

1 Group theory

Version 1: 22. august 2006

The purpose of this chapter is to present a number of important topics in the theory of groups. We have primarily chosen topics which are relevant to get a better understanding of finite groups, eg. to determine up to isomorphism all groups with certain given properties. This may be useful in later chapters to study Galois groups of finite normal field extensions.

Most readers of this text may have already learned some basic facts about groups. Therefore some parts of this chapter is written in a rather compact form.

A number of fairly elementary *Exercises* are included in the text.

The text contains some references on the form (AT; p ..). They are references to the Lecture Notes by Anders Thorup: Algebra (2. udgave), written in Danish. This is for the convenience of some readers. However most of the present text may be read independently of AT.

Contents

1	Group theory	1
1.1	Definitions and examples	3
1.2	Subgroups	5
1.3	Powers and orders of elements	6
1.4	Some subgroups	8
1.5	Cosets and Lagrange's theorem	9
1.6	Product of subgroups	11
1.7	Normal subgroups and factor groups	11
1.8	Homomorphisms, isomorphisms, automorphisms	13
1.9	The homomorphism theorem. Noether's isomorphism theorems	15
1.10	Cyclic groups	16
1.11	Conjugation. The class equation	19
1.12	Characteristic subgroups	21
1.13	The automorphism group of a cyclic group	23
1.14	Sylow's theorems	23
1.15	Direct products. Abelian groups	26
1.16	Permutation groups	29
1.17	Chains of subgroups, composition series	33
1.18	Higher commutator subgroups. Solvable groups	35
1.19	Semidirect products of groups	37
1.20	Groups of a given order	38

1.1 Definitions and examples

Definition 1.1 A *group* is a nonempty set G on which there is defined a law of composition (sometimes also referred to as a binary operation.) This is a map $\star : G \times G \rightarrow G$, $(a, b) \mapsto a \star b$, satisfying the following properties:

- (1) For all $a, b, c \in G$: $(a \star b) \star c = a \star (b \star c)$. (*Associativity of \star*)
- (2) There exists $e \in G$, such that for all $a \in G$: $a \star e = e \star a = a$. (*Existence of a unit/neutral/trivial element in G .*)
- (3) For all $a \in G$ there exists an element $a' \in G$ such that $a \star a' = a' \star a = e$. (*Existence of inverse elements in G .*)

Remark 1.2 Clearly there is only one element $e \in G$ satisfying condition (2). Indeed if $e' \in G$ satisfies $e' \star a = a$ for all $a \in G$, then in particular $e = e' \star e = e'$. The unique element e occurring in condition (2) is called the *unit element* of G . It is also sometimes referred to as the *trivial* or the *neutral* element.

Also clearly the element a' in condition (3) is uniquely determined by a . Indeed, if for some $a'' \in G$ we also have $a'' \star a = e$, then

$$a'' = a'' \star e = a'' \star (a \star a') = (a'' \star a) \star a' = e \star a' = a'.$$

We call the (unique) element a' in condition (3) for the *inverse* of a and denote it by a^{-1} .

The uniqueness of inverse elements imply that we have the following relations for all $a, b \in G$:

$$\begin{aligned}(a^{-1})^{-1} &= a \\ (a \star b)^{-1} &= b^{-1} \star a^{-1}.\end{aligned}$$

(AT, p. 40)

Definition 1.3 If the group G contains only finitely many elements, say n , we call n the *order* of G and write $|G| = n$. We then call G a *finite* group. The group G is called *infinite* if it is not finite. We then write $|G| = \infty$.

Definition 1.4 If G is a group with a *commutative* composition, it is called *abelian*. Thus in addition to (1) – (3) above we also have for all $a, b \in G$ that $a \star b = b \star a$.

Definition 1.5 If $a, b \in G$ satisfy $a \star b = b \star a$ they are said to *commute*. The *commutator* of a, b is defined by

$$[a, b] = a \star b \star a^{-1} \star b^{-1}.$$

Clearly a and b commute if and only if $[a, b] = e$, ie. their commutator is trivial.

If we want to specify the composition \star used to make a set G into a group we write (G, \star) . Thus for example $(\mathbb{Z}, +)$ is a group, because addition of integers satisfy the conditions (1)-(3) with 0 as unit element and $-a$ as the inverse of $a \in \mathbb{Z}$. It is even abelian, because addition of integers is commutative. It is also an example of an infinite group.

Definition 1.6 For $n \in \mathbb{N}$ we define the *symmetric group of degree n* , denoted S_n , as the set of all permutations of the integers $1, \dots, n$. The elements in S_n are thus the bijective maps $\sigma : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ and they form a group with “composition of maps” as composition. (AT; p. 53). The elements of S_n are also referred to simply as *permutations of n* .

Remark 1.7 A typical permutation (element $\sigma \in S_n$) may be represented concretely in several ways:

The tabular description. We write a table (matrix) where the integer $i, 1 \leq i \leq n$ is placed above the integer, it is mapped to:

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

The direct description is essentially the tabular description, with the top row removed:

$$\sigma = [\sigma(1) \ \sigma(2) \ \dots \ \sigma(n)]$$

This description would appear to be “simpler” than the previous one and it is used frequently in the combinatorial studies of permutations. However it is not easy to use when you want to compute the “product” (composition) of two permutations. Therefore it will not be used later on in these notes.

The cycle decomposition : The element is written as a product of disjoint cycles,

$$\sigma = (i_1, i_2, \dots, i_r)(j_1, j_2, \dots, j_s) \dots (k_1, k_2, \dots, k_t).$$

Here the cycle (i_1, i_2, \dots, i_r) means that

$$i_1 \mapsto i_2, i_2 \mapsto i_3, \dots, i_{r-1} \mapsto i_r, i_r \mapsto i_1$$

and the subsets of the i 's, j 's etc are disjoint. The length of a cycle is the number elements in it. Thus $\sigma = (i_1, i_2, \dots, i_r)$ has length r .

If an integer $i \in \{1, \dots, n\}$ is a fixpoint for the permutation σ , (ie. $\sigma(i) = i$) then (i) is going to be a cycle with only one element in the cycle decomposition and is usually omitted. As an example $\sigma = (2, 3, 4)(5, 6)$ is the permutation in S_6 given by

$$\sigma(1) = 1, \sigma(2) = 3, \sigma(3) = 4, \sigma(4) = 2, \sigma(5) = 6, \sigma(6) = 5.$$

The unit element e in S_n is also denoted (1). The cycle decomposition of a permutation is unique up to the ordering of the cycles and ”rotations” within a cycle: Thus for example $(i_1, i_2, i_3)(j_1, j_2) = (i_3, i_1, i_2)(j_2, j_1)$.

Definition 1.8 (CYCLE TYPE) Suppose that $\sigma \in S_n$ is written as a product of disjoint cycles and that the number of cycles of length i in the product is $m_i \geq 0$. Then $\sum_{i \geq 1} im_i = n$ and the *cycle type* $ct(\sigma)$ of σ is defined as $ct(\sigma) = (1^{m_1}, 2^{m_2}, 3^{m_3}, \dots)$. The *sign* of σ is defined by $\text{sign}(\sigma) = (-1)^{(n - \sum_{i \geq 1} m_i)}$. (AT; p. 62). The permutation σ is called *even/odd* if $\text{sign}(\sigma) = +1/-1$. In particular, a cycle of length i is even if and only if i is odd.

A *cycle type of n* is by definition one of the $ct(\sigma)$, $\sigma \in S_n$. The number of cycle types of n is denoted $p(n)$. The cycle types of 4 are $(1^4), (1^2, 2), (1, 3), (2^2), (4)$. Thus $p(4) = 5$. The cycle types play also a rôle for abelian groups of prime power order in Section 1.15.

Exercise 1.9 Compute the cycle type of all permutations in S_3 .

Definition 1.10 If K is an arbitrary field and $n \in \mathbb{N}$ we define the *general linear group of degree n over K* , denoted $GL(n, K)$, as the set of all invertible $n \times n$ -matrices with coefficients from K with matrix multiplication as composition. It is known from linear algebra that a quadratic matrix with coefficients from a field is invertible if and only if its determinant is non-zero. (AT; p 46-47)

1.2 Subgroups

Definition 1.11 Let (G, \star) be a group. A non-empty subset $H \subseteq G$ is called a *subgroup* of G , if it satisfies the condition that $a \star b^{-1} \in H$ for all $a, b \in H$. Equivalently H is a subgroup of G , if we have that $a \star b \in H$ for all $a, b \in H$ and in addition that (H, \star) is a group.

In practice you may prove that a subset H of G is a subgroup by showing

- (i) $e \in H$
- (ii) If $a \in H$ then $a^{-1} \in H$
- (iii) If $a, b \in H$ then $a \star b \in H$.

Definition 1.12 Any group G has G and $\{e\}$ as subgroups. These are referred to as the *trivial* subgroups of G . All other subgroups are called *non-trivial*.

For example, the subset of *even* integers form a non-trivial subgroup of $(\mathbb{Z}, +)$.

Remark 1.13 Suppose that \mathcal{X} is a nonempty set of subgroups of the group G . Then the intersection $U = \bigcap_{H \in \mathcal{X}} H$ is again a subgroup of G . This is easily verified from the definition of a subgroup and may be used to show the following:

Lemma 1.14 Let A be an arbitrary subset of the group G . Then there exists a unique subgroup U of G with the following properties:

(i) $A \subseteq U$

(ii) If H is any subgroup of G with $A \subseteq H$ then $U \subseteq H$.

Proof Let

$$\mathcal{X} = \{K \mid K \text{ is a subgroup of } G \text{ and } A \subseteq K\}.$$

The set \mathcal{X} is nonempty, since $G \in \mathcal{X}$ and thus $U := \bigcap_{H \in \mathcal{X}} H$ is a subgroup of G . Since $A \subseteq K$ for all $K \in \mathcal{X}$ we get $A \subseteq U$, so (i) is fulfilled. If H is any subgroup of G with $A \subseteq H$ then $H \in \mathcal{X}$ and thus by definition of U we have $U \subseteq H$. This shows (ii). \square

Definition 1.15 In the situation of the above lemma the subgroup U is called the *subgroup of G generated by A* . This is then the (unique) smallest subgroup of G containing M and it will be denoted $\langle A \rangle$ in the following. If $A = \{a_1, a_2, \dots, a_n\}$ is a finite subset of G we also write $\langle a_1, a_2, \dots, a_n \rangle$ for the subgroup generated by A . (See Remark 1.22 for a description of the elements in $\langle A \rangle$.) In particular a subgroup of G on the form $\langle a \rangle$ for some $a \in G$ is called a *cyclic* subgroup of G . We also refer to $\langle a \rangle$ as the *cyclic subgroup generated by a* .

In the following we are going to use “multiplication” as composition in an abstract group G . Thus we consider (G, \cdot) unless otherwise specified and the product $a \cdot b$ of two elements in G will mostly also be denoted simply by ab , omitting the \cdot .

1.3 Powers and orders of elements

Remark 1.16 Let G be a group and $a \in G$. We describe the elements in the subgroup $\langle a \rangle$. They are the *powers* of a : Define $a^0 = e$ and $a^n = a \cdot a \cdots a$ (n times) for $n \in \mathbb{N}$. If $n \in \mathbb{Z}$ is negative then $-n$ is positive and we define $a^n = (a^{-n})^{-1}$. It is wellknown that we have the following *power rules* for the powers of a :

$$a^{n+m} = a^n a^m, \quad (a^n)^m = a^{nm}, \quad \text{for } n, m \in \mathbb{Z}.$$

This shows that $\langle a \rangle$ is the set all of powers of a . Indeed, if a is contained in a subgroup H of G , then clearly also all powers of a are contained in H . Thus all powers of a are contained in $\langle a \rangle$. On the other hand, the power rules show that the set of all powers of a form a subgroup of G .

Definition 1.17 Let G be a group and $a \in G$. The *order* $|a|$ of a is defined as the order of $\langle a \rangle$.

Theorem 1.18 Let G be a group and $a \in G$. The order $|a|$ of a is finite if and only if $a^m = e$ for some $m \in \mathbb{N}$. In that case $|a| = \min\{k \in \mathbb{N} \mid a^k = e.\}$ If $|a| = n$ is finite then we have for all $m \in \mathbb{Z}$:

$$a^m = e \iff n \mid m.$$

Proof Clearly $|a|$ is finite if and only if $a^{m_1} = a^{m_2}$ for some $m_1, m_2 \in \mathbb{Z}$, $m_1 > m_2$. But then $m = m_1 - m_2 \in \mathbb{N}$ satisfies $a^m = e$. Indeed, $a^m = a^{m_1 - m_2} = a^{m_1}(a^{m_2})^{-1} = e$, using the power rules. If $n = \min\{k \in \mathbb{N} \mid a^k = e\}$ then by the above the powers $a^0 = e, a^1, \dots, a^{n-1}$ are all different, so that $|a| \geq n$. Writing $m \in \mathbb{Z}$ on the form $m = nt + r$, $0 \leq r < n$ then the power rules imply that $a^m = a^r$. Thus $|a| \leq n$, ie. $|a| = n$. We notice additionally that

$$a^m = e \iff a^r = e \iff r = 0 \iff n \mid m. \quad \square$$

Exercise 1.19 Show that if all elements $\neq e$ in a group has order 2 then G is abelian.

Example 1.20 Let $\sigma = (1, 2, 3)(4, 5) \in S_5$, the symmetric group of degree 5. The powers σ^i of σ are for $1 \leq i \leq 6$

$$(1, 2, 3)(4, 5), (1, 3, 2), (4, 5), (1, 2, 3), (1, 3, 2)(4, 5), (1)$$

so that $|(1, 2, 3)(4, 5)| = 6$.

Generally the order of an element in S_n is the least common multiple of the lengths of the cycles in the cycle decomposition of the element. (AT; p. 74)

Theorem 1.21 Let G be a group and $a \in G$ with $|a| = n$ finite. Suppose $n = rs$ $r, s \in \mathbb{N}$. Let $m \in \mathbb{Z}$ be arbitrary. Then

- (1) $|a^r| = s$
- (2) $\langle a^m \rangle = \langle a^{(m,n)} \rangle$.
- (3) $|a^m| = n/(m, n)$.

