Chapter 1
Preliminaries

Here we record some basic definitions and elementary results about group, rings, and varieties of algebraic systems. We assume a basic knowledge in undergraduate algebra. In particular, in group theory, the reader is supposed to be familiar with definitions and basic properties of subgroups, cosets, cyclic subgroups, direct products, the structure of finite abelian groups, normal subgroups, the Homomorphism Theorems. The Sylow Theorems may be referred to occasionally, but they are not used in the proofs of the main results of the book, which are all about finite p-groups. Some familiarity with rings and modules is assumed, although many of the definitions are briefly reproduced.

We shall often use exponent notation for images under mappings, that is, a^φ or A^φ for $\varphi(a)$ or $\varphi(A)$ respectively, and sometimes also the right operator notation, $a\varphi$ for $\varphi(a)$, say. The identity mapping of a set M will be denoted by 1_M. Standard notation $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ is fixed for the sets of natural numbers, integers, rational, real and complex numbers, respectively. We shall say that a value is (a,b)-bounded, say, if there is a function depending only on a and b, such that the value does not exceed this function.

§ 1.1. Groups

Some basic definitions. The sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are groups with respect to addition. The set $\mathbb{Z}/n\mathbb{Z}$ of residues modulo n is a group with respect to addition mod n. Every vector space is a group with respect to addition. The set $\mathbb{S}_M$ of all bijections of a set M onto M is a group with respect to the composition of mappings, the identity mapping 1_M being the neutral element and the inverse mapping being the inverse element. When M is finite of order n, the notation $\mathbb{S}_n$ is often used; $\mathbb{S}_n$ is called the *symmetric group on n letters*.

The set of all bijective linear mappings of a vector space V over a field k is a subgroup of $\mathbb{S}_V$ denoted by $GL(V)$. The set $GL_n(k)$ of all non-degenerate $n \times n$ matrices over k is a group with respect to matrix multiplication. If n is the dimension of V, then fixing a basis of V, we associate a matrix to each linear transformation of V. This correspondence is an isomorphism of $GL(V)$ and $GL_n(k)$.

We use 1 to denote both the neutral element (identity) of a group and the *trivial subgroup* consisting of the neutral element only. To signify that H is a subgroup of G, we write $H \leq G$ or $G \geq H$; strict inequality $H < G$ means that $H \leq G$ and $H \neq G$, that is, H is a *proper* subgroup of G. Saying that a subset or a subgroup is *minimal* or *maximal* with respect to some property,

we shall mean minimal or maximal with respect to inclusion.

A (sub)group generated by a subset M is the minimal subgroup containing M, denoted by $\langle M\rangle$; it is unique since it equals the intersection of all subgroups containing M. We know that $\langle M\rangle$ consists of all products $m_1^{\varepsilon_1}\cdots m_s^{\varepsilon_s}$, where $m_i\in M$ and $\varepsilon_i=\pm 1$. Note that if $M\subseteq H\leq G$, then $\langle M\rangle\leq H$. Usually, braces are omitted within the angle brackets, so that $\langle a\mid P(a)\rangle=\langle\{a\mid P(a)\}\rangle$; in a similar way, $\langle A_1,A_2,\dots\rangle=\langle A_1\cup A_2\cup\dots\rangle$.

The cardinality of a set M is denoted by $|M|$. The index of a subgroup $H\leq G$ is denoted by $|G:H|$. Recall a useful inequality

$$|G:H\cap K|\leq |G:H|\cdot|G:K| \tag{1.1}$$

for the indices of subgroups. It follows that the intersection of n subgroups of index at most m has (m,n)-bounded index (less than or equal to m^n).

