Introduction to Group Theory
Lecture Notes for MA 462

Jürgen Bierbrauer

February 8, 1999

Contents

Chapter 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:*

- $g_1(g_2 g_3) = (g_1 g_2) g_3$ *for all* $g_i \in G$ *(***associativity***).*
- *There is an element $e \in G$ (the* **neutral element***) such that $eg = ge = g$ for all $g \in G$.*
- *For every $g \in G$ there is an element $g^{-1} \in G$ (the* **inverse element***) such that $gg^{-1} = g^{-1}g = e$.*

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

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

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

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. □

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.

Chapter 2

Groups of symmetry

As a toy example consider the 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

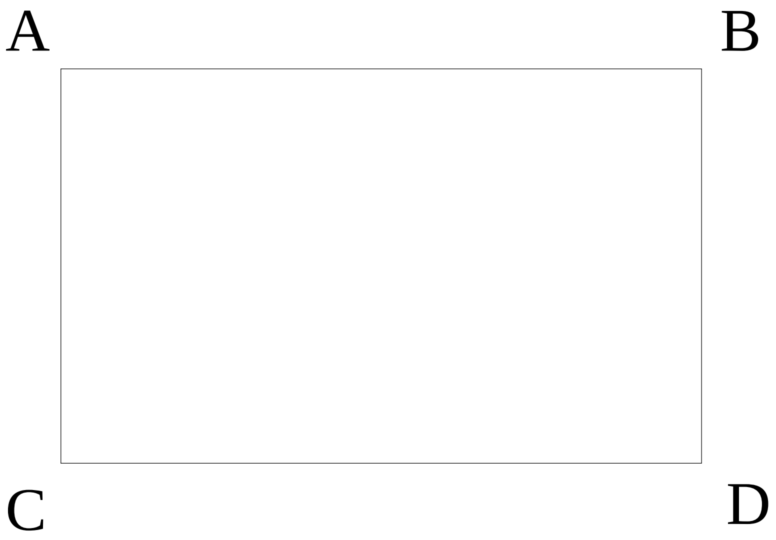

Figure 2.1: The rectangular playing card

(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.

2.1. 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}

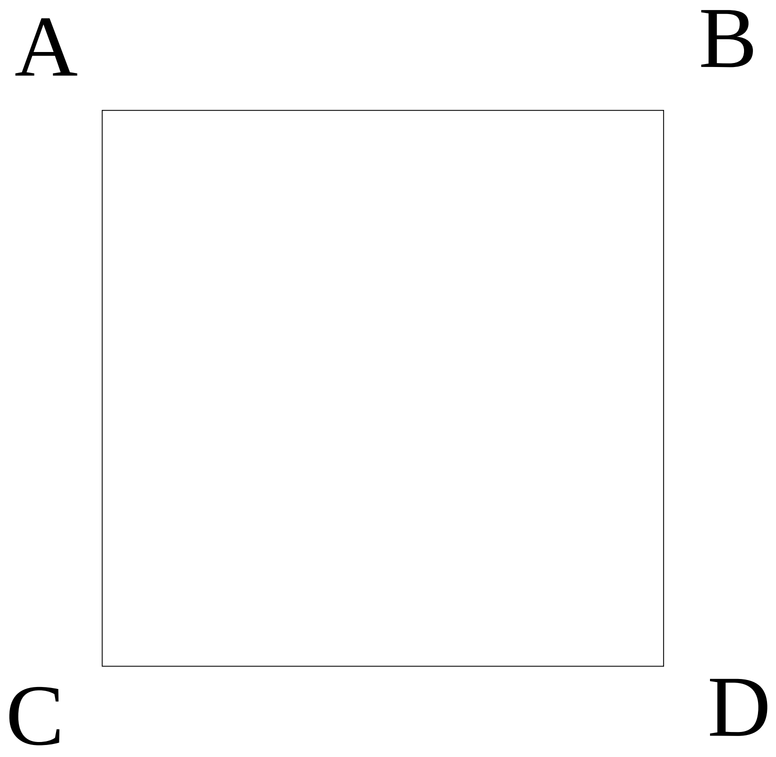

Figure 2.2: The quadratic playing card

of permutation (symmetry) f is the inverse mapping.