Here (m, n) denotes the greatest common divisor of m and n .

Proof (1) Suppose $|a^r| = s'$. Since $(a^r)^s = a^{rs} = a^n = e$ we have $s' \mid s$ by Theorem 1.18 applied to a^r . On the other hand since $|a^r| = s'$ we have $a^{rs'} = (a^r)^{s'} = e$. Theorem 1.18 applied to a shows $n = rs \mid rs'$ and therefore $s \mid s'$. Thus $s = s' = |a^r|$.

(2) Since $(m, n) \mid m$ we have $a^m \in \langle a^{(m,n)} \rangle$ and thus $\langle a^m \rangle \subseteq \langle a^{(m,n)} \rangle$. It is wellknown that there exists $k, l \in \mathbb{Z}$ such that $(m, n) = km + ln$. Then $a^{(m,n)} = a^{km}a^{ln} = (a^m)^k$, using the power rules and the fact that $a^n = e$. Thus $a^{(m,n)} \in \langle a^m \rangle$, showing $\langle a^{(m,n)} \rangle \subseteq \langle a^m \rangle$.

(3) By (2) $|a^m| = |a^{(m,n)}|$. Writing $n = (m, n)n'$ we have using (1) that $|a^{(m,n)}| = n' = n/(m, n)$. \square

Powers play also rôle in the description of $\langle A \rangle$, $A \subseteq G$.

Remark 1.22 Let A be an arbitrary subset of the group G . The elements of $\langle A \rangle$ may be described as follows. They are finite products $a_1^{n_1}a_2^{n_2} \cdots a_t^{n_t}$, where $a_1, a_2, \dots, a_t \in A$, $n_1, n_2, \dots, n_t \in \mathbb{Z}$. Clearly if a and b are such finite products then ab^{-1} is also such a product. As in Remark 1.16 we conclude that $\langle A \rangle$ is the set of all these products. We give a concrete example below.

Exercise 1.23 Let A be an arbitrary subset of the group G . Show that $\langle A \rangle$ is abelian if and only if $a_1a_2 = a_2a_1$ for all $a_1, a_2 \in A$.

1.4 Some subgroups

We consider some important subgroups of symmetric and general linear groups.

Example 1.24 (VIERERGRUPPE) Let $G = S_4$ be the symmetric group of degree 4. Let

$$A = \{\alpha = (1, 2)(3, 4), \beta = (1, 3)(2, 4)\}.$$

We compute $\langle A \rangle$. If $\gamma = (1, 4)(2, 3)$ have $\alpha\beta = \beta\alpha = \gamma$. Thus Remark 1.22 shows $\langle A \rangle = \{(1), \alpha, \beta, \gamma\}$. The product of any two of α, β, γ equals the third. This is Kleins Vierergruppe of order 4, which we usually denote V .

If we instead consider the matrices

$$\mathbf{a} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{b} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \mathbf{c} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in \mathbf{GL}(2, \mathbb{R})$$

then again the product of any two of $\mathbf{a}, \mathbf{b}, \mathbf{c}$ equals the third and they all have order two. This is another realization of the Vierergruppe.

Example 1.25 (DIHEDRAL GROUP) Let $G = S_5$ be the symmetric group of degree 5. Let

$$A = \{\sigma = (1, 2, 3, 4, 5), \rho = (1, 5)(2, 4)\}.$$

We compute $\langle A \rangle$. It is easy to compute that

$$(*) \quad \rho\sigma = \sigma^4\rho.$$

By Remark 1.22 $\langle A \rangle$ consists of elements on the form $\sigma^{m_1}\rho^{n_1}\sigma^{m_2}\rho^{n_2}\dots$, where $m_i, n_i \in \mathbb{Z}$. As $|\rho| = 2$ we may assume for all i that $0 \leq n_i \leq 1$. The n_i 's which are 0 may be omitted, since $\rho^0 = 1$. Thus an element in $\langle A \rangle$ has the form $\sigma^{m_1}\rho\sigma^{m_2}\rho\dots$. But (*) shows that $\rho\sigma^m = \sigma^{4m}\rho$ for all $m \geq 0$. (Apply (*) m times). Thus any element in $\langle A \rangle$ may be written as $\sigma^m\rho^n$ where $0 \leq m \leq 4, 0 \leq n \leq 1$. (The restriction on m is because $|\sigma| = 4$.) We get $|\langle A \rangle| = 10$. In fact $\langle A \rangle$ is (isomorphic to) a dihedral group D_5 (AT; p. 48). The element a corresponds to a rotation and b to a reflexion.

More generally in S_n , $n \geq 3$ we have that we may realize a dihedral group D_n of order $2n$ as $\langle (1, 2, \dots, n), (1, n)(2, n-1)(3, n-2)\dots \rangle$.

Example 1.26 (QUATERNION GROUP) If we consider the matrices

$$\mathbf{i} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \mathbf{j} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \in \mathbf{GL}(2, \mathbb{C})$$

then it can be shown that $\pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}$ together with $\pm I$ (I the identity matrix) form a group of order 8, where all elements except $\pm I$ have order 4. This is the quaternion group Q . (AT; p. 50)

1.5 Cosets and Lagrange's theorem

Definition 1.27 Let A and B be arbitrary subsets of the group G . We define a new subset AB of G by

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

ie. as the set of all products of an element in A and an element in B . Note that generally it is *not* true that $AB = BA$. If $A = \{a\}$ consists of a single element, we write aB instead of $\{a\}B$ and Ba instead of $B\{a\}$.

Exercise 1.28 Let H be a subgroup of G . Show that $HH = H$. If K is a subset of G satisfying $KK = K$, is K then necessarily a subgroup?

Remark 1.29 Let us note that referring to the above definition the maps $b \mapsto ab$ and $b \mapsto ba$ are *bijections* between B and aB and between B and Ba respectively. Thus $|B| = |aB| = |Ba|$.

Definition 1.30 Let H be an arbitrary subgroup of G . We define relations ${}_H\sim$ and \sim_H on G by

$$a{}_H\sim b \iff ab^{-1} \in H, \quad a \sim_H b \iff a^{-1}b \in H.$$

It is easily checked that ${}_H\sim$ and \sim_H are equivalence relations on G . For example, if $a \sim_H b$ and $b \sim_H c$, ie. $a^{-1}b$ and $b^{-1}c \in H$, then $a^{-1}c = (a^{-1}b)(b^{-1}c) \in H$. This means $a \sim_H c$.

Remark 1.31 The ${}_H\sim$ -equivalence class of G containing the element $a \in G$ is

$$Ha = \{ha \mid h \in H\}.$$

Indeed writing $b \in G$ as $b = (ba^{-1})a$ we see that

$$b \in Ha \iff ba^{-1} \in H \iff b {}_H\sim a.$$

Similarly we see that the \sim_H -equivalence class of G containing the element $a \in G$ is

$$aH = \{ah \mid h \in H\}.$$

Definition 1.32 If H is a subgroup of G then the subsets of G on the form Ha , $a \in G$ are called *left cosets* to H in G and the subsets of G on the form aH , $a \in G$ are called *right cosets* to H in G . An element in a (left or right) coset is referred to as a *representative* of the coset.

Theorem 1.33 (LAGRANGE'S THEOREM) *If H is a subgroup of the finite group G , and $|G : H|$ is the number of left cosets to H in G , then $|G| = |G : H||H|$. Moreover $|G : H|$ is also the number of right cosets to H in G .*

Proof By Remark 1.29 any left coset to H in G contains $|H|$ elements. Remark 1.31 shows that for $a_1, a_2 \in G$ the left cosets Ha_1 and Ha_2 are either equal or disjoint. It follows that $|G| = |G : H||H|$. A similar argument works for right cosets. \square

Definition 1.34 H is a subgroup of the group G , then the number $|G : H|$ of left cosets to H in G is called the *index* of H in G . It is also the number of right cosets to H in G . Note that if G is finite, then the index $|G : H|$ divides $|G|$.

Corollary 1.35 *If H is a subgroup of the finite group G , then $|H|$ divides $|G|$. In particular, if $a \in G$ then $|a|$ divides $|G|$.*

Example 1.36 The corollary shows that all elements in a finite group have finite order. However, the set of *all* complex roots of unity form a *infinite* group (with multiplication as composition) where all elements have *finite* order. The complex roots of unity are studied in Chapter IV of this book.

Example 1.37 A group of G of prime order p is cyclic. Indeed, if $a \in G$, $a \neq 1$, then $|a| = p$, by Corollary 1.35. Thus $G = \langle a \rangle$.

Corollary 1.38 *If H is a subgroup of the finite group G , and if K is a subgroup of H then*

$$|G : K| = |G : H||H : K|.$$

Proof Apply Lagrange's theorem to the subgroup H of G and to the subgroup K of H to get $|G| = |G : H||H : K||K|$. Applying Lagrange's theorem to the subgroup K of G we get $|G| = |G : K||K|$. The result follows. (AT; p. 82) \square

Lemma 1.39 *Suppose that H and K are subgroups of G . The subset HK of G (see Definition 1.27) consists of exactly $|K : H \cap K|$ left cosets to H in G and of exactly $|H : H \cap K|$ right cosets to K in G . Thus for the number of elements in HK we have:*

$$|HK| = |H||K|/|H \cap K|.$$

Proof (AT, p. 82). Use the following to show that HK consists of $|K : H \cap K|$ left cosets to H in G : For $k_1, k_2 \in K$ we have

$$Hk_1 = Hk_2 \Leftrightarrow k_1k_2^{-1} \in H \Leftrightarrow k_1k_2^{-1} \in H \cap K \Leftrightarrow (H \cap K)k_1 = (H \cap K)k_2.$$

The details are left to the reader. \square

1.6 Product of subgroups

Theorem 1.40 *Suppose that H and K are subgroups of G . The subset HK of G is again a subgroup of G , if and only if the subsets HK and KH are equal: $HK = KH$.*

Proof Before we start, here is a *warning*: The condition $HK = KH$ does *not* mean that $hk = kh$ for all $h \in H, k \in K$. (Why?)

Suppose first that HK is a subgroup of G . Let $h \in H, k \in K$ be an arbitrary elements. Since $k \in K \subseteq HK$ and $h \in H \subseteq HK$ and since HK is a subgroup of G we get $kh \in HK$. Thus $KH \subseteq HK$. Next we show that $hk \in KH$. We know that $k^{-1}h^{-1} \in KH$. Since $KH \subseteq HK$ we may write $k^{-1}h^{-1} = h_1k_1$ for suitable elements $h_1 \in H, k_1 \in K$. Inverting this equation we get $hk = k_1^{-1}h_1^{-1} \in KH$. (Use the relations described in Remark 1.2.) Thus also $HK \subseteq KH$ and we get equality. Assume now that $HK = KH$. Suppose that $a = hk, b = h_1k_1 \in HK$ where $h, h_1 \in H, k, k_1 \in K$. We need to show $ab^{-1} \in HK$. (Definition 1.11.) Now $ab^{-1} = h(kk_1^{-1})h_1^{-1}$. Since $(kk_1^{-1})h_1^{-1} \in KH = HK$, we may write $(kk_1^{-1})h_1^{-1} = h_2k_2$ for some $h_2 \in H, k_2 \in K$. Thus $ab^{-1} = hh_2k_2 \in HK$, as desired. \square

1.7 Normal subgroups and factor groups

Definition 1.41 Let N be a subgroup of G . We call N *normal* in G and write $N \triangleleft G$, if the following condition is fulfilled: For all $a \in G, h \in N$: $aha^{-1} \in N$.

Remark 1.42 If you want to prove that a subgroup N of G is a normal subgroup ($N \triangleleft G$) most often the condition in Definition 1.41 is the most convenient. However, there are other equivalent definitions, listed below. The proof that they are equivalent is left as an easy exercise. (AT, p. 84)

- (i) For all $a \in G$: $aNa^{-1} \subseteq N$.
- (ii) For all $a \in G$: $aNa^{-1} = N$.
- (iii) For all $a \in G$: $aN = Na$.

Note that the last condition means that any left coset to N is also a right coset to N . Thus the equivalence relations ${}_N \sim$ and \sim_N from Definition 1.30 are *identical*.

Remark 1.43 In an *abelian* group all subgroups are normal. There is an example of a non-abelian group where all subgroups are normal. This is the quaternion group of order 8. See Example 1.26. It has only one element of order 2, generating the unique subgroup of order 2. There are 3 subgroups of order 4, generated by \mathbf{i}, \mathbf{j} and \mathbf{k} respectively, all of them normal.

Definition 1.44 Clearly the trivial subgroups G and $\{e\}$ of a group G are normal subgroups. We call $G \neq \{e\}$ *simple*, if only the trivial subgroups are normal.

Corollary 1.45 Let N, K be a subgroups of G with $N \triangleleft G$. Then also NK is a subgroup of G .

Proof We use Remark 1.42(iii) to see that

$$NK = \cup_{k \in K} Nk = \cup_{k \in K} kN = KN.$$

The result follows from Theorem 1.40. \square

Exercise 1.46 Show that the following condition is equivalent to $N \triangleleft G$:

$$\text{For all } a, b \in G : ab \in N \iff ba \in N.$$

Exercise 1.47 Let H be a subgroup of G .

- (1) Show that $\langle aHa^{-1} | a \in G \rangle$ is the *smallest normal subgroup* of G containing H .
- (2) Show that $\bigcap_{a \in G} aHa^{-1}$ is the *largest normal subgroup* of G contained in H .

Exercise 1.48 Let H be a subgroup of G of finite index $|G : H| = n$. Let $G = \bigcup_{i=1}^n a_i H$ be the decomposition of G into disjoint right cosets of H .

- (1) Show that $\langle a_i H a_i^{-1} | i = 1, \dots, n \rangle$ is the *smallest normal subgroup* of G containing H .
- (2) Show that $\bigcap_{i=1}^n a_i H a_i^{-1}$ is the *largest normal subgroup* of G contained in H .

Remark 1.49 Suppose that $N \triangleleft G$ and that $a, b \in G$. The left cosets $A = Na$ and $B = Nb$ are subsets of G and thus we may consider their product AB , as in Definition 1.27. Using Remark 1.42(iii) and the fact that $NN = N$, we see that

$$AB = (Na)(Nb) = N(aN)b = N(Na)b = Nab.$$

Thus the product of two left cosets to N in G is another left coset to N in G . This observation allows us to define the factor group G/N below. Let us remark also that since left and right cosets to a normal subgroup coincide we may also use right cosets: $aNbN = abN$.