An element $x^g=g^{-1}xg$ is the *conjugate* of x under g. Note that $(a^b)^c=a^{bc}$ and $(ab)^c=a^cb^c$ for any elements a,b,c in a group. For any subset M, a similar notation is used: $M^g=g^{-1}Mg=\{g^{-1}mg\mid m\in M\}$. A subgroup $H\leq G$ is *normal*, denoted by $H\trianglelefteq G$, if $H^g=H\Leftrightarrow Hg=gH$ for every $g\in G$. The *factor-group* G/N of a group G by a normal subgroup N is the set of cosets $\{Ng\mid g\in G\}$ with multiplication $Ng\cdot Nh=Ngh$; this operation is well-defined precisely because $N\trianglelefteq G$. The *normal closure* $\langle S^G\rangle$ of a subset S in a group G is the minimal normal subgroup of G containing S, the intersection of all normal subgroups containing S; clearly, $\langle S^G\rangle=\langle s^g\mid s\in S,\ g\in G\rangle$. For any subset S of a group G and a subgroup $H\leq G$, the set $N_H(S)=\{g\in H\mid S^g=S\}$ is a subgroup called the *normalizer* of S in H. The subset S is said to be *K-invariant* if $K\leq N_G(S)$.

Lemma 1.2. *A subgroup $H\leq G$ is contained in the normalizer $N_G(S)$ of a subset $S\subseteq G$ if and only if $S^h\subseteq S$ for every $h\in H$.*

Proof. Indeed, $S^{h^{-1}}\subseteq S\Rightarrow S=(S^{h^{-1}})^h\subseteq S^h$ for every $h\in H$, plus $S^h\subseteq S$ by the hypothesis; hence $S^h=S$ for every $h\in H$. (If S is finite, the result follows immediately from the fact that $|S|=|S^h|$.) □

For a subgroup $H\leq G$ and a subset $S\subseteq G$, the set $C_H(S)=\{g\in H\mid sg=gs \text{ for all } s\in S\}$ is a subgroup called the *centralizer* of S in H. For a one-element $S=\{s\}$ we simply write $C_G(s)$.

Lemma 1.3. *For subgroups K,H,L,M,N in a group G*

(a) *$K\leq C_G(H)$ if and only if $H\leq C_G(K)$,*

(b) *if both L and M are N-invariant, then $C_L(M)$ and $N_L(M)$ are N-invariant too.*

Proof. (a) $K\leq C_G(H)\Leftrightarrow kh=hk$ for all $h\in H$, $k\in K\Leftrightarrow H\leq C_G(K)$.

(b) For any $c\in C_L(M)$, $m\in M$ and $n\in N$ we have $c^nm=(cm^{n^{-1}})^n=(m^{n^{-1}}c)^n=mc^n$ since $m^{n^{-1}}\in M$, so $C_L(M)^n\subseteq C_L(M)$; hence $C_L(M)$ is

N-invariant by Lemma 1.2. For any $v \in N_L(M)$ and $n \in N$ we have $M^{v^n} = (M^n)^{v^n} = (M^v)^n = M^n = M$, so $N_L(M)^n \subseteq N_L(M)$; hence $C_L(M)$ is N-invariant by Lemma 1.2. □

The *centre* of a group G is $Z(G) = C_G(G) = \{z \in G \mid zg = gz \text{ for all } g \in G\}$. Clearly, $Z(G)$ is the intersection of the centralizers of all elements of G.

For any two subsets M and N of a group the *product* MN is the set $\{mn \mid m \in M, n \in N\}$. If M, say, consists of one element, $M = \{m\}$, then we simply write mN, which agrees with the usual notation for cosets if N is a subgroup. If H is a subgroup and N is a normal subgroup of a group G, then the set $HN = NH$ is also a subgroup of G, so that $\langle H, N\rangle = HN$; if both H and N are normal subgroups, then HN is a normal subgroup too.

The (external) *direct product* $A \times B$ of two groups A, B is the set of pairs (a, b), $a \in A$, $b \in B$, with the component-wise operation $(a_1, b_1) \cdot (a_2, b_2) = (a_1a_2, b_1b_2)$, so that $(1, 1)$ is the neutral element of $A \times B$ and $(a, b)^{-1} = (a^{-1}, b^{-1})$. Then A and B can be identified with the normal subgroups $\widehat{A} = \{(a, 1) \mid a \in A\}$ and $\widehat{B} = \{(1, b) \mid b \in B\}$ respectively, for which $\widehat{A} \cap \widehat{B} = 1$ and $\widehat{A}\widehat{B} = A \times B$. Conversely, if a group $G = MN$ is a product of two normal subgroups M, N with trivial intersection $M \cap N = 1$ (internal direct product), then G is isomorphic to the direct product $M \times N$, the isomorphism given by $mn \to (m, n)$. Thus, the notions of internal and external direct products are equivalent.