2.2. 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 2.1 is contained in the symmetry group of the quadratic card. Is that all? No, here is 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 2.2. 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 fact, we can check that if we know the image of A there are at most two symmetries achieving that. An upper bound on the number of symmetries is therefore $4 \cdot 2 = 8$ and we have already eight symmetries. In later chapters we will learn more efficient and secure ways to determine symmetry groups.

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

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

Chapter 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 2.1:

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.

Chapter 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.

4.1. Definition (symmetric group). *Let Ω be 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

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

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 $c = (A, D)(B, C)$.

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

$$a_1 \mapsto a_2 \mapsto a_3 \mapsto \cdots \mapsto a_n \mapsto a_1$$

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

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

4.3. 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

Chapter 5

Subgroups

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

5.1. 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 Chapter 2 are clearly subgroups of each other: $V < D_8$. This also shows in the group table of D_8 as given in Chapter 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:

5.2. 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:

5.3. 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. Let us make sure the Definition 5.3 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:

5.4. 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 5.4 explains why we used the notion of **order** with apparently different meanings. We see that the order of an element as in Definition 5.3 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.

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

Chapter 6

Cosets and Lagrange's theorem

In this chapter 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.

6.1. 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.

6.2. 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:

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

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

6.4. 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 Chapter 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 chapter that the order of an element $g \in G$ also is the order of the subgroup generated by g. It follows from Theorem 6.3 that $o(g)$ must divide $|G|$.

6.5. 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 (Chapter 25).

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.

6.6. 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.*

Chapter 7

Divisors and the Euclidean algorithm

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

7.1. 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 example: $gcd(7, 21) = 7, gcd(16, 24) = 8, gcd(100, 37) = 1$. The **Euclidean algorithm** is an efficient method to compute the gcd of two given numbers. 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 a and b. 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 $u = 3, v = -19$.

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

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

7.3. 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.

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

We will obtain a group-theoretic proof of Theorem 7.4 a little later, in Chapter 11. Theorem 7.4 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:

7.5. Theorem.

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

Chapter 8

Congruences and the cyclic groups

Let n be a natural number. When we calculate mod n we treat n as 0 and we identify any two integers if their difference is a multiple of n. $\mathbb{Z}/n\mathbb{Z}$ has only n objects, which we may identify with the n possible remainders when an integer is divided by n (long division). If that case we write $a \equiv b(\mod n)$, which simply means that $n \mid (a-b)$. Addition and multiplication in $\mathbb{Z}/n\mathbb{Z}$ is inherited from the integers. We just read the result mod n. Observe that there are precisely n classes mod n, in other words $|\mathbb{Z}/n\mathbb{Z}| = n$. Mod 2 we have just two classes (even and odd). If we write $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$ we have for example $1 + 1 = 2$ 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.

8.1. 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 chapter we will be more precise about what it means that two groups have the same structure and should be considered as the same group.

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

Chapter 9

Isomorphisms

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

9.1. 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:

9.2. Theorem. *Let $g \in G, o(g) = n$. The subgroup $\langle g \rangle$ of G as considered in Theorem 5.4 is isomorphic to the cyclic group Z_n.*

9.3. 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 6.6.

Chapter 10

Calculating in cyclic groups

A finite group is cyclic if it consists of the powers of one of its elements g. If $o(g) = n$, then the group is Z_n. Let us calculate the order of each element of the cyclic group $\langle g \rangle \cong Z_n$. An arbitrary element has the form g^i, where $i = 0, 1, \ldots, n-1$. By definition $o(g^i)$ is the smallest natural number j such that $(g^i)^j = g^{ij} = e$. The exponent ij 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 7.5). We conclude $j = n/gcd(i, n)$.

10.1. 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 10.1 this is equivalent with $gcd(i, n) = 1$. Comparison with Definition 7.3 shows that the number of such elements is $\phi(n)$.