Definition 1.50 Suppose that $N \triangleleft G$ and let G/N be the set of (left) cosets to N in G . We define a composition \cdot on G/N by $(Na, Nb) \mapsto NaNb = Nab$. By Remark 1.49 this is welldefined. It does not depend on the choice of coset representatives in Na and Nb . (We have in the definition chosen a and b as representatives.) Then $(G/N, \cdot)$ is a group, called the *factor group of G modulo N* . The unit element is $N = N1$ and the inverse element to Na is Na^{-1} . Since the composition \cdot in G/N is induced from the composition of G , we omit it. Obviously $|G/N| = |G : N|$.

Remark 1.51 (BAR NOTATION FOR FACTOR GROUPS) It is important to remember that if $N \triangleleft G$ and $a \in G$ then Na has two meanings: It is a coset of N in G , ie. a *subset* of G . But it is also an *element* in the factor group G/N . Therefore to make clear that we are working in a factor group we are often going to use the notation \bar{a} for an element Na in the factor group G/H . The composition in G/H may then be written as

$$\overline{ab} = \bar{a}\bar{b}.$$

Correspondingly we are often using the notation \bar{G} for G/N . In this so-called *bar notation* it should always be clear what the normal subgroup N is.

Example 1.52 Consider the abelian group $(\mathbb{Z}, +)$. Theorem 1.75 The subgroups of $(\mathbb{Z}, +)$ are exactly those on the form $n\mathbb{Z}$ for some $n \geq 0$. (All multiples of n .) (This is a special case of Theorem 1.75 below.) If $n \geq 1$ then the factor group $\mathbb{Z}/n\mathbb{Z}$ is the so-called *residue class group* modulo n . (AT; p. 43). It is a cyclic group with \bar{e} as a generator. (Cyclic groups are studied in Section 1.10.) Note that the unit element in the additive group $\mathbb{Z}/n\mathbb{Z}$ is $\bar{0}$.

Remark 1.53 Suppose that $N \triangleleft G$ and that G is finite. Then also G/N is finite. Suppose that $\bar{a} \in G/N$ and that $a \in \bar{a}$, considering \bar{a} as a coset to N . (Remark 1.51.) Then $|\bar{a}| \mid |a|$. Indeed, if $|a| = k$ then $a^k = e$ so that $\bar{a}^k = \overline{a^k} = \bar{e}$. By Theorem 1.18 $|\bar{a}| \mid k$. This is a special case of Exercise 1.56.

1.8 Homomorphisms, isomorphisms, automorphisms

Definition 1.54 Suppose that $\phi : G \rightarrow H$ is a map between two groups G and H . We call ϕ a *homomorphism* if

$$\phi(ab) = \phi(a)\phi(b) \text{ for all } a, b \in G.$$

It should be noted that this definition involves both compositions of G and H . A *monomorphism* is an injective homomorphism. Thus ϕ satisfies also: $\phi(a) = \phi(b) \Rightarrow a = b$. An *epimorphism* is a surjective homomorphism. Thus ϕ satisfies also: For all $c \in H$ there exists a $a \in G$ with $\phi(a) = c$.

Example 1.55 (THE CANONICAL EPIMORPHISM) Suppose that $N \triangleleft G$ and let $\bar{G} = G/N$ be the factor group. In the notation of Remark 1.51 the map $\kappa : G \rightarrow \bar{G} = G/N$ defined by $\kappa(a) = \bar{a}$ is an epimorphism. It is clearly surjective and the relation $\overline{ab} = \bar{a}\bar{b}$ shows that it is a homomorphism. We refer to κ as the *canonical epimorphism*. (AT; p. 90)

Exercise 1.56 Let $\phi : G \rightarrow H$ be a homomorphism between the finite groups G and H . Let $a \in G$. Show (eg. using Theorem 1.18) that $|\phi(a)| \mid |a|$. Why is Remark 1.53 a special case of this?

Definition 1.57 Let $\phi : G \rightarrow H$ be a homomorphism between the groups G and H . We define the *kernel* $\text{Ker}(\phi)$ and the *image* $\text{Im}(\phi)$ of f by

$$\text{Ker}(\phi) = \{a \in G \mid \phi(a) = e\}$$

$$\text{Im}(\phi) = \phi(G) = \{c \in H \mid \text{There exists } a \in A \text{ such that } \phi(a) = c\}.$$

Lemma 1.58 If $\phi : G \rightarrow H$ is a homomorphism between the groups G and H , then:

- (i) $\text{Ker}(\phi) \triangleleft G$.
- (ii) The map ϕ is a monomorphism if and only if $\text{Ker}(\phi) = \{e\}$.
- (iii) $\text{Im}(\phi)$ is a subgroup of H .
- (iv) The map ϕ is an epimorphism if and only if $\text{Im}(\phi) = H$.

Proof Exercise. (AT; p. 89-90) \square

Definition 1.59 A homomorphism $\phi : G \rightarrow H$ is called an *isomorphism* if the map ϕ is a bijection. By Lemma 1.58 this is the case if and only if $\text{Ker}(\phi) = \{e\}$ and $\text{Im}(\phi) = H$. We write $G \simeq H$ and call the groups *isomorphic*, if there exists a isomorphism between G and H .

Remark 1.60 It should be noted that \simeq is a equivalence relation on the set of all groups. To see this we need only check the following three facts:

- (i) The identity map $\text{Id} : G \rightarrow G$ is an isomorphism.
- (ii) If $\phi : G \rightarrow H$ is an isomorphism, then $\phi^{-1} : H \rightarrow G$ is also an isomorphism.
- (iii) $\phi : G \rightarrow H$ and $\psi : H \rightarrow K$ are isomorphisms, then also the composite map $\psi \circ \phi : G \rightarrow K$ is an isomorphism.

The equivalence classes for \simeq are called *isomorphism classes*. Groups in an isomorphism class are usually considered as “equal”.

Definition 1.61 An isomorphism $\phi : G \rightarrow G$, where G is a group, is called an *automorphism* of G . The set of automorphisms of G is denoted $\text{Aut}(G)$.

Remark 1.62 $\text{Aut}(G)$ is again a group (called the *automorphism group* of G) if we define the product of two automorphisms as their composite. We need only check the following facts, which are special cases of the statements in Remark 1.60:

- (i) The identity map $\text{Id} : G \rightarrow G$ is an automorphism.
- (ii) If $\phi : G \rightarrow G$ is an automorphism, then $\phi^{-1} : G \rightarrow G$ is also an automorphism.
- (iii) $\phi : G \rightarrow G$ and $\psi : G \rightarrow G$ are automorphisms, then also the composite map $\psi \circ \phi : G \rightarrow G$ is an automorphism.

Definition 1.63 If G is a group, $a \in G$ then we define the *inner automorphism* k_a corresponding to a by

$$k_a(g) = aga^{-1}.$$

The map k_a is also sometimes called *conjugation by a* . (AT; p 115). It is easily checked that indeed $k_a \in \text{Aut}(G)$ and that for $a, b \in G$ we have for the composites of the inner automorphisms that $k_a \circ k_b = k_{ab}$. In particular $(k_a)^{-1} = k_{a^{-1}}$. The set $\text{Aut}_i(G)$ of inner automorphisms of G is thus a subgroup of $\text{Aut}(G)$. We even have $\text{Aut}_i(G) \triangleleft \text{Aut}(G)$ by the following exercise.

Exercise 1.64 Show that for all $a \in G, \phi \in \text{Aut}(G)$ we have

$$\phi \circ k_a \circ \phi^{-1} = k_{\phi(a)}.$$

1.9 The homomorphism theorem. Noether's isomorphism theorems

The following result is rather fundamental for the understanding of the structure of groups.

Theorem 1.65 (THE HOMOMORPHISM THEOREM) *Let $\phi : G \rightarrow H$ be a homomorphism of groups. Then $\text{Ker}(\phi) \triangleleft G$ and $G/\text{Ker}(\phi) \simeq \text{Im}(\phi)$. More precisely, if we consider ϕ as a homomorphism $G \rightarrow \text{Im}(\phi)$, (cfr. Lemma 1.58) then ϕ induces an isomorphism $\bar{\phi} : G/\text{Ker}(\phi) \rightarrow \text{Im}(\phi)$, such that $f = \bar{\phi} \circ \kappa$, where κ is the canonical epimorphism $G \rightarrow G/\text{Ker}(\phi)$.*

Proof The key observation for the proof is the following. Suppose that $a, b \in G$ are in the same coset to $N = \text{Ker}(\phi)$, ie. $ab^{-1} \in \text{Ker}(\phi)$. Then $\phi(a) = \phi(b)$. This means that the map $\bar{\phi} : G/\text{Ker}(\phi) \rightarrow \text{Im}(\phi)$ defined by $\bar{\phi}(\bar{a}) = \phi(a)$ is the desired isomorphism. The details are left to the reader. (AT; p. 91) \square

Definition 1.66 We define

$$Z(G) = \{a \in G \mid ag = ga \text{ for all } g \in G\} = \{a \in G \mid k_a = \text{Id}\}.$$

This normal subgroup $Z(G)$ of G is called the *center* of G . It is sometimes also denoted $\text{Cent}(G)$. (AT; p 116). Note that also any subgroup of $Z(G)$ is normal in G . (Why?)

Example 1.67 The map $\phi : a \mapsto k_a$ is an epimorphism $G \rightarrow \text{Aut}_i(G)$. The kernel of ϕ is $Z(G)$. (Definition 1.66). Theorem 1.65 tells us that

$$\text{Aut}_i(G) \simeq G/Z(G).$$

Example 1.68 (THE ALTERNATING GROUPS) In Definition 1.8 we defined the sign of a permutation $\sigma \in S_n$ in a symmetric group. Thus $\sigma \mapsto \text{sign}(\sigma)$ is a map $S_n \rightarrow \{1, -1\}$. We may consider $\{1, -1\}$ as a multiplicative group of order 2. It is quite remarkable that the map sign is in fact a homomorphism. This is not very easy to show. We omit the proof. See eg. (AT; p. 63). Let us assume $n \geq 2$. Then the 2-cycle $(1, 2)$ is odd, ie. $\text{sign}((1,2))=-1$. Let $A_n = \text{Ker}(\text{sign})$. Theorem 1.65 tells us that A_n is a normal subgroup of index 2 in S_n . It consists of all even permutations of S_n and is called the alternating group.

Example 1.69 (THE SPECIAL LINEAR GROUPS) If K is an arbitrary field and $n \in \mathbb{N}$ then it is known from linear algebra that the determinant map is a homomorphism from $GL(n, K)$ to K^* , the multiplicative group of K . The kernel of this homomorphism, the set of matrices with determinant 1, form a normal subgroup, the Special Linear group $SL(n, k)$. The homomorphism theorem tells us that $GL(n, K)/SL(n, q) \simeq K^*$.

Here are some important applications of Theorem 1.65 which are called *Noethers isomorphism theorems*. We only sketch the proofs. (AT; pp. 94-96).

Theorem 1.70 (NOETHERS FIRST ISOMORPHISM THEOREM) *Let N, K be subgroups of G , $N \triangleleft G$. Then $N \cap K \triangleleft K$ and $NK/N \simeq K/N \cap K$.*

Proof It is easily seen that $N \cap K \triangleleft K$ using that $N \triangleleft G$. By Corollary 1.45 NK is a subgroup of G and clearly $N \triangleleft NK$. For each $k \in K$ we let $\bar{k} = kN \in NK/N$. The map $\phi : K \rightarrow NK/N$ defined by $\phi(k) = \bar{k}$ is clearly a homomorphism. The kernel of ϕ is $N \cap K$, because $\bar{k} = \bar{e} \iff k \in N$. Using the definition of NK is easily seen that ϕ is an epimorphism, ie. $\text{Im}(\phi) = NK/N$. Therefore we may apply the Homomorphism theorem 1.65. \square

Theorem 1.71 (NOETHERS SECOND ISOMORPHISM THEOREM) *Let N be normal in G and κ the canonical epimorphism $\kappa : G \rightarrow G/N = \bar{G}$. Then the maps $\alpha : K \rightarrow \kappa(K) \subseteq \bar{G}$ and $\beta : \bar{K} \rightarrow \kappa^{-1}(\bar{K})$ yield a 1-1 correspondence between the subgroups K of G containing N and the subgroups \bar{K} of \bar{G} . This correspondence satisfies $K \triangleleft G \iff \kappa(K) \triangleleft \bar{G}$. If $K \triangleleft G$, then $G/K \simeq \bar{G}/\kappa(K)$. (If $\kappa(K)$ is written K/N , then the isomorphism may be formulated as follows: $G/K \simeq (G/N)/(K/N)$.)*

Proof Omitted \square

1.10 Cyclic groups

Definition 1.72 A group G is called *cyclic* if $G = \langle a \rangle$ for some $a \in G$. A generator for G is by definition an element $b \in G$ such that $G = \langle b \rangle$.

Remark 1.73 If the cyclic group $G = \langle a \rangle$ is finite of order n , then a^m is a generator of G if and only if $(n, m) = 1$. This follows easily from Theorem 1.21(3).

Exercise 1.74 Show that an abelian group is simple if and only if it is a cyclic group of prime order. Hint: You may start by using Remark 1.43 to show that a simple abelian group is cyclic.

