_1, h_2, h_3\rangle$ has order 20. It is most important to find an element in H mapping 1 to a column $\neq 1$. An example for such an element is

$$h_4 = (1, 2)(5, 6)(7, 8)(11, 12)m(1, 1, 1, 1, 2, 2, 1, 1, 1, 1, 2, 2).$$

It maps $v_1 \leftrightarrow v_2, v_3 \mapsto v_3, v_4 \mapsto v_4, v_5 \leftrightarrow -v_6$.

Let us collect the information on M_{12} we have so far. As H is transitive on $\{1, 2, 3, 4, 5, 6\}$ and the stabilizer of 1 in H has order at least 20 it follows $|H| \geq 120$, consequently $|M_{12}| \geq 12 \times 11 \times 6 \times 120 = 12 \times 11 \times 10 \times 9 \times 8$.

On the other hand, consider the action of the permutation group M_{12} on the 5-tuples from $\{1, 2, \ldots, 12\}$. What is the stabilizer of the 5-tuple

$(1,2,3,4,5)$? As Q_6 is the sixth point in the hyperplane generated by $Q_1,\ldots,Q_5$, this point must be fixed as well. It follows that all points of $\mathcal{Q}$ must be fixed. The stabilizer is therefore ± 1 in $Aut(\mathcal{G}_{12})$, it is the identity in M_{12}. The length of the orbit of our 5-tuple therefore equals $|M_{12}|$, which therefore cannot exceed the number of all 5-tuples.

17.9 Theorem. *The permutation group M_{12} on 12 objects is 5-transitive. Its order is*

$$|M_{12}| = 12 \times 11 \times 10 \times 9 \times 8.$$

The Mathieu group is much older than the Witt design and the ternary Golay code. We have here a prime example for the interplay of group theory, coding theory and design theory. The Mathieu group M_{12}, the ternary Golay code and the small Witt design $S(5,6,12)$ are equivalent objects, but this statement has to be taken with a grain of salt. We saw how to construct the code in a canonical way from its parameters and how to obtain the design and the group. However, as we cannot operate with permutations alone, it is not all that easy to determine the group. Starting from the group, the design is immediate but the code poses a problem. One has to guess that one should use the field of 3 elements and to find the right ternary vectors. Starting from the design the group is immediate (it is the group of automorphisms of the design) but once again the code does not seem to be canonically determined from that point of view.

Let us collect the most important information obtained:

17.10 Theorem. *There is a $[12,6,6]_3$-code. It is self-dual and uniquely determined under the action of the monomial group. Its automorphism group (the stabilizer in the monomial group) has order $2 \times 12 \times 11 \times 10 \times 9 \times 8$. It induces a permutation group M_{12} on 12 objects, the* **small Mathieu group,** *which is 5-transitive of order $12 \times 11 \times 10 \times 9 \times 8$.*

Exercises

1. Show that the existence of an $[n,k,d]_q$ implies the existence of $[n-1,k-1,d]_q$ and $[n-1,k,d-1]_q$-codes.

2. How many $[12,6,6]_3$-codes are contained in $\mathbb{F}_3^{12}$?

Bibliography

[1] E. R. Berlekamp (ed.): Key Papers in the Development of Coding Theory, *IEEE Press,* New York 1974.

[2] J.Bierbrauer: *A new family of* 4*-designs, Graphs and Combinatorics* **11** (1995), 209-211.

[3] J. Bierbrauer: *Introduction to Coding Theory, Chapman and Hall, CRC Press* 2004.

[4] P. J. Cameron and J. H. van Lint: *Designs, Graphs, Codes and their Links, Cambridge University Press* 1991.

[5] C. J. Colbourn and J. H. Dinitz (eds.):
The CRC Handbook of Combinatorial Designs, CRC Press 1996.

[6] M. J. E. Golay: *Notes on Digital Coding,*
Proceedings of the IRE, June 1949.

[7] R. Lidl and H. Niederreiter: *Introduction to finite fields and their applications, Cambridge University Press* ^{1}*1986, revised edition 1994.*

[8] S. S. Magliveras and D. W. Leavitt: *Simple six designs exist, Proc. 14th Southeastern Conference on Combinatorics, Graph Theory, Computing, Congressus Numerantium* **40** (1983), 195-205.

[9] E. Mathieu: *Sur les fonctions cinq fois transitives de* 24 *quantités,* Journal Math. Pures et Appliquées **6** (1861), 241-243.

[10] E. Mathieu: *Mémoire sur l'étude des fonctions de plusieurs quantités, Journal Math. Pures et Appl.* **18** (1873), 25-46.

[11] L. Teirlinck: *Non-trivial t-designs without repeated blocks exist for all t*, Discrete Mathematics **65** (1987), 301-311.

[12] L. Teirlinck: *Locally trivial t-designs and t-designs without repeated blocks,* Discrete Mathematics **77** (1989), 345-356.

[13] T. M. Thompson: *From error-correcting codes through sphere packings to simple groups,* The Mathematical Association of America, Washington DC, 1983.

[14] E. Witt: *Die 5-fach transitiven Gruppen von Mathieu, Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg* **12** (1938), 256-264.

[15] E. Witt: *Über Steinersche Systeme, Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg* **12** (1938), 265-274.

[16] 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.