10.2. 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 6.5). We have $o(g^i) = d$ if and only if $gcd(i, n) = n/d$ by Theorem 10.1. Write $i = \frac{n}{d} \cdot j$. The condition on j is $gcd(j, d) = 1$. We obtain the following generalization of Theorem 10.2:

10.3. 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. 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 $g^j \in \langle g^i \rangle$. □

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

We leave the proof as an exercise.

Chapter 11

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:

11.1. 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.

11.2. 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 11.2 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 10.2) we see that Theorem 11.2 yields the promised group-theoretic proof of Theorem 7.4.

Chapter 12

Normal subgroups and factor groups

We turn to another point of our check list given in the beginning of Chapter 5, factor groups. Let $H < G$. The idea is to define a group where multiplication is like in G but elements of H are treated as if they were the neutral element. As we talk about groups in general (not just abelian groups) we use right cosets, keeping in mind that we could have used left cosets just as well. So the elements of the factor group are the right cosets Ha. There are $[G : H]$ such cosets (see Chapter 6). We want to define the product of two right cosets as

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

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

12.1. 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 12.1 says that for every $n \in N$ and $g \in G$ we have $g^{-1}ng \in N$.

12.2. 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 12.1 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 6.4). 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.

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

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

12.4. 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 Chapter 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 groups also helps us to understand congruences (see Chapter 8) from a different perspective. The integers $\mathbb{Z}$ form an abelian group under addition. This is an infinite cyclic group. It has only two generators, 1 and its "inverse" -1 (recall that we use additive notation and that the neutral element is 0). In fact every integer is either a multiple ("power") of 1 (for example $4 = 1 + 1 + 1 + 1$) or a negative ("inverse") thereof. The set $n\mathbb{Z}$ of all multiples of n forms a subgroup. Our set of congruence classes $\mathbb{Z}/n\mathbb{Z}$ is simply the factor group in the sense of the present chapter.

Chapter 13

Group homomorphisms

We defined group isomorphisms in Chapter 9. An important and natural generalization are homomorphisms.

13.1. 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 13.1 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 Chapter 9).

13.2. 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.

13.3. 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 13.3 often helps to prove that certain subgroups are normal. It suffices to find a group homomorphism, which has the subgroup as its kernel. The kernel determines if f is one-to-one (injective).

13.4. 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 $f(g_1g_2^{-1}) = e$, hence $g_1g_2^{-1} \in Ker(f)$. We conclude $g_1g_2^{-1} = e$, hence $g_1 = g_2$. $\square$

We come to our next structural theorem.

13.5. 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 13.4 that $\overline{f}$ is indeed an isomorphism. $\square$

Chapter 14

The signum and alternating groups

We return to permutations and the symmetric group, which we left in Chapter 4. It will turn out that there are two types of permutations, which we will call even and odd, respectively.

14.1. 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. The essential combinatorial idea is in the following lemma:

14.2. 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:

14.3. 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:

14.4. 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 14.3). 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.

14.5. Lemma. *We have*

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

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

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

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

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

14.7. 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.

14.8. 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 13.5).

14.9. 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:

14.10. 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:

14.11. 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 Chapter 20.

Chapter 15

Permutation representations

We started out with groups of symmetries. These are groups consisting of a 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 13.1) shows how this is made precise:

15.1. 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 13.5) 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.

15.2. 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 13.3 that $V \lhd S_4$. By Theorem 13.5 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.

Chapter 16

Orbits and the orbit lemma

16.1. 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 $i \mapsto j$.*

16.2. 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. □

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

16.4. 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)

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

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

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

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

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

Proof. We have to establish a bijection between cosets of G_1 and elements of the orbit. Let $h \in G_1, g \in G$. Then

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

This follows from the definition of the stabilizer: $\pi(h) : i \mapsto i$. This shows that every element of the coset $G_1 g$ maps i to the same element element of the orbit. This shows already that the length of the orbit cannot be larger than the number of cosets. Assume now we have $g_1, g_2 \in G$ such that $i\pi(g_1) = i\pi(g_2)$. It follows $i = i\pi(g_1 g_2^{-1})$, equivalently $g_1 g_2^{-1} \in G_i$. We conclude that $g_1 \in G_i g_2$. This shows that elements mapping i to the same image must be in the same coset. $\square$