Theorem 1.75 *A subgroup of a cyclic group is again cyclic. More precisely: If $H \neq \{e\}$ is a subgroup of $G = \langle a \rangle$, and if $k \in \mathbb{N}$ is minimal with respect to the property $a^k \in H$ then $H = \langle a^k \rangle$.*

Proof Suppose that $H \neq \{e\}$ is a subgroup of $G = \langle a \rangle$. Then there exists a $t \neq 0$ such that $a^t \in H$. Since also $a^{-t} \in H$ we may assume that $t \in \mathbb{N}$. Let $k \in \mathbb{N}$ be minimal with respect to the property $a^k \in H$. Suppose that $a^t \in H$ and write $t = mk + r$ where $0 \leq r < k$. We get $a^r = a^t(a^{mk})^{-1} \in H$, using the power rules. By the minimality of k we get $r = 0$. Thus $a^t = a^{mk} \in \langle a^k \rangle$. (AT; p. 74). \square

Theorem 1.76 *Let $G = \langle a \rangle$ be a finite cyclic group of order n , Let r be a divisor of n . Then G has exactly one subgroup of order r , namely $\langle a^{n/r} \rangle$.*

Proof For $r = 1$ the result is trivial. Suppose $r > 1$. Write $n = rs$. By Theorem 1.21 (1) $K = \langle a^{n/r} \rangle = \langle a^s \rangle$ has order r . Let H be a subgroup of G of order r and let $s' \in \mathbb{N}$ be minimal with $a^{s'} \in H$. Then $H = \langle a^{s'} \rangle$, by Theorem 1.75. By Theorem 1.21 (3) we get $r = n/(n, s')$, such that $s = (n, s')$. This forces $s \mid s'$ and thus $H \subseteq K$, ie. $H = K$. \square

The next example does not really tell us something, we do not already know, eg. from Example 1.52. We use here however the word “classification”. To “classify” groups with a certain given property means that you provide a fixed list of non-isomorphic groups and then show that *any* group with the given property is isomorphic to a group from the list. Thus you exhibit one group from each isomorphism class (See Remark 1.60.) A famous example of this is the classification of the finite simple groups, which goes far beyond these notes. In a later section we give more examples of classifications.

Example 1.77 (THE CLASSIFICATION OF CYCLIC GROUPS) Suppose that $G = \langle a \rangle$ is a cyclic group. Consider the map $\phi : \mathbb{Z} \rightarrow G$ defined by $\phi(n) = a^n$. The power rules (Remark 1.16) shows that this is a homomorphism from $(\mathbb{Z}, +)$ to G . Since $G = \langle a \rangle$ it is an epimorphism. The kernel of ϕ is a subgroup of \mathbb{Z} and thus have the form $k\mathbb{Z}$ for some $k \geq 0$, by Theorem 1.75. If $k = 0$ then ϕ is an isomorphism and G is infinite. Otherwise by the previous theorem k is the order of G . The homomorphism theorem shows that $G \simeq \mathbb{Z}/k\mathbb{Z}$. Thus any cyclic group is isomorphic to one of the groups $\mathbb{Z}/k\mathbb{Z}$, $k \geq 0$. We refer to this cyclic group as C_k , when $k > 1$. In the literature it is often denoted \mathbb{Z}_k .

We now illustrate a connection between elementary number theory and group theory.

Definition 1.78 (EULER'S φ -FUNCTION, TOTIENT FUNCTION) We define $\varphi : \mathbb{N} \rightarrow \mathbb{N}$ as follows: $\varphi(n)$ is the number of integers r with $1 \leq r \leq n$ and $(n, r) = 1$. This is Euler's φ -function, which is also called the totient function. (AT; p. 34, 44)

Remark 1.79 The number of elements of order n in a cyclic group of order n is $\varphi(n)$. This fact follows again from Theorem 1.21(3). It is used to prove the next Theorem, which plays a rôle in Chapter IV.

Theorem 1.80 For $n \in \mathbb{N}$ we have

$$n = \sum_{k|n} \varphi(k).$$

Proof We list the orders of the n elements in a cyclic group G of order n . Each such element has an order k dividing n . An element of order k generates the (unique) subgroup of order k in G . (Theorem 1.76). The number of elements of order k in G is therefore $\varphi(k)$, by the previous remark. \square

Here is a perhaps surprising result:

Theorem 1.81 Let G be a finite group. Suppose that for any $k \in \mathbb{N}$ the equation $x^k = e$ has at most k solutions in G . Then G is cyclic.

Proof For $k \mid n = |G|$, let $s(k)$ be the number of elements of order k in G . Clearly

$$n = \sum_{k|n} s(k).$$

If $s(k) \neq 0$ and $a \in G$ has order k then the elements in $\langle a \rangle$ are solutions to the equation $x^k = e$ in G . By assumption there are no more solutions to this equation in G . Thus $s(k) = \varphi(k)$ by Remark 1.79. We have thus shown that for $k \mid n$ we have $s(k) \leq \varphi(k)$. Thus

$$n = \sum_{k|n} s(k) \leq \sum_{k|n} \varphi(k) = n$$

by Theorem 1.80. This is only possible when $s(k) = \varphi(k)$ for all $k \mid n$. In particular $s(n) = \varphi(n) \neq 0$. Thus G has an element of order n . \square

This Theorem has an interesting application in the theory of fields. (See (AT; Chapter RNG and POL) or Chapter II of these notes for some basic facts about fields and polynomials).

Theorem 1.82 Let G be a finite subgroup of the multiplicative group K^* of a field K . Then G is cyclic.

Proof (See also (AT; p. 240)) Suppose that $|G| = n$. Let $k \in \mathbb{N}$. The solutions to $x^k = e$ in G are all roots of the polynomial $x^k - 1 \in K[X]$. But a polynomial of degree k over a field has at most k roots. Thus the number of solutions to $x^k = e$ in G is at most k . Apply Theorem 1.81 to get that G is cyclic. \square

1.11 Conjugation. The class equation

Definition 1.83 Let S be a subgroup of G . We call two subsets X and Y of G *S-conjugate* if there exists an $a \in S$ such that $Y = k_a(X)$, ie. $Y = \{aga^{-1} | g \in X\}$. We then write $X \sim_S Y$. Clearly \sim_S is an equivalence relation on the subsets of G . The subsets in the \sim_S -class of X are called the *S-conjugates* of X and the set of *S-conjugates* of X is referred to as the *S-conjugacy class* of X . We are primarily (but not always!) interested in the important case where $S = G$. We refer to *G-conjugates* and *G-conjugacy classes* simply as *conjugates* / *conjugacy classes*, omitting the G .

Example 1.84 Let $\kappa, \sigma \in S_n$ with $\sigma = (i_1, i_2, \dots, i_r)(j_1, j_2, \dots, j_s) \dots (k_1, k_2, \dots, k_t)$. Then the $\kappa\sigma\kappa^{-1}$ has the cycle decomposition (see Remark 1.7)

$$(\kappa(i_1), \kappa(i_2), \dots, \kappa(i_r)) (\kappa(j_1), \kappa(j_2), \dots, \kappa(j_s)) \dots (\kappa(k_1), \kappa(k_2), \dots, \kappa(k_t))).$$

Thus two elements σ_1, σ_2 of S_n are conjugate if and only if they have the same cycle type: $ct(\sigma_1) = ct(\sigma_2)$. (*Definition 1.8*.)

Definition 1.85 Let $X \subseteq G$, and S a subgroup of G . We define the *normalizer* $N_S(X)$ of X in S by

$$N_S(X) = \{a \in S \mid aXa^{-1} = X\}$$

and the *centralizer* $C_S(X)$ of X in S by

$$C_S(X) = \{a \in S \mid aga^{-1} = g \text{ for all } g \in X\}.$$

Trivially $N_S(X)$ and $C_S(X)$ are subgroups of S satisfying $C_S(X) \subseteq N_S(X)$. In the special case where $X = \{g\}$ has only one element, clearly $N_S(X) = C_S(X)$. This subgroup is denoted $C_S(g)$, the centralizer of g in S .

Remark 1.86 If X is a subgroup of G then $N_G(X)$ is the *largest* subgroup of G with $X \triangleleft G$. This is an immediate consequence of the definition.

Exercise 1.87 Let $X \subseteq G$, and S a subgroup of G . Show that $C_S(X) \triangleleft N_S(X)$.

Theorem 1.88 Let $X \subseteq G$ and S a subgroup of G . The number of different *S-conjugates* of X equals $|S : N_S(X)|$.

Proof The *S-conjugates* of X have the form aXa^{-1} , $a \in S$. Moreover for $a, b \in S$ we have

$$aXa^{-1} = bXb^{-1} \iff (b^{-1}a)X(b^{-1}a)^{-1} = X \iff b^{-1}a \in N_S(X) \iff aN_S(X) = bN_S(X).$$

This argument is a special case of something more general, the Orbit formula (Theorem 1.141) (AT; p. 112-116) \square

An element a is in $Z(G)$ (Definition 1.66) exactly when it is only conjugate to itself. We compute the center of a symmetric group:

Theorem 1.89 *If $n \geq 3$ then $Z(S_n) = \{e\}$.*

Proof An element of $\sigma \in S_n$ is always conjugate to its inverse since σ and σ^{-1} have the same cycle type. (Use Example 1.84.) Thus only elements of order 1 or 2 can be central, since a central element is conjugate only to itself. But for any $k \geq 1$, $k \leq \frac{n}{2}$ there is more than one element in S_n which is a product of k 2-cycles. \square

Lemma 1.90 *Let g_1, g_2, \dots, g_k be a set of representatives for the conjugacy classes of elements in the finite group G . (Exactly one element from each conjugacy class.) Then*

$$|G| = \sum_{i=1}^k |G : C_G(g_i)|.$$

Proof The number of elements in the conjugacy class containing g_i is $|G : C_G(g_i)|$, by Theorem 1.88. Since each element of G is in exactly one conjugacy class (\sim_G -equivalence class), the result follows. \square

There is a reformulation of the above lemma using the center of G . As already mentioned, a central elements form a conjugacy class by itself. Thus we have:

Theorem 1.91 (THE CLASS EQUATION) *Let g_1, g_2, \dots, g_l be a set of representatives for the conjugacy classes of non-central elements in the finite group G . Then*

$$|G| = |Z(G)| + \sum_{i=1}^l |G : C_G(g_i)|.$$

The class equation is in some cases quite useful. The following is an easy application of it (AT; p. 118):

Definition 1.92 *Let p be a prime. A p -group is a group G , whose order is a power of p .*

Theorem 1.93 *Suppose that $|G| = p^a$ for some prime number p and $a \geq 1$, ie. a non-trivial p -group. Then $Z(G) \neq \{e\}$.*

Proof It is enough to show $p \mid |Z(G)|$. In the class equation of Theorem 1.91 the summands $|G : C_G(g_i)|$, satisfy $1 \neq |G : C_G(g_i)|$, since g_i is noncentral. Also $|G : C_G(g_i)| \mid |G| = p^a$, by Lagranges theorem. Thus $p \mid |G : C_G(g_i)|$, implying $p \mid \sum_{i=1}^l |G : C_G(g_i)|$. Since also $p \mid |G|$ we get $p \mid |Z(G)|$. \square

Corollary 1.94 *Suppose that $|G| = p^2$ for some prime number p . Then G is abelian.*

Proof Suppose not. Then $Z(G) \neq G$ and we get $|Z(G)| = p$, by Theorem 1.93. Then $G/Z(G) \simeq C_p$. Therefore, if $a \in G \setminus Z(G)$ then any element in G may be written on the form $a^i z$, $z \in Z(G)$ (since $G/Z(G) = \langle \bar{a} \rangle$.) But any two elements on this form commutes. \square

Theorem 1.95 Suppose that $|G| = p^n$ for some prime number p and $n \geq 0$. Then G contains series of normal subgroups

$$G_n = \{e\} \subset G_{n-1} \subset \dots \subset G_1 \subset G = G_0.$$

where for all i , $0 \leq i \leq n-1$ we have $|G_i : G_{i+1}| = p$. In particular, G contains a normal subgroup of order p^k for $k = 0, \dots, n$. (AT; p. 118)

Proof We use induction on n . There is nothing to prove for $n = 1$. Assume $n \geq 2$. By Theorem 1.93 we may find an element a of order p in $|Z(G)|$ (a suitable power of an element $\neq e$ in $Z(G)$.) Then trivially $G_{n-1} = \langle a \rangle \triangleleft G$, so the result is true for $m = 1$. By the induction hypothesis the factor group $\overline{G} = G/\langle a \rangle$ of order p^{n-1} contains a normal series

$$\overline{G}_{n-1} = \{e\} \subseteq \overline{G}_{n-2} \subseteq \dots \subseteq \overline{G}_1 \subseteq \overline{G} = \overline{G}_0$$

of subgroups of order p^m , $0 \leq m \leq n-1$. By Noethers second isomorphism theorem 1.71 a normal subgroup of order p^m in \overline{G} corresponds to a normal subgroup of order p^{m+1} in G . \square

Exercise 1.96 Suppose that $G/Z(G)$ is a cyclic group. Show that G is abelian.

1.12 Characteristic subgroups

A subgroup N of G is normal in G , if and only if it is invariant under all inner automorphisms, i.e. $k_a(H) \subseteq H$ for all $a \in G$. (See Remark 1.42(i)). This means $\phi(H) \subseteq H$ for all $\phi \in \text{Aut}_i(G)$ and is a motivation for the following:

Definition 1.97 A subgroup N of G is called *characteristic* in G , if $\phi(H) \subseteq H$ for all $\phi \in \text{Aut}(G)$. Equivalently $\phi(H) = H$ for all $\phi \in \text{Aut}(G)$. We then write $N \text{ char } G$.

Lemma 1.98 Let M, N be subgroups of G . We have

- (1) $M \text{ char } G \Rightarrow M \triangleleft G$. The converse is not true.
- (2) $M \text{ char } N \triangleleft G \Rightarrow M \triangleleft G$.
- (3) $M \text{ char } N \text{ char } G \Rightarrow M \text{ char } G$.

Proof (1): This is trivial from the definition.

(2): Assume $M \text{ char } N \triangleleft G$ and let $a \in G$ be arbitrary. We need to show $aMa^{-1} = M$. We know that $k_a(N) = N$ since $N \triangleleft G$. Thus the restriction ϕ of k_a to N , defined by $\phi(n) = ana^{-1}$, $n \in N$ is an automorphism of N . Since $M \text{ char } N$ we get $aMa^{-1} = \phi(M) = M$.

(3): Assume $M \text{ char } N \text{ char } G$ and let $\phi \in \text{Aut}(G)$ be arbitrary. We need to show $\phi(M) = M$. Since $N \text{ char } G$ the restriction ϕ' of ϕ to N is an automorphism of N . Since $M \text{ char } N$ we get now $\phi(M) = \phi'(M) = M$. \square

Exercise 1.99 Let M, N be subgroups of G . Give examples to show that the following statements are FALSE:

- (1) $M \triangleleft G \Rightarrow M \text{ char } G$.
- (2) $M \triangleleft N \triangleleft G \Rightarrow M \triangleleft G$.
- (3) $M \triangleleft N \text{ char } G \Rightarrow M \triangleleft G$.