Example 1.4. Suppose that M and N are normal subgroups of a group G. Then $MN/(M \cap N) \cong \overline{M} \times \overline{N}$, where $\overline{M} = M/(M \cap N)$ and $\overline{N} = N/(M \cap N)$. Indeed, $MN/(M \cap N) = \overline{M}\overline{N}$, both $\overline{M}$ and $\overline{N}$ are normal subgroups, and $\overline{M} \cap \overline{N} = 1$ since $m(M \cap N) = n(M \cap N)$ for $m \in M$, $n \in N$ implies that $m \in N$, say.

The *Cartesian product* $\mathrm{Cr}_{i\in I} A_i$ of a family of groups $\{A_i \mid i \in I\}$ is the set of all functions $f : I \to \bigcup_{i\in I} A_i$ such that $f(i) \in A_i$; this is a group with respect to the coordinate-wise operation $(fg)(i) = f(i)g(i)$. The set of those functions f that have non-trivial values only on a finite subset of I (depending on f) is the *direct product* $\mathrm{Dr}_{i\in I} A_i$, a subgroup of $\mathrm{Cr}_{i\in I} A_i$. For a finite set of groups both definitions coincide and the resulting group is isomorphic to $A_1 \times \cdots \times A_n$ (with arbitrary order of parentheses). The equivalent definition of the internal direct product is that $G = \langle A_i \mid i \in I\rangle$, $A_i \trianglelefteq G$ for all $i \in I$, and $A_j \cap \langle A_i \mid i \neq j\rangle = 1$.

The *order* of an element a of a group denoted by $|a|$ is the least positive integer k such that $a^k = 1$, or ∞ if no such k exists. It is easy to see that $|a| = |\langle a\rangle|$. The *exponent* of a group G is the least $n \in \mathbb{N}$ such that $x^n = 1$ for all $x \in G$ (or ∞ if such n does not exist). Clearly, the exponent is the least common multiple of the orders of all elements of G. We denote by G^n the subgroup of a group G generated by all nth powers of the elements of G;

clearly, G^n is the smallest normal subgroup such that the factor-group is of exponent dividing n. A group is *torsion-free* if it has no non-trivial elements of finite order. Let p be a prime number. An element of a group is a *p-element*, if its order is a power of p. A group G is a *p-group*, if it consists of p-elements. For a p-group G, we define the subgroups $\Omega_i(G) = \left\langle x \in G \mid x^{p^i} = 1 \right\rangle$. A maximal (with respect to inclusion) p-subgroup is a *Sylow p-subgroup*. The Sylow Theorems state that in a finite group of order $p^k n$, where $p \nmid n$, all Sylow p-subgroups have order p^k (so that every p-subgroup is contained in a subgroup of order p^k), and all Sylow p-subgroups are conjugate.

A *section* M/N of a group G is a factor-group of any of its subgroups: $M \leq G$ and $N \trianglelefteq M$; a section is said to be normal if both M and N are normal in G. Any chain of nested subgroups

$$1 = G_0 \leq G_1 \leq G_2 \leq \ldots \leq G_n = G$$

is a *series* of G of length n. If all of the G_i are normal in G, the series is *normal*; if each G_i is a normal subgroup of G_{i+1}, the series is *subnormal*. The sections G_{i+1}/G_i of a subnormal series are the *factors* of the series. (Of course, one can number the terms of a series in any other way.)

Abelian groups. Recall that a group is *abelian* or *commutative* if $ab = ba$ for any two elements a and b. Abelian groups are often written additively, using $+$ for the operation and 0 for the neutral element (and for the trivial subgroup); but we still denote factor-groups as M/N, rather than $M - N$. For example, the additive group of integers $\mathbb{Z}$ is generated by 1, which is *not* the neutral element here. We denote by ka the kth power of an element a, speak about direct sums of abelian groups instead of direct products, etc.