Chapter 17

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 Chapter 2. The symmetry group turned out to be D_8 in this case (see Theorem 2.3). 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 16.6) shows that $|G| = n \cdot |H|$, where $H = G_1$ is the stabilizer of point 1. It suffices to determine H. Let $g \in H$. Then g must permute the two neighbours 2 and n of 1. Assume g fixes 2. Then g must fix the unique new neighbour 3 of 2. Proceding in this fashion we see that $g = e$. The only other possibility is $g : 2 \leftrightarrow n$. The continuation is uniquely determined: $g : 3 \leftrightarrow n-1, \ldots$. In our hexagonexample we have $g = (2,6)(3,5)$. Geometrically g is the reflexion across the line connecting 1 and 4. We have seen that $|H| = 2$ and conclude $|G| = 2n$.

17.1. 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.**

It can be shown that every element in $D_{2n} \setminus Z_n$ has order 2 (see the Problems).

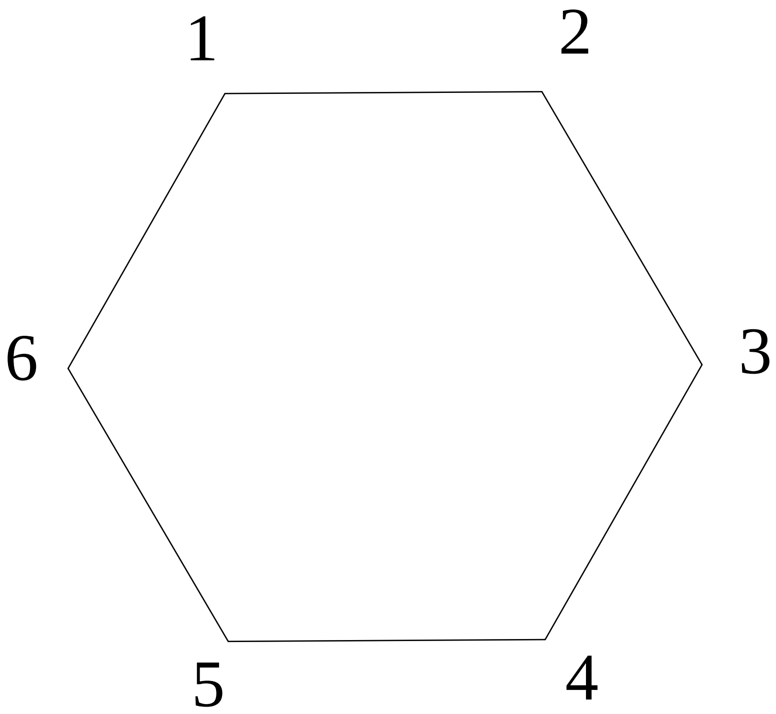

Figure 17.1: The regular hexagon

Chapter 18

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.

18.1. 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 16.6 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 17.1). 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