Example 1.100 If H is any subgroup of the finite *cyclic* group G , then $H \text{ char } G$. Indeed we have seen (Theorem 1.76) that H is the unique subgroup of order $|H|$ in G . Thus $\phi(H) = H$ for all $\phi \in \text{Aut}(G)$.

Exercise 1.101 Show that $Z(G) \text{ char } G$ (eg. using Exercise 1.64)

The following may be quite useful to show that a subgroup is characteristic:

Lemma 1.102 Let A be a subset of the group G . Suppose that $\phi(A) \subseteq A$ for all $\phi \in \text{Aut}(G)$. If $H = \langle A \rangle$, then $H \text{ char } G$.

Proof This follows easily from the explicit description of the elements in $\langle A \rangle$ in Remark 1.22. If you apply an automorphism ϕ to such an element you get an element of the same type (with $a_i \in A$ replaced by $\phi(a_i) \in A$). \square

Lemma 1.103 Suppose that $|G| = mn$, where m and n are relatively prime. Let $N \triangleleft G$, $|N| = n$. Then $N = \{a \in G \mid |a| \mid n\}$. In particular $N \text{ char } G$.

Proof Let $X = \{a \in G \mid |a| \mid n\}$. Then clearly $N \subseteq X$ (eg. by Corollary 1.35). Let $a \in X$ and consider $\bar{a} \in \bar{G} = G/N$. Then $|\bar{a}| \mid m = |\bar{G}|$. On the other hand $|\bar{a}| \mid |a| \mid n$ by Remark 1.53. We get $|\bar{a}| = 1$, since $(m, n) = 1$ ie. $\bar{a} = e$ or $a \in N$. By Lemma 1.102 we see $N \text{ char } G$. (Exercise 1.56). \square

Definition 1.104 The *commutator subgroup* $G^{(1)}$ of G is the subgroup of G generated by the set of all commutators $[a, b] = aba^{-1}b^{-1}$ of elements $a, b \in G$. (Definition 1.5)

Corollary 1.105 We have $G^{(1)} \text{ char } G$, where $G^{(1)}$ is the commutator subgroup of G .

Proof If $\phi \in \text{Aut}(G)$ and $[a, b]$ is a commutator then $\phi([a, b]) = [\phi(a), \phi(b)]$ is another commutator. Apply Lemma 1.102. \square

1.13 The automorphism group of a cyclic group

Example 1.106 Let $G = \langle a \rangle$ be a cyclic group of finite order n so that $G \simeq C_n$. (Example 1.77) We want to describe $\text{Aut}(G)$. Let ϕ be a homomorphism $\phi : G \rightarrow G$. Then ϕ is uniquely determined by the value $\phi(a)$, since for all $r \in \mathbb{Z}$ we have $\phi(a^r) = \phi(a)^r$. We may thus assume $\phi(a) = a^m$ for a unique $m \in \{0, 1, \dots, n-1\}$. Then $\text{Im}(\phi) = \langle a^m \rangle$ and $|\text{Im}(\phi)| = n/(n, m)$ by Theorem 1.21. Thus

$$\phi \in \text{Aut}(G) \iff \phi \text{ is surjective} \iff (n, m) = 1.$$

An automorphism $\phi \in \text{Aut}(G)$ uniquely determines an element $\alpha(\phi)$ in the Residue class group $\mathbb{Z}/n\mathbb{Z}$. The map α is as follows: If $\phi(a) = a^m$ then $\alpha(\phi) = \bar{m}$, using the bar notation for $\mathbb{Z}/n\mathbb{Z}$. Note that the power a^m does not depend on the choice of $m \in \bar{m}$. Note also that $(m, n) = 1$ for any $m \in \bar{m}$. Thus \bar{m} is a so-called prime residue class modulo n . (AT; p. 43-44). Moreover $\alpha(\phi \circ \psi) = \alpha(\phi)\alpha(\psi)$. This shows that $\text{Aut}(G)$ is isomorphic to the multiplicative group of prime residue class modulo n . Thus $|\text{Aut}(G)| = \varphi(n)$ where φ is Euler's φ -function. (Definition 1.78 above, AT, p. 43-44).

The prime order case is going to be important later:

Theorem 1.107 Let p be a prime number. Then $\text{Aut}(C_p)$ is a cyclic group of order $p-1$.

Proof The residue class ring $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is a field with p elements. (AT; p. 180. See also Chapter II of these notes.) By Example 1.106 $\text{Aut}(C_p)$ is isomorphic to the multiplicative group of \mathbb{F}_p . This group is cyclic by Theorem 1.82. \square

1.14 Sylow's theorems

The perhaps most important tool to study finite groups are the amazing theorems of Sylow. A subgroup H of a finite group G satisfies $|H| \mid |G|$. You may ask: If $m \mid |G|$, does G necessarily contain a subgroup of order m ? The answer is yes, if m is a power of a prime. Generally the answer is no: A counterexample of small order is $G = A_4$ of order 12, which does not contain a subgroup of order 6.

Definition 1.108 Let G be a finite group, p a prime. A subgroup P of G is called a p -subgroup, if $|P| = p^n$ for some $n \geq 0$. If in addition $p \nmid |G : P|$ then P is called a p -Sylow subgroup. In that case $|G| = p^n r$, where $p \nmid r$. Let us note that (although it is quite uninteresting) the case $p \nmid |G|$ is covered by this definition! We have $n = 0$ and the trivial subgroup $\{e\}$ is a p -Sylow subgroup of G .

We proceed to prove Sylow's theorems. The proofs are essentially different from the ones in (AT; p. 127-128).

Lemma 1.109 *Let G be a finite abelian group, p a prime. If $p \mid |G|$, then G contains an element of order p .*

Proof We use induction on $|G|$. The result is clear for $|G| = 1, 2, 3$ (Remark 1.37.) Let $a \in G$, $a \neq 1$. Suppose first that $p \mid |a|$. Then a power of a has order p by Theorem 1.21 (1) and we are done. Suppose next that $p \nmid |a| = k$. Since G is abelian $\langle a \rangle \triangleleft G$. By the induction hypothesis there is an element \bar{b} of order p in the factor group $\bar{G} = G/\langle a \rangle$. (Note that by Lagrange's Theorem 1.33 $p \mid |\bar{G}|$.) Choose an element $b \in \bar{b}$. Then $p \mid |b|$, by Remark 1.53. As before, a power of b has order p . \square

Theorem 1.110 (SYLOW'S FIRST THEOREM) *Let G be a finite group, p a prime. Then G contains a p -Sylow subgroup.*

Proof We use induction on $|G|$. The result is trivial for $|G| = 1, 2, 3$. We may assume $p \mid |G|$. (See Definition 1.108) Suppose first that G contains a subgroup $H \neq G$ such that $p \nmid |G : H|$. Then we may apply the induction hypothesis to H . Since $p \nmid |G : H|$, a p -Sylow subgroup of H is also a p -Sylow subgroup of G . Therefore we may assume that for *all* subgroups $H \neq G$ we have $p \mid |G : H|$. In the class equation (Theorem 1.91) we see then that all summands $|G : C_G(g_i)|$ (g_i noncentral) are divisible by p . Since $p \mid |G|$ we conclude $p \mid |Z(G)|$. By Lemma 1.109 we may find an element $a \in Z(G)$ of order p . Since $\langle a \rangle \triangleleft G$ (see a note in Definition 1.66) we may apply the induction hypothesis to $\bar{G} = G/\langle a \rangle$. If \bar{P} is a p -Sylow subgroup of \bar{G} , then the corresponding subgroup P of G (using Noether's Theorem 1.71) is a p -Sylow subgroup of G . \square

Definition 1.111 Let p be a prime. The set of p -Sylow subgroups of a finite group G is denoted $\text{Syl}_p(G)$. It is always non-empty. Also define $m_p(G) = |\text{Syl}_p(G)|$, the number of p -Sylow subgroups of G .

Corollary 1.112 *Let G be a finite group, p a prime. If $p^n \mid |G|$ for some $n \geq 0$ then G contains a subgroup of order p^n . In particular, if $p \mid |G|$, then G contains an element of order p .*

Proof A p -Sylow subgroup of G contains a subgroup of order p^n , eg. by Corollary 1.95. This is also a subgroup of G . \square

Lemma 1.113 *Let $P \in \text{Syl}_p(G)$. Any p -subgroup Q of $N_G(P)$ is contained in P .*

Proof By Remark 1.86 $P \triangleleft N_G(P)$. Also $|P|$ and $|N_G(P) : P|$ are relatively prime, since $|N_G(P) : P| \mid |G : P|$ and $p \nmid |G : P|$. Apply Lemma 1.103. \square

Corollary 1.114 *Let $P \in \text{Syl}_p(G)$. Then $P \text{char} N_G(P)$. In particular, $P \triangleleft G \Rightarrow P \text{char} G$.*

Proof If $\phi \in \text{Aut}(N_G(P))$ then $\phi(P) = P$, by the previous Lemma 1.113. If $P \triangleleft G$, then $G = N_G(P)$. \square

The reader is advised that the next proof is slightly tricky.

Theorem 1.115 (SYLOW'S SECOND THEOREM) *Let G be a finite group, p a prime. All p -Sylow subgroups of G are conjugate in G (Definition 1.83). Any p -subgroup of G is contained in a p -sylow subgroup of G .*

Proof If $P \in \text{Syl}_p(G)$ and $a \in G$ then also $k_a(P) = aPa^{-1} \in \text{Syl}_p(G)$, since $|P| = |aPa^{-1}|$.

Let \mathcal{X}_P be the set of (G -)conjugates to a fixed $P \in \text{Syl}_p(G)$. (Definition 1.83.) By Theorem 1.88 $|\mathcal{X}_P| = |G : N_G(P)|$.

Let S be a arbitrary p -subgroup of G . It is enough to show that S is contained in some $Q \in \mathcal{X}_P$: This will imply that *any* p -subgroup of G is conjugate to a subgroup of P .

Clearly \mathcal{X}_P is a union of S -conjugacy classes of subsets (subgroups) of G . The number of S -conjugates of $Q \in \mathcal{X}_P$ is $|S : N_S(Q)|$, again by Theorem 1.88. Now $N_S(Q)$ is a p -subgroup of $N_G(Q)$, and $Q \in \text{Syl}_p(G)$, so that $N_S(Q) \subseteq Q$, by Lemma 1.113. We then get easily $N_S(Q) = S \cap Q$. We now get an equation

$$(*) \quad |G : N_G(P)| = |\mathcal{X}_P| = \sum_i |S : S \cap Q_i|$$

where we have chosen one representative Q_i for each S -conjugacy class of \mathcal{X}_P . Since S is a p -group all summands $|S : S \cap Q_i|$ are powers of p , possibly $p^0 = 1$. In fact, since $p \nmid |G : P|$ we get $p \nmid |G : N_G(P)|$. Therefore at least one $|S : S \cap Q_i|$ is not divisible by p , ie. $|S : S \cap Q_i| = 1$. We conclude $S \subseteq Q_i$, as desired. \square

Remember that $m_p(G)$ is the number of p -Sylow subgroups of G .

Corollary 1.116 *Let G be a finite group, p a prime, $P \in \text{Syl}_p(G)$. Then $m_p(G) = |G : N_G(P)|$.*

Proof Theorem 1.115 and Theorem 1.88. \square

The idea in the proof of Theorem 1.115 is also used in the next proof.

Theorem 1.117 (SYLOW'S THIRD THEOREM) *Let G be a finite group, p a prime. We have that $m_p(G)$ is a divisor of $|G|$ and that $m_p(G) \equiv 1 \pmod{p}$, ie $p \mid (m_p(G) - 1)$.*

Proof The first statement follows from Corollary 1.116 and Lagranges theorem. The equation (*) above may be applied to $S = P$. We are then considering the P -conjugacy classes of \mathcal{X}_P , which we know is equal to $\text{Syl}_p(G)$. Thus (*) may be formulated like this:

$$(**) \quad m_p(G) = \sum_i |P : P \cap Q_i|$$

where we have chosen one representative Q_i for each P -conjugacy class of $\text{Syl}_p(G)$. A summand $|P : P \cap Q_i|$ is divisible by p unless $P = P \cap Q_i$. This equality is only possible for $Q_i = P$. It follows that $m_p(G) \equiv 1 \pmod{p}$, as desired. \square

Note that Corollary 1.116 put further restriction on $m_p(G)$, than stated in Theorem 1.117: $m_p(G) \mid |G : P|$, if $P \in \text{Syl}_p(G)$.

We illustrate the “method of counting elements” in the study of groups of a given order:

Example 1.118 A group of G order $105 = 3 \cdot 5 \cdot 7$ is not simple. In fact we claim that either $m_5(G) = 1$ or $m_7(G) = 1$. so that one of the Sylow subgroups of G is normal in G . We know that $m_7(G) \mid 15$. If $m_7(G) > 1$ then $m_7(G) = 15$. (It cannot be 3 or 5 by Theorem 1.117.) Since two different 7-Sylow groups have only the element e in common, we see that G contains $15(7-1)=90$ elements of order 7. Similarly, if $m_5(G) > 1$ we get $m_5(G) = 21$ and thus $21(5-1)=84$ elements of order 5. We than have $90 + 84 > 105$ elements of order 5 or 7, a contradiction.

Exercise 1.119 Let G be a finite group, p a prime. A p -element in G is an element of order p^i for some $i \geq 0$. Let $P \in \text{Syl}_p(G)$. Then the following statements are equivalent:

- (i) The set of p -elements in G form a subgroup of G
- (ii) $P \triangleleft G$.
- (iii) P char G
- (iv) $m_p(G) = 1$.

Exercise 1.120 Show that a *finite* abelian group is cyclic if and only if its p -Sylow subgroups are cyclic for all primes p .

The following definition will be important later:

Definition 1.121 If $|G| = p^k m$ where $p \nmid m$ then a normal subgroup N of G of order m is called a *normal p -complement* in G . In that case we have (using Lemma 1.39) that if $P \in \text{Syl}_p(G)$, then $G = NP$ and $N \cap P = \{e\}$.