If A is an abelian group and $n \in \mathbb{N}$, then $nA = \{na \mid a \in A\}$ is a subgroup of A. If n is coprime to the exponent of a finite abelian group A, then $a \to na$ is an injective mapping, since $na = nb \Rightarrow n(a-b) = 0 \Rightarrow a - b = 0$, and hence $nA = A$.

Suppose that $p_1, \ldots, p_n$ are all distinct prime divisors of the order of a finite abelian group A. It is clear that all p_i-elements in A form a subgroup A_{p_i} which is the unique Sylow p_i-subgroup of A. Suppose that, for an element $a \in A$, we have $|a| = m = p_1^{k_1} \cdots p_n^{k_n}$, $k_i \geq 0$ (only the p_i are involved by Lagrange's Theorem). Put $m_i = m/p_i^{k_i}$; the greatest common divisor of all of the m_i is 1, and hence there exist integers u_i such that $1 = u_1 m_1 + \cdots + u_n m_n$. It follows that $a = 1a = u_1 m_1 a + \cdots + u_n m_n a$, where $p_i^{k_i} m_i a = ma = 0$ so that $m_i a \in A_{p_i}$ for each i. Therefore, $A = A_{p_1} + \cdots + A_{p_n}$. Since $A_{p_i} \cap (A_{p_1} + \cdots + \widehat{A}_{p_i} + \cdots + A_{p_n}) = 0$ for each i (the order of an element in the intersection can be only 1), the sum is direct: $A = A_{p_1} \oplus \cdots \oplus A_{p_n}$.

The above decomposition is a part of the Structure Theorem for finite (finitely generated) abelian groups. This theorem takes especially simple form for finite abelian p-groups: every such a group is a direct sum of cyclic groups

of orders $p^{k_1}, \dots, p^{k_s} \geq p$ and the set $\{k_1, \dots, k_s\}$ is an invariant, that is, does not depend on the choice of the summands (which are in no way unique).

A finite abelian group has *rank* n, if it is a direct sum of n cyclic groups, and n is minimal possible. For a finite p-group P, the rank r is equal to the number of (non-trivial) cyclic subgroups in the direct sum $P = \langle a_1 \rangle \oplus \cdots \oplus \langle a_r \rangle$ and does not depend on such decomposition, as follows from the Structure Theorem.

An abelian group E of prime exponent p is called *elementary abelian*. In the additive notation, E can be viewed as a vector space over $\mathbb{F}_p$, the field of p elements (of residues mod p, say). The addition of vectors is the group operation, and multiplying a vector g by a residue i is taking the ith power ig of the element g (this is well-defined since $pg = 0$); the axioms of a vector space over $\mathbb{F}_p$ are easily checked: for example, we have $i(x + y) = ix + iy$ for $x, y \in E$, $i \in \mathbb{F}_p$, since the group is abelian. One can say that the theory of elementary abelian groups of exponent p is "categorically equivalent" to the theory of vector spaces over $\mathbb{F}_p$: every statement about E as a group of exponent p can be translated into the language of a vector space over $\mathbb{F}_p$ and vice versa. The rank of E as a group is exactly the dimension of E as a space. The automorphism group $\operatorname{Aut} E$ coincides with the group of non-degenerate linear transformations over $\mathbb{F}_p$, and so on.

Suppose that $P = \langle a_1 \rangle \oplus \cdots \oplus \langle a_r \rangle$ is an abelian p-group with $|a_i| = p^{k_i} \geq p$; then $\Omega_1(P) = \left\langle p^{k_1 - 1} a_1 \right\rangle \oplus \cdots \oplus \left\langle p^{k_r - 1} a_r \right\rangle$. The number of cyclic summands, r, is equal to the rank of $\Omega_1(P)$, which is the dimension of $\Omega_1(P)$, an invariant. Thus, the number of cyclic summands for P is always equal to the rank of P and to the rank of $\Omega_1(P)$. Considering the ranks of Ω_{i+1}/Ω_i is a way to prove the uniqueness part of the Structure Theorem (Exercise 1.18). We also have $pP = \langle pa_1 \rangle \oplus \cdots \