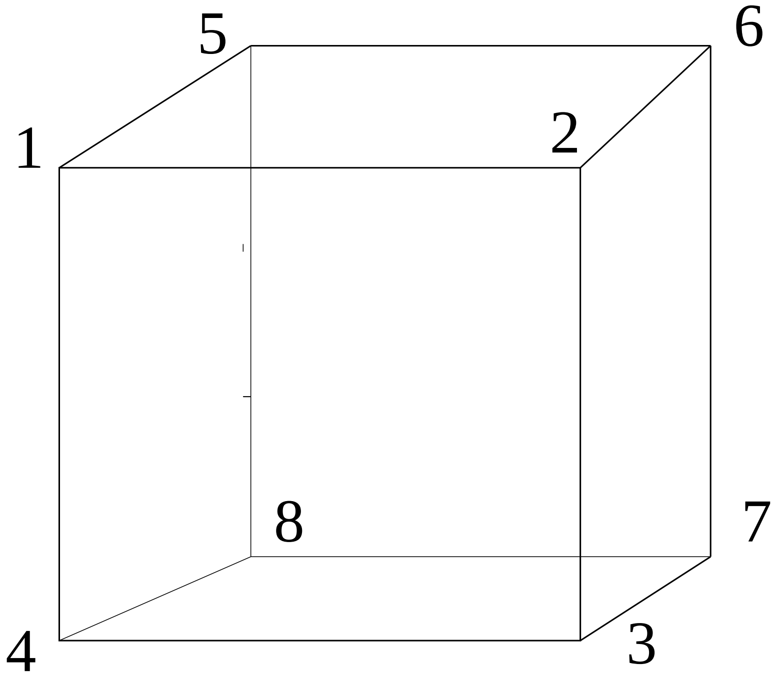

Figure 18.1: The cube

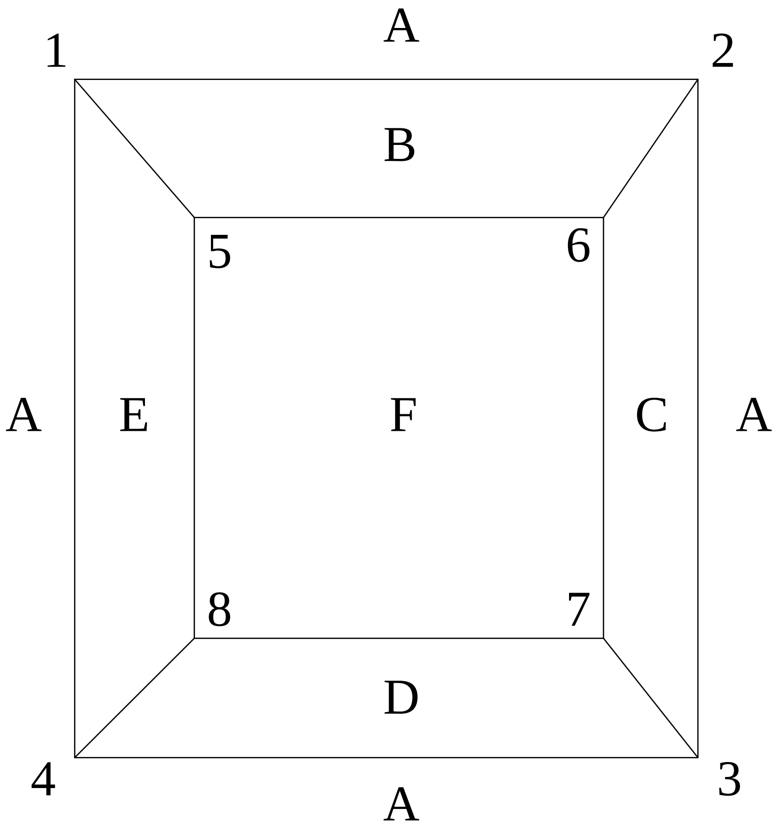

Figure 18.2: A flat version of the cube

must be fixed. The same argument holds for all other vertices. We conclude $|G| = 6 \cdot 8 = 48$. $\square$

Along the way we have also seen that the stabilizer of a face is D_8. Consider the action of G on the 4 pair 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 $g(2)$. 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 13.5 that G/K is isomorphic to a subgroup of S_4. As $|G/K| = 24 = |S_4|$ it follows $G/K \cong S_4$.

18.2. 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.

18.3. 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 17.1). 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 13.5 that the permutation representation of G on the faces yields an isomorphism between G and the automorphism group of the face-graph.