Remark 1.122 By Lemma 1.103 a normal p -complement N in G is a characteristic subgroup of G .

1.15 Direct products. Abelian groups

It will be important later to decide whether a Galois group of an extension is isomorphic to a group we already know. In that connection it may be useful to show that it is (isomorphic to) a direct or semidirect product of smaller groups. Semidirect products are treated in Section 1.19.

Definition 1.123 Let H, K be groups. The cartesian product $H \times K$ of H and K is a group using componentwise composition: $(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2)$ for $a_1, a_2 \in H, b_1, b_2 \in K$. This new group is called *the outer direct product* of H and K and is also denoted $H \times K$.

How can you recognize from the inside of a group G that it is isomorphic to an outer direct product? Here is the answer!

Theorem 1.124 Suppose that H and K are subgroups of G satisfying

- (i) $G = HK$
- (ii) $H \triangleleft G, K \triangleleft G$
- (iii) $H \cap K = \{e\}$.

Then $G \simeq H \times K$.

Proof Suppose that $a \in H, b \in K$. Consider the *commutator* $x = aba^{-1}b^{-1}$ of a and b . Writing $x = a(ba^{-1}b^{-1})$ we get $x \in H$, since by (ii) we have $(ba^{-1}b^{-1}) \in H$. Similarly writing $x = (aba^{-1})b^{-1}$ we get $x \in K$. By (iii) we get $x = e$. It follows that

$$(*) \quad ab = ba \text{ for all } a \in H, b \in K$$

Consider the map $\phi : H \times K \rightarrow G$ defined by $\phi(a, b) = ab$. The equation (*) shows that ϕ is a homomorphism. We use Lemma 1.58. Condition (i) shows that $\text{Im}(\phi) = G$. Suppose that $(a, b) \in \text{Ker}(\phi)$ for some $(a, b) \in H \times K$. Then $ab = e$ or $a = b^{-1}$. Thus $a \in H \cap K = \{e\}$. We get $a = b = e$. Thus ϕ is an isomorphism. \square

Definition 1.125 When the conditions (i)-(iii) of Theorem 1.124 are satisfied we call G is an *inner direct product* of H and K . Moreover H, K are called *direct factors* of G .

The simplest non-trivial example of an inner direct product is the Vierergruppe V (Example 1.24). The subgroups of order 2 are isomorphic to C_2 . Choosing H, K to be any two of these subgroups then (i)-(iii) of Theorem 1.124 are satisfied, so that $V \simeq C_2 \times C_2$.

Since inner and outer direct products are isomorphic we often omit the words inner/outer.

Remark 1.126 The above may be extended to 3 or more groups. If H_1, H_2, \dots, H_n are groups it is obvious how to define the group $H_1 \times H_2 \times \dots \times H_n$. The conditions of Theorem 1.124 have to be like this for subgroups H_i of G :

- (i) $G = H_1H_2\dots H_n$

(ii) $H_i \triangleleft G$, $1 \leq i \leq n$

(iii) $H_i \cap (H_1 H_2 \dots H_{i-1} H_{i+1} \dots H_n) = \{e\}$, $1 \leq i \leq n$.

We may then deduce $G \simeq H_1 \times H_2 \times \dots \times H_n$. Note that (iii) is stronger than you might expect. The condition (iii)' $H_i \cap H_j = \{e\}$ for all $i \neq j$ is not enough!! Indeed, the 3 subgroups of order 2 in the Vierergruppe V provide a counterexample. They satisfy (i),(ii),(iii)', but the Vierergruppe has order 4, not 8.

Example 1.127 Let $G = \langle a \rangle$ be a cyclic group of finite order n . Suppose that $n = qr$ where q and r are relatively prime: $(q, r) = 1$. Then there exist $k, l \in \mathbb{Z}$ with $kq + lr = 1$. Let $H = \langle a^r \rangle, K = \langle a^q \rangle$. By Theorem 1.21 $|H| = q, |K| = r$. Then (i)-(iii) of Theorem 1.124 are satisfied, (iii) because $(q, r) = 1$, (ii) because G is abelian and (i) by Lemma 1.39. We conclude $C_n \simeq C_q \times C_r$. In the case where $q = p^k$ is the power of a prime we see: If $p \mid n$ then $C_n \simeq C_{p^k} \times C_r$ so C_n is a direct product of a cyclic group of prime power order p^k and a cyclic group C_r of order prime to P . If we repeat this argument we get the following:

Lemma 1.128 *Any finite cyclic group is isomorphic to a direct product of cyclic groups of prime power order. (These direct factors are in fact the Sylow subgroups.)*

We finish this section by showing without proof the structure theorem for finite abelian groups (AT; p. 99-106), and giving the formula for the number of isomorphism classes of abelian groups of a given order.

Theorem 1.129 *Let G be a finite abelian group. There exist integers $m_1 \mid m_2 \mid \dots \mid m_k$, $m_1 > 1$, such that $G \simeq C_{m_1} \times C_{m_2} \times \dots \times C_{m_k}$. The integers determine G up to isomorphism. This means the following: If we also know that $G \simeq C_{n_1} \times C_{n_2} \times \dots \times C_{n_l}$ with $n_1 \mid n_2 \mid \dots \mid n_l$, $n_1 > 1$, then $k = l$ and $m_i = n_i$ for $i = 1, \dots, k$.*

Corollary 1.130 *Let p be a prime number, $n \in \mathbb{N}$. The number of isomorphism classes of abelian groups of order p^n equals the number $p(n)$ of cycle types of n . (Definition 1.8.)*

Proof By the Theorem an abelian group G of order p^n is isomorphic to $C_{m_1} \times C_{m_2} \times \dots \times C_{m_k}$ where each m_i has the form p^{c_i} and $c_1 \leq c_2 \leq \dots \leq c_k$ and $c_1 + \dots + c_k = n$. The c_i 's determine G up to isomorphism. If m_j is the number of c_i 's equal to j , then $(1^{m_1}, 2^{m_2}, \dots)$ is a cycle type of n . \square

Theorem 1.131 *Let G be a finite abelian group of order $n = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$ where the p_i 's are different primes and all $r_i > 0$. Then*

$$G \simeq P_1 \times \dots \times P_k$$

where each P_i is an abelian group of order $p_i^{r_i}$.

Proof This follows easily from the two previous results. \square

Corollary 1.132 Let $n = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$ where the p_i 's are different primes and all $r_i > 0$. The number of isomorphism classes of abelian groups of order n equals $p(r_1)p(r_2)\dots p(r_k)$.

Proof Two abelian groups G and H of order n are isomorphic if and only if their p_i -Sylow subgroups are isomorphic for $i = 1, \dots, k$. Indeed using Theorem 1.131 isomorphisms between the Sylow subgroups of G and H may be used to define an isomorphism between G and H . On the other hand if $G \simeq H$ then then their p_i -Sylow groups are isomorphic, eg. by Exercise 1.56 and Lemma 1.103. Now we apply Corollary 1.130 to get the result. \square

As an example the number of isomorphism classes of abelian groups of order $144 = 2^4 3^2$ equals $p(4)p(2) = 5 \cdot 2 = 10$.

You may find tables of the $p(r)$'s and a lot of information about them on the Internet. See <http://www.research.att.com/~njas/sequences/A000041>

1.16 Permutation groups

Definition 1.133 Let Ω be an arbitrary set ($\neq \emptyset$) and $S(\Omega)$ the set of all bijective maps of Ω onto Ω . Using composition of maps $S(\Omega)$ is a group. If Ω is finite, eg. $\Omega = \{1, 2, \dots, n\}$ then $S(\Omega)$ is isomorphic to the symmetric group S_n . See Exercise 1.134. A permutation group on Ω is simply a subgroup of $S(\Omega)$.

Exercise 1.134 Let Ω and Ω_1 be an arbitrary sets ($\neq \emptyset$) and $t : \Omega \rightarrow \Omega_1$ a bijection. Show that the map $\hat{t} : S(\Omega) \rightarrow S(\Omega_1)$ defined by $\hat{t}(\sigma) = t^{-1} \circ \sigma \circ t$ is an isomorphism. In particular, if $|\Omega| = n$, then $S(\Omega) \simeq S_n$.

Remark 1.135 If Ω is finite then any permutation of Ω may be written as a product of disjoint cycles, just as in the case of S_n . (Remark 1.7.) Here if $a_1, \dots, a_r \in \Omega$, the cycle (a_1, a_2, \dots, a_r) means that

$$a_1 \mapsto a_2, a_2 \mapsto a_3, \dots, a_{r-1} \mapsto a_r, a_r \mapsto a_1.$$

Therefore also the definition of cycle type and sign (Definition 1.8) may be carried over directly to $S(\Omega)$.

Exercise 1.136 Explain why the isomorphisms \hat{t} described in Exercise 1.134 preserve the cycle types of elements.

Definition 1.137 A permutation group G on Ω is called *transitive*, if for arbitrary (a, b) , $a, b \in \Omega$ there exists $\sigma \in G$ st. $\sigma(a) = b$.

Definition 1.138 A permutation group G on Ω is called *doubly transitive*, if for arbitrary $a, b, c, d \in \Omega$ $a \neq b$ and $c \neq d$ there exists $\sigma \in G$ such that $\sigma(a) = c$ og $\sigma(b) = d$.

Clearly doubly transitive implies transitive.

Exercise 1.139 Suppose that G is a permutation group on the finite set Ω , $|\Omega| = n$. Suppose that G contains an n -cycle (Definition 1.135.) Show that G is transitive. Is G doubly transitive?

Definition 1.140 If G is a permutation on Ω then the action of G splits Ω up into disjoint subsets, called *orbits*. The orbit containing the element $a \in \Omega$ is $G.a = \{\sigma(a) \mid \sigma \in G\}$. The *stabilizer* of a in G is the subgroup of G defined by $G_a = \{\sigma \in G \mid \sigma(a) = a\}$.

There is a well-known important connection between orbits and stabilizers: (AT; p.114)

Theorem 1.141 (THE ORBIT FORMULA) *If G is a permutation on Ω , $a \in \Omega$ then*

$$|G.a| = |G : G_a|.$$

(This means that either both numbers are infinite or they are both finite and equal.)

Proof For $\sigma_1, \sigma_2 \in G$ we have

$$\sigma_1(a) = \sigma_2(a) \iff (\sigma_1^{-1}\sigma_2)(a) = a \iff \sigma_1^{-1}\sigma_2 \in G_a \iff \sigma_1 G_a = \sigma_2 G_a.$$

This shows that the map $\sigma G_a \mapsto \sigma(a)$ is a well-defined bijection between the right cosets of G_a in G and the elements in the orbit $G.a$. Further details may be found in (AT; p. 114-115). \square

Here are some results about doubly transitive permutation groups:

Theorem 1.142 *Let $N \neq \{e\}$ be a normal subgroup in a doubly transitive permutation group G on Ω . Then N is transitive.*

Proof Let $a, b \in \Omega$, $a \neq b$. We want to find $\sigma \in N$ with $\sigma(a) = b$. As $N \neq \{e\}$ there exists $c \neq d$ in Ω with $\tilde{\sigma}(c) = d$ for some $\tilde{\sigma} \in N$. As G is doubly transitive, there exists $\tau \in G$ with $\tau(c) = a$, $\tau(d) = b$. Then $\tau \tilde{\sigma} \tau^{-1}(a) = b$. Since $N \triangleleft G$ we get $\tau \tilde{\sigma} \tau^{-1} \in N$ ie. $\tau \tilde{\sigma} \tau^{-1}$ may be used as σ . \square

Theorem 1.143 *Let G be doubly transitive on Ω , where $|\Omega| > 1$. Then G_a is a maximal subgroup in G , ie. there are no subgroups lying properly between G_a and G .*

Proof Let H be a subgroup of G satisfying $G_a \subset H$. We want to show $H = G$. Since $G_a \neq H$ we may find $\tau \in H$ with $\tau(a) = b$, $b \neq a$. Let ρ be arbitrary in G . We show $\rho \in H$. Let $\rho(a) = c$. If $c = a$ then $\rho \in G_a \subset H$ and we are done. We may thus assume $c \neq a$. As G is doubly transitive, there exists $\sigma \in G$ with $\sigma(a) = a$, $\sigma(b) = c$. Thus $\sigma \in G_a$. Now $\sigma\tau(a) = c$ implies $\rho^{-1}\sigma\tau(a) = a$, ie. $\rho^{-1}\sigma\tau \in G_a \subseteq H$. As $\sigma, \tau \in H$, we get $\rho \in H$, as desired. \square

It is a basic fact that any group is realizable as a permutation group on the set of its elements (AT; p. 111). We have:

Theorem 1.144 (CAYLEY'S THEOREM) *Let G be an arbitrary group. Then there exists an injective homomorphism φ of G onto a transitive subgroup of $S(G)$. In particular, any group of finite order n is isomorphic to a transitive subgroup of the symmetric group S_n .*

Proof For $g \in G$ let φ_g be the following element in $S(G)$:

$$\varphi_g : a \mapsto ga, \quad a \in G.$$

Then φ_g is a bijective map on G , ie. φ_g is a well defined element in $S(G)$. The associativity of group multiplication shows that

$$\varphi_{g_1 g_2} = \varphi_{g_1} \circ \varphi_{g_2}.$$

Thus $\varphi : g \mapsto \varphi_g$ is a homomorphism of G into $S(G)$. Furthermore

$$\text{Ker}(\varphi) = \{g \in G \mid \varphi_g = \text{Id}_G\} = \{g \in G \mid ga = a \forall a \in G\} = \{e\}.$$

Thus φ is injective by Lemma 1.58. The image of G by φ is a transitive subgroup in $S(G)$. Indeed, if $a, b \in G$ are arbitrary, then $\varphi_g(a) = b$ for $g = ba^{-1}$. Finally $S(G) \simeq S_n$, by Exercise 1.134. \square

Remark 1.145 If $|G| = n$ and $g \in G$ then φ_g defined above is a permutation of G . We may describe the cycle structure of φ_g (Definition 1.135) explicitly! If $|g| = r$ then applying φ_g repeatedly to an element $a \in G$ we get the elements in the set $\{a, ga, g^2a, \dots, g^{r-1}a\}$. This shows that φ_g is a product of $|G|/r$ disjoint r -cycles! You may then also decide whether φ_g is an even or an odd permutation. An r -cycle is odd, if and only if r is even. (Definition 1.8.) Thus φ_g is odd if and only if $r = |g|$ is even and $|G|/r$ is odd.

Here is a perhaps surprising application of the remark.

Theorem 1.146 *Suppose that G has a cyclic 2-Sylow group P . Then G has a normal 2-complement N . (Definition 1.121)*

Proof Let $|G| = 2^k m$, m odd. (We may assume $k \geq 1$. Otherwise $G = N$.) Let $P = \langle h \rangle \in \text{Syl}_2(G)$. By Remark 1.145 the element φ_h is an odd permutation. Therefore the subgroup $G_1 = \{g \in G \mid \varphi_g \text{ is even}\}$ has index 2 in G . We use induction on k . If $k = 1$ we are done, since G_1 is then a normal 2-complement. If $k > 1$ and the result has been shown up to $k - 1$ we see that G_1 must have a normal 2-complement N , since its 2-Sylow subgroup is cyclic of order 2^{k-1} . (Why?) Using Remark 1.122 and Lemma 1.98(2) we get that N is a normal 2-complement in G . \square

Corollary 1.147 *If $|G| = 2n$, n odd, then G has a normal subgroup of index 2 and order n .*

A generalization of Cayley's theorem for finite groups is sometimes useful:

Let H be a subgroup of G of index $|G : H| = n$, $n \in \mathbb{N}$, and let $G = \bigcup_{i=1}^n g_i H$ be the decomposition of G into disjoint right cosets of H . Let us assume $g_1 = e$. For each $g \in G$ we have that $G = \bigcup_{i=1}^n g g_i H$ is another decomposition of G into disjoint right cosets to H . Thus

$$\begin{pmatrix} g_1 H & g_2 H & \cdots & g_n H \\ g g_1 H & g g_2 H & \cdots & g g_n H \end{pmatrix}$$

is a permutation of the cosets $g_i H$, $1 \leq i \leq n$, and may thus be seen as an element in the symmetric group S_n . We define a map $\rho : G \rightarrow S_n$ by demanding that for all i , $1 \leq i \leq n$ we have $g \rho(g)(i) \in g g_i H$. (Thus $\rho(g)(i) = j$, if $g g_i H = g_j H$.) We check that $\rho(g)$ is in fact a permutation of $\{1, 2, \dots, n\}$: It is enough to show that $\rho(g)$ is injective: If $\rho(i) = \rho(i') = j$ then $g g_i H = g g_{i'} H = g_j H$, which forces $g_i H = g_{i'} H$ and thus $i = i'$.

In analogy with the proof of Cayley's theorem it is easily seen that ρ is a homomorphism and that $\rho(G)$ is a transitive subgroup of S_n . The order of $\rho(G)$ is then divisible by n by the orbit formula. Let us investigate the kernel of ρ . We have

$$g \in \text{Ker}(\rho) \iff \rho(g)(i) = i \text{ for all } i \iff g g_i H = g_i H \text{ for all } i \iff g \in \bigcap_{i=1}^n g_i H g_i^{-1}.$$

This shows that $\text{Ker}(\rho)$ is the largest normal subgroup of G , which is contained in H . (See Exercise 1.48).

We get now using the homomorphism theorem:

Theorem 1.148 *Suppose that G has a subgroup H of finite index $n = |G : H|$. Then G contains a normal subgroup N with the following properties:*

- (i) $N \subseteq H$. In particular $n \mid |G : N|$.
- (ii) The factor group G/H is isomorphic to a subgroup of the symmetric group S_n . In particular $|G : N| \mid n!$

If $H = \{e\}$ we obtain Cayley's theorem. Here are some applications:

Theorem 1.149 *Suppose that H is a subgroup of index 3 in G . Then either $H \triangleleft G$ or G has a normal subgroup of index 2.*

Proof By Theorem 1.148 G has a normal subgroup N , $N \subseteq H$ such that $3 \mid |G : N| \mid 3! = 6$. If $|G : N| = 3$ we get $N = H \triangleleft G$. If $|G : N| = 6$ then Theorem 1.148 shows that $G/N \simeq S_3$. Since A_3 is normal of index 2 in S_3 . By Noethers Theorem 1.71 G then has a normal subgroup of index 2. \square

Theorem 1.150 *If G has a proper subgroup H of index ≤ 4 then G is not simple unless G is cyclic of order 2 or 3.*

Proof A subgroup of index 2 is normal. By the previous theorem we may assume $|G : H| = 4$. By Theorem 1.148 G has a normal subgroup N such that G/N is isomorphic to a subgroup X of S_4 of order 4, 8, 12 or 24. If $|X|$ is 4, 8 or 24 then G has a proper normal subgroup by Theorem 1.93 or Example 1.69. If $X = A_4$ then G has a normal subgroup of index 3 corresponding to the Klein Vierergruppe in A_4 . Otherwise X contains an odd permutation and then the even permutations form a subgroup of index 2 in X . Noethers Theorem 1.71 gives us a normal subgroup of index 2 in G . \square

It is known that A_5 is a simple group of order 60 (AT; p. 131) and we are not going to present a proof of this fact. But using it we can show:

Theorem 1.151 *Let G be a simple group of order 60. Then $G \simeq A_5$.*

Proof Let G be simple, $|G| = 60$. We need only show that G has a subgroup of index 5. Then by Theorem 1.148 G is isomorphic to a subgroup H of order 60 in S_5 . If $H \neq A_5$ then $H \cap A_5$ is a subgroup of index 2 in A_5 (by Lemma 1.39), a contradiction.

The number $m_5(G)$ of 5-Sylow subgroups in G is 6 by Theorem 1.117, since it cannot be 1. We get then $6 \cdot (5 - 1) = 24$ elements of order 5 in G . The number $m_2(G)$ of 2-Sylow subgroups in G is 1, 3, 5 or 15. It cannot be 1 or 3 by the previous theorem and Corollary 1.116. If it is 5, we are done. So assume $m_2(G) = 15$. If any two different 2-sylow subgroups have only e in common we get $15 \cdot (4 - 1) = 45$ different 2-elements, too many since $24 + 45 > 60$. Suppose that $P_1 \cap P_2 = Q \neq \{e\}$, where $P_i \in \text{Syl}_2(G)$ and $|Q| = 2$. Let $C = C_G(Q)$, the centralizer. (Definition 1.85.) Clearly $P_1, P_2 \subseteq C$, so that $4 \mid |C| \neq 4$. We get $|C| = 12, 20$ or 60 . Only $|C| = 12$ is possible since G is simple, so C has index 5. \square

1.17 Chains of subgroups, composition series

Definition 1.152 We consider finite chains of subgroups of a group G as follows:

$$G_s = \{e\} \subseteq G_{s-1} \subseteq \dots \subseteq G_1 \subset G = G_0.$$

Such a chain is called a *normal series* for G , if $G_i \triangleleft G$ for all i , $0 \leq i \leq s$ and it is called a *subnormal series* for G , if $G_{i+1} \triangleleft G_i$ for all i , $0 \leq i \leq s-1$. In both cases we may for $1 \leq i \leq s$ consider the factor groups \overline{G}_i , defined by $\overline{G}_i = G_{i-1}/G_i$. The non-trivial factor groups (where $G_{i-1} \neq G_i$) are called the *factors* of the series.

The reader should be aware of the fact that in some texts on group theory subnormal series are referred to as normal series.

Definition 1.153 Consider two finite chains of subgroups of a group G :

$$(*) \quad G_s = \{e\} \subseteq G_{s-1} \subseteq \dots \subseteq G_1 \subseteq G = G_0$$

$$(**) \quad H_t = \{e\} \subseteq H_{t-1} \subseteq \dots \subseteq H_1 \subseteq G = H_0.$$

We call $(**)$ a *refinement* of $(*)$ if they are equal or if $(**)$ is obtained by adding some groups to $(*)$.

If H is a proper subgroup of G then the chain $\{e\} \subseteq H \subseteq G$ is a refinement of the chain $\{e\} \subseteq G$.

Definition 1.154 A *composition series* of G is a finite subnormal series with simple factors. Thus in the notation of Definition 1.152 there is no subgroup N with $G_{i+1} \subset N \subset G_i$ and $N \triangleleft G_i$. (This follows from Theorem 1.71.) The factors of a composition series are called *composition factors* of G .

As an example the chain in Theorem 1.95 is a composition series. The composition factors are cyclic groups of order p .

Exercise 1.155 Show that the group $(\mathbb{Z}, +)$ does not have a composition series.

Exercise 1.156 Let G be a finite group. Show that there exists a composition series for G .

Example 1.157 Let $G = \langle a \rangle$ be a cyclic group of order 6. Then G has two different composition series

$$\{e\} \subset \langle a^2 \rangle \subset G$$

with factors $G/\langle a^2 \rangle$ and $\langle a^2 \rangle$ of orders 2 and 3 and

$$\{e\} \subset \langle a^3 \rangle \subset G$$

with factors $G/\langle a^3 \rangle$ and $\langle a^3 \rangle$ of orders 3 and 2.

Definition 1.158 Two (sub)normal series of a group are called *equivalent* if they have the same number of composition factors and there is a bijection between the factors of the two series, such that the corresponding factors are isomorphic.

The two composition series in Example 1.157 are equivalent. (Just interchange the order of the composition factors). This is no coincidence. The equivalence follows from the *Jordan-Hölder theorem*, which we present now.

Theorem 1.159 (Jordan-Hölder) *Any two composition series of a group G are equivalent.*

This theorem follows from another result of Schreier:

Theorem 1.160 (Schreier) *Two (sub-)normal series of a finite group have refinements which are equivalent (sub-)normal series.*

We are not going to discuss the proofs of these theorems here. They are not really difficult (but it is easy to get lost in notational difficulties). They may be found in most books on group theory or in notes on group theory on the Internet.

1.18 Higher commutator subgroups. Solvable groups

In Definition 1.104 we defined the commutator subgroup $G^{(1)}$ of the group G as the subgroup generated by the commutators $[a, b]$ of elements $a, b \in G$. By Corollary 1.105 $G^{(1)}$ char G and in particular $G^{(1)} \triangleleft G$.

Proposition 1.161 *Let H be a normal subgroup of G . Then*

$$G/H \text{ is abelian} \iff G^{(1)} \subseteq H.$$

Thus $G^{(1)}$ is the smallest normal subgroup of G with abelian factor group.

Proof We use bar notation for the factor group $\overline{G} = G/H$. (Remark 1.51). We have that \overline{G} is abelian, if and only if all commutators $[\overline{a}, \overline{b}]$, $a, b \in G$ are trivial. Since $[\overline{a}, \overline{b}] = \overline{[a, b]}$ this is equivalent to that $[a, b] \in H$ for all $a, b \in G$. Since $G^{(1)}$ is generated by the commutators $[a, b]$, the result follows. \square

Remark 1.162 If the subgroup H satisfies $G^{(1)} \subseteq H \subset G$, then $H \triangleleft G$: Let us use bar notation for the factor group $\overline{G} = G/G^{(1)}$. Then we have that $\overline{H} = H/G^{(1)}$ is a subgroup of the abelian group $\overline{G} = H/G^{(1)}$ and thus it is normal in \overline{G} . By Noethers second isomorphism Theorem 1.71 we get $H \triangleleft G$.

Definition 1.163 We define the *higher commutator subgroups* $G^{(i)}$, $i \geq 0$ of the group G inductively as follows:

$$G^{(0)} = G, \quad G^{(i+1)} = [G^{(i)}, G^{(i)}], \quad i \geq 0$$

We refer to $G^{(i)}$ as the i 'th commutator subgroup of G . The commutator subgroup defined earlier is then just the first (1'th) commutator subgroup. Let us note that $G^{(i)} \triangleleft G$ for all i . We even have $G^{(i)}$ char G , by Corollary 1.105 and Lemma 1.98.

Definition 1.164 The group G is called *solvable*, if $G^{(r)} = \{e\}$ for some $r \geq 0$.

Theorem 1.165 A group G is solvable if and only if it has a subnormal series with abelian factors.

Proof If G is solvable then the chain of higher commutator subgroups subnormal series with abelian factors, by Proposition 1.161. On the other hand if $G_s = \{e\} \subseteq G_{s-1} \subseteq \dots \subseteq G_1 \subset G = G_0$ is a subnormal series with abelian factors. We show by induction on $i \geq 1$ that $G^{(i)} \subseteq G_i$. Since G/G_1 is abelian we get $G^{(1)} \subseteq G_1$, by Proposition 1.161. This is the start of the induction argument. Suppose that we have shown $G^{(i)} \subseteq G_i$. Then trivially $G^{(i+1)} = [G^{(i)}, G^{(i)}] \subseteq [G_i, G_i]$. But since G_i/G_{i+1} is abelian we get $[G_i, G_i] \subseteq G_{i+1}$. Thus $G^{(i)} \subseteq G_i$ for all i . In particular $G^{(s)} \subseteq G_s = \{e\}$, so that G is solvable. \square

The chain in Theorem 1.95 is a subnormal series with abelian factors. Thus *finite groups of prime power order are solvable*.

In some texts on group theory the condition that a group should have a subnormal series with abelian factors is used as the *definition* of a solvable group. We are going to use Theorem 1.165 below without referring to it.

Theorem 1.166 Subgroups and factor groups of a solvable group is again solvable.

Proof Let G be solvable. If H is a subgroup of the G then trivially $H^{(i)} \subseteq G^{(i)}$ for all i . This shows that H is solvable. If $N \triangleleft G$ we consider a subnormal series (*) as above for G with abelian factors. By Theorem 1.160 the subnormal series $\{e\} \subseteq N \subseteq G$ has a refinement

$$(**) H_t = \{e\} \subseteq H_{t-1} \subseteq \dots \subseteq H_s = N \subseteq \dots \subseteq H_1 \subseteq G = H_0,$$

which is equivalent to a refinement of (*). Both refinements have abelian factors, since (*) has abelian factors. By Noethers Theorem 1.71

$$\{e\} = \overline{H_s} \subseteq \overline{H_{s-1}} \subseteq \dots \subseteq \overline{G}$$

is subnormal series for $\overline{G} = G/N$ with abelian factors. \square

Theorem 1.167 Let $N \triangleleft G$. Then G is solvable if and only if N and $\overline{G} = G/N$ are solvable.