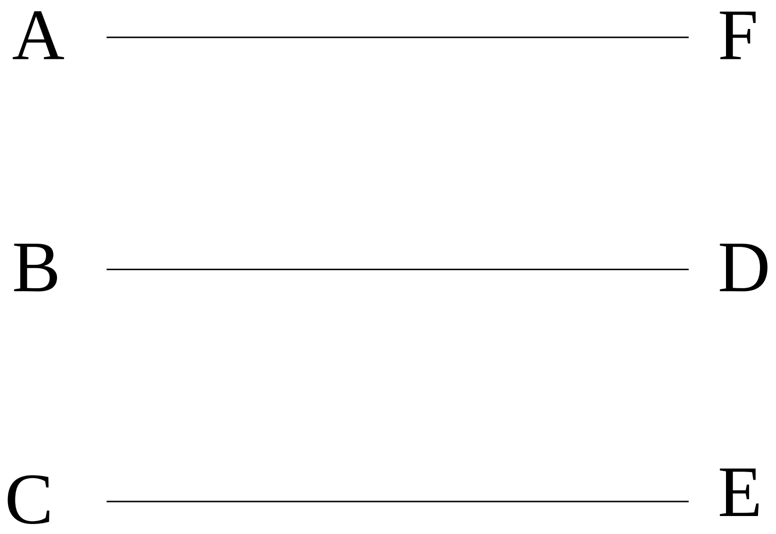

Figure 18.3: A graph related to the cube

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

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

Chapter 19

Prime fields

19.1. 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 $x \cdot y \in F$. 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 $x \in F$.*
- *$F \setminus \{0\} = F^x$ is an abelian group under multiplication. Denote the neutral element of F^x 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.

19.2. 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 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 $\mathbb{F}_p^x$. 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 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 7.2 that there are integers b and w such that $ab + pw = 1$. This proves our claim. □

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

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

Proof. Let $d \mid p - 1$. Every element $x \in \mathbb{F}_p^x$ 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 $\mathbb{F}_p$ is the number of generators of Z_d, which by Theorem 10.2 is $\phi(d)$. We have seen that for every divisor d of the group order $p - 1$ the number of elements of order d is either 0 or $\phi(d)$. Comparison with Theorem 10.3 shows that it is impossible that our group has no elements of order $p - 1$. The group is therefore cyclic. □

Chapter 20

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.

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

20.2. 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.

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

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

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

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

Let g be in the kernel of the action of $GL(n,p)$ 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 $\mathbb{F}_p e_i$ 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 $\mathbb{F}_p(e_i - e_j)$ 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.

20.5. Proposition. *The kernel Z of $GL(n,p)$ in its action on the 1-dimensional subspaces consists of the scalar matrices $diag(\lambda, \ldots, \lambda)$, where $\lambda \in \mathbb{F}_p^x$. It follows from Theorem 19.3 that $Z \cong Z_{p-1}$.*

20.6. Definition. *The group $PGL(n,p) = GL(n,p)/Z$ 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 $GL(n,p)$ is in bijection with the ordered bases of our space $\mathbb{F}_p^n$. Let us count these bases: The first vector v_1 is an arbitrary nonzero vector. There are $p^n - 1$ 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 $\mathbb{F}_p v_1$. The number of choices $p^n - p$. The number of choices for the pair (v_1, v_2) is $(p^n - 1)(p^n - p)$. 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 $p^n - p^i$, as the vectors from the subspace generated by $v_1, v_2, \ldots, v_i$ are forbidden. We obtain the following formula:

20.7. Theorem.

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

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

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

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 10.4. □

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

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

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

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

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

20.10. 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.*

Chapter 21

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.

21.1. Definition. *A group isomorphism $f : G \longrightarrow G$ is an* **automorphism** *of G (see also Chapter 9). 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.

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

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

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

This operation has made its appearance in Chapter 12 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.

21.3. 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. □

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

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

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.

Chapter 22

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:

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

$$\alpha(\pi_1(g)) = \pi_2(\alpha(g)).$$

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:

22.2. 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:

22.3. 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:

22.4. 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 22.4:

22.5. 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 21.4).

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 Chapter 6). Finally we show that multiplication from the right is in principle sufficient to describe all transitive permutation representations.

22.6. 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 16.6 that all the elements mapping $i \mapsto j$ form the coset Hg. This gives us the desired bijection. $\square$

Chapter 23

Conjugacy classes

23.1. 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 22.5 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:

23.2. 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:

23.3. Lemma. *The conjugate of the n-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 23.3 that the m-cycles form one conjugate class.

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

We know from Chapter 4 that the cycle type is uniquely determined. Lemma 23.3 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:

23.5. 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 23.3 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 $(2,2)$.

Chapter 24

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

24.1. 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 calculations shows it is closed under inverses. □

24.2. 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 24.1, 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. □

The concept of conjugation is particularly fruitful. We showed in Chapter 21 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.

24.3. 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 21.3). 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. □

Consider the group $V \lhd S_4$. As V is (elementary) abelian, it has no inner automorphisms. Apply Theorem 24.3. 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 15.2 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.

Chapter 25

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 6.3): 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.

25.1. 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.

25.2. 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 22.5), 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. □

25.3. 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 25.2 (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. □

25.4. 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:

25.5. 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 $g \in \mathbb{N}_G(P)N = N\mathbb{N}_G(P)$. $\square$

Chapter 26

Proof of the Sylow theorems

26.1. 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 25.3 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 $P \leq I\!N(Q)$. It follows from Theorem 24.1 that PQ is a group. As $PQ/Q \cong P/(P \cap Q)$ by Theorem 24.2 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 25.3 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 $[G : P] = [G : I\!N_G(P)][I\!N_G(P) : P]$. Assume $|P| < p^n$. Then $[G : P]$ is a multiple of p. We know that the first factor equals the cardinality of $Syl_p(G)$ and is not divisible by p. It follows that $|I\!N_G(P)/P|$ is divisible by p. By Cauchy's theorem we can find a group of order p in $I\!N_G(P)/P$. This yields a group of order $p \cdot |P|$ containing P, which contradicts the maximality of P. We conclude that $Syl_p(G)$ consists of the subgroups of order p^n. All the statements of the Sylow theorems have been proved.

Chapter 27

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.

27.1. 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. Are there any non-abelian simple groups?

27.2. 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 23.5). 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 $\mathbb{C}(g) \not\subseteq A_5$, then $g^{S_5} = g^{A_5}$. Upon inspection of the table we see that A_5 has five conjugacy classes of lengths 1,12 (5-cycles),12 (5-cycles),20 (3-cycles),15 (products of two transpositions).

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

We can prove more:

27.3. 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. $\square$

We mention that all the alternating groups $A_n, n \geq 5$ are simple. Likewise, the groups $PSL(n,p)$ are simple except for $PSL(2,2)$ and $PSL(2,3)$.

Chapter 28

Problems

1. Write the permutation

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

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

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

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

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

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

6. Find a normal subgroup of the group D_8.

7. Find all normal subgroups of S_4.

8. Prove that the intersection of two subgroups is a subgroup.

9. Prove that the intersection of two normal subgroups is a normal subgroup.

10. Prove that the symmetry group V from Theorem 2.1 is elementary-abelian.

11. Give an example showing that the image of a homomorphism is not in general a normal subgroup.

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

13. Prove the following: if $g \in G, o(g) = n$ and $h \in H, o(h) = m$, then the element $(g, h) \in G \times H$ has order $lcm(n, m)$.

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

15. Prove Proposition 10.4.

16. Show that the subgroups of order 2 in S_3 are not normal.

17. Prove Proposition 16.5.

18. Show that D_{2n} is not abelian when $n > 2$.

19. Find an element of order 3 of the cube group and the corresponding symmetry of the face graph (see Chapter 18).

20. Determine the number of elements of order 3 in the cube group.

21. Show that every element in $D_{2n} \setminus Z_n$ has order 2.

22. Let Γ be the graph on $2n$ vertices, which has n disjoint edges. Determine the order of its automorphism group.

23. Determine the center of the quaternion group Q_8.

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

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

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

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

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

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

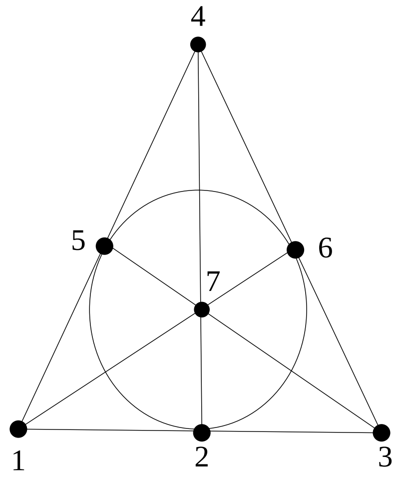

Figure 28.1: The Fano plane

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