Proof We have seen that N and $\overline{G} = G/N$ are solvable, if G is solvable. Assume now that N and $\overline{G} = G/N$ are solvable. A subnormal series with abelian factors for $\overline{G} = G/N$ induces by Theorem 1.71 a subnormal series

$$\{e\} \subseteq H_s = N \subseteq \dots \subseteq H_1 \subseteq G = H_0$$

with all factors H_i/H_{i+1} abelian, $0 \leq i \leq s-1$. Add to this a subnormal series for N with abelian factors to get a subnormal series for G with abelian factors. \square

Remark 1.168 A simple non-trivial solvable group G is cyclic of prime order. Indeed if $G \neq \{e\}$ is solvable then $G^{(1)} \subset G$ is a normal subgroup. If G is also simple we get $G^{(1)} = \{e\}$ so that G is abelian. Then apply Exercise 1.74.

Theorem 1.169 *A finite group is solvable if and only if it has a composition series with all composition factors cyclic of prime order.*

Proof If G has a composition series with all composition factors cyclic of prime order it is solvable (Theorem 1.165). If G is finite, it has a composition series by Exercise 1.156. If G is also solvable the composition factors are solvable simple groups, and thus cyclic of prime order (Remark 1.168.) \square

The next result is important in Chapter V of these notes!

Theorem 1.170 *The symmetric group S_n is solvable if and only if $n \leq 4$.*

Proof Here are subnormal series for S_3 and S_4 with abelian factors: $\{e\} \subset A_3 \subset S_3$ and $\{e\} \subset V \subset A_4 \subset S_4$, where V is the “Vierergruppe”. Let $n \geq 5$. It is known that then the alternating group A_n is a nonabelian simple group (AT: p. 131). (In fact for this theorem we need only use the simpler fact, that A_5 is simple and thus non-solvable. Why?) It follows that S_n is not solvable (Theorem 1.166.) \square

Exercise 1.171 Verify that for $n \geq 5$ the only non-trivial normal subgroup of S_n is A_n .

1.19 Semidirect products of groups

There is a useful generalization of the direct product called the semidirect product.

Definition 1.172 Let H, K be groups. Suppose that there exists a homomorphism $\alpha : K \rightarrow \text{Aut}(H)$. The cartesian product $H \times K$ of H and K may be given a group structure using the following composition:

$$(a_a, b_1)(a_2, b_2) = (a_1\alpha(b_1)(a_2), b_1b_2) \text{ for } a_1, a_2 \in H, b_1, b_2 \in K.$$

Note that $\alpha(b_1) \in \text{Aut}(H)$, and therefore $\alpha(b_1)(a_2) \in H$. It can be calculated that $H \times K$ becomes a group which we denote $H \rtimes K$ or even $H \rtimes_{\alpha} K$ if we want to specify α . In this group $(1,1)$ is the unit element and the inverse to (a, b) is $(\alpha(b^{-1})(a^{-1}), b^{-1})$. This group is referred to as an outer semidirect product.

This may look as a rather complicated definition, but it should become more transparent, when you look at the semidirect product from the inside. The following theorem should be compared with Theorem 1.124!

Theorem 1.173 *Suppose that H and K are subgroups of G satisfying*

- (i) $G = HK$
- (ii) $H \triangleleft G$.
- (iii) $H \cap K = \{e\}$.

For $b \in K$ let $\alpha(b)$ be the restriction of the inner automorphism k_b of G to the normal subgroup H . Then $\alpha : K \rightarrow \text{Aut}(H)$ is a homomorphism and $G \simeq H \rtimes_{\alpha} K$. We refer such a group as an inner semidirect product of H by K .

Example 1.174 We refer to Example 1.25. The subgroups $H = \langle \sigma \rangle$ and $K = \langle \rho \rangle$ of $G = \langle \sigma, \rho \rangle$ satisfy the conditions of Theorem 1.173. The relation $\rho\sigma = \sigma^4\rho$ mentioned in this example may be rewritten as $\rho\sigma\rho^{-1} = \sigma^{-1}$, since $\sigma^4 = \sigma^{-1}$. Thus $\alpha(\rho)$ is the automorphism of H inverting all its elements.

Example 1.175 Suppose that $H = \langle a \rangle$ is cyclic of order $n \geq 2$ and that $K = \langle b \rangle$ is cyclic of order 2. Let $\alpha(b) \in \text{Aut}(H)$ be determined by $\alpha(b)(a) = a^{-1}$. Then $H \rtimes_{\alpha} K$ is isomorphic to the dihedral group of order $2n$.

Example 1.176 (*Some Frobenius groups*) The Frobenius groups is an important class of permutation groups. Most advanced books on group theory have treatment of them. We look at the simplest of them, which we call $F(p, t)$. Let p be an odd prime and t a divisor of $(p - 1)$. Let K be a cyclic group of order k . We have seen (Theorem 1.107) that $\text{Aut}(C_p)$ is cyclic of order $(p - 1)$. Let α be an isomorphism between K and the subgroup of $\text{Aut}(C_p)$ of order t . Then α may be seen as a homomorphism $K \rightarrow \text{Aut}(C_p)$. Then we define $F(p, t) = C_p \rtimes_{\alpha} K$. It is not difficult to see that if we choose another isomorphism α' we get a group isomorphic to $F(p, t)$. In the particular case, where $t = 2$ the only automorphism of order 2 is the one of the previous example. We get that $F(p, 2)$ is the dihedral group of order $2p$.

1.20 Groups of a given order

We want to apply the result obtained so far to study finite groups of “small” order. We are going to consider two isomorphic groups as the same group, as it is usual in group theory. So we really count isomorphism classes. (Remark 1.60). *The number of groups of a given order refers to the number of isomorphism classes of groups of that order.* For any $n \in \mathbb{N}$ we have at least one group of order n , the cyclic group C_n . A statement like *There is only one group of order n* means then that any group of order n is isomorphic to C_n .

We already know by Examples 1.37 and 1.77 that the following is true:

Proposition 1.177 *Let p be prime. Then there is only one group of order p , namely C_p .*

We also have the following general results:

Proposition 1.178 *Let p be prime. Then there are exactly two groups of order p^2 , namely C_{p^2} and $C_p \times C_p$.*

Proof By Corollary 1.94 G is abelian, if $|G| = p^2$. The result follows from Theorem 1.129.

(Here is a direct argument: If G contains an element of order p^2 then G is cyclic ($\simeq C_{p^2}$). Otherwise all non-trivial elements of G have order p . Choose $a \in G$, $a \neq e$ and $b \in G \setminus \langle a \rangle$. Put $H = \langle a \rangle$, $K = \langle b \rangle$. Then H and K satisfies the conditions (i)-(iii) of Theorem 1.124. Indeed (iii) is trivially fulfilled and (i) follows from Lemma 1.39. (ii) follows from Remark 1.43. We conclude $G \simeq H \times K \simeq C_p \times C_p$.) \square

Theorem 1.179 *Let p, q be different primes, $p < q$.*

- (1) *If $p \nmid (q - 1)$ then there is exactly one group of order pq , namely C_{pq} .*
- (2) *If $p \mid (q - 1)$ then there are exactly two groups of order pq , namely C_{pq} and $F(q, p)$.*

In any case $m_q(G) = 1$.

Proof Let $|G| = pq$ and $Q \in \text{Syl}_q(G)$. By Theorem 1.117 $m_q(G) \mid p$. Since $q \nmid (p - 1)$ because $p < q$ we get $m_q(G) = 1$, ie. $Q \triangleleft G$. Let $P \in \text{Syl}_p(G)$. We get $m_p(G) \mid q$. If $p \nmid (q - 1)$ we must have $m_p(G) = 1$, by Theorem 1.117. We get also $P \triangleleft G$. Now Theorem 1.124 shows that $G \simeq P \times Q$. In particular G is abelian. Thus if $P = \langle a \rangle$ and $Q = \langle b \rangle$ then $ab = ba$ and for all $k \geq 0$ we have $(ab)^k = a^k b^k$. This shows that $|ab| = pq$ so G is cyclic.

If $p \mid (q - 1)$ it is possible that $m_p(G) = q$. Then G is not cyclic and non-trivial elements of P and Q cannot commute, by the above. In that case G is a semidirect product of Q by P , by Theorem 1.173. The map α in the Theorem is a homomorphism $\alpha : P \rightarrow \text{Aut}(Q)$. The kernel of α is $\{e\}$, since an element in the kernel would commute with all elements in Q . Now Example 1.176 shows that $G \simeq F(q, p)$. \square

This result shows in particular that *a non-abelian group of order $2p$, p an odd prime, is isomorphic to a dihedral group.*

Theorem 1.180 *Let p, q be different primes. If G is a group of order p^2q then either $m_p(G) = 1$ or $m_q(G) = 1$. In particular G is solvable.*

Proof If $p > q$ then $m_p(G) = 1$ by Theorem 1.117. Assume $p < q$ and that $m_q(G) > 1$. Then $m_q(G) = p^2$. (The possibility $m_p(G) = q$ is excluded since $p < q$.) Since two q -Sylow groups have only e in common we get $p^2(q - 1)$ elements of order q . We then have only $p^2 = p^2q - p^2(q - 1)$ elements in G of order $\neq q$. The elements of a p -Sylow subgroup have this property, and thus G has only one p -Sylow subgroup, ie. $m_p(G) = 1$.

Exercise 1.181 Suppose that $n \geq 2$ and that we know that there is only one (isomorphism class of) groups of order n . Show that $n = p_1 p_2 \dots p_k$ for prime numbers $p_1 < p_2 < \dots < p_k$ with the property that for all $i < j$ we have $p_i \nmid (p_j - 1)$.

Here is a table of the number of groups of a given order 2-11, which we already know:

Group order	2	3	4	5	6	7	8	9	10	11
Number of gps	1	1	2	1	2	1		2	2	1
Nonabelian	0	0	0	0	1	0		0	1	0

Except for order 8 this follows from the results 1.177, 1.178 and 1.179.

There are 5 groups of order 8. Of these 3 are abelian by Corollary 1.130. We show

Lemma 1.182 *A nonabelian group of order 8 is isomorphic to D_4 or to the quaternion group Q .*

Proof Exercise 1.19 shows that G contains an element a of order 4. Then $\langle a \rangle \triangleleft G$, since it has index 2. Suppose that some element b outside $\langle a \rangle$ has order 2. Then we must have $bab^{-1} = a^{-1}$ and $G \simeq D_4$. (Example 1.175). Otherwise $|b| = 4$. Then if we map a to \mathbf{i} and b to \mathbf{j} then this may be extended to an isomorphism $G \simeq Q$. \square

We continue the list of the number of groups of small order:

Group order	7	8	9	10	11	12	13	14	15	16	17	18	19
Number of gps	1	5	2	2	1	5	1	2	1	14	1	5	1
Nonabelian	0	2	0	1	0	3	0	1	0	9	0	3	0

The cases of order 12, 16 and 18 are not covered completely by the results above. In the cases of 12 and 18 we know that in the non-abelian case one of the Sylow subgroups is normal so that the group is a semidirect product. It is not difficult to study these semidirect products. The most difficult case is groups of order $16 = 2^4$. Generally it soon gets very difficult to classify groups of a given prime power order p^r as r grows.

Index

- abelian group, 3
- alternating group, 15
- automorphism, 14
- automorphism group, 14
- automorphism group of cyclic group, 22

- bar notation, 13

- canonical epimorphism, 13
- Cayley's theorem, 31
- center of p -group, 20
- center of group, 20
- centralizer, 19
- characteristic subgroup, 21
- class equation, 20
- classification, 17
- commutative, 3
- commutator, 3
- commutator subgroup, 22
- composition factor, 34
- composition series, 34
- conjugacy class, 19
- conjugate elements, 19
- conjugate subsets, 19
- conjugates, 19
- conjugates, number of, 19
- coset, 9
- cycle decomposition of permutation, 4
- cycle type of integer, 5
- cycle type of permutation, 5
- cyclic group, 16
- cyclic groups, classification, 17
- cyclic subgroup, 6

- dihedral group, 8
- direct product, 26
- doubly transitive, 29

- epimorphism, 13
- equivalent series, 35
- Euler's φ -function, 17

- even permutation, 5

- factor group, 12
- factors of series, 33
- Frobenius groups, 38

- general linear group, 5
- generated, 6
- generator of cyclic group, 16
- group, 3
- group of prime order, 10
- groups of order p^2 , 39
- groups of order p^2q , 39
- groups of order pq , 39

- higher commutator subgroup, 36
- homomorphism, 13
- homomorphism theorem, 15

- image of homomorphism, 14
- index of subgroup, 10
- inner automorphism, 15
- inner direct product, 27
- inner semidirect product, 38
- inverse element, 3
- isomorphic groups, 14
- isomorphism, 14
- isomorphism class, 14
- isomorphism theorems, 16

- Jordan-Hölder, 35

- kernel of homomorphism, 14

- Lagrange's theorem, 9
- left coset, 9

- monomorphism, 13

- neutral element, 3
- Noethers first isomorphism theorem, 16
- Noethers second isomorphism theorem, 16

normal p -complement, 26
 normal subgroup, 11
 normalizer, 19

 odd permutation, 5
 orbit, 30
 orbit formula, 30
 order of element, 7
 order of group, 3
 order of power of element, 7
 order of products of subgroups, 10
 outer direct product, 26
 outer semidirect product, 37

 p -element, 26
 p -group, 20
 p -subgroup, 23
 permutation, 4
 permutation group, 29
 power rules, 6
 powers of element, 6
 product of subgroups, 11
 product of subsets, 9

 quaternion group, 8

 representative of coset, 9
 residue class group, 13
 right coset, 9

 Schreiers theorem, 35
 semidirect product, 37
 sign, 5
 simple abelian group, 16
 simple group, 11
 solvable group, 36
 special linear group, 16
 stabilizer, 30
 subgroup, 5
 subgroup generated by subset, 6
 Sylow subgroup, 23
 Sylow's theorems, 23
 symmetric group, 4

 totient function, 17

 transitive, 29
 trivial element, 3
 trivial subgroup, 5

 unit element, 3

 vierergruppe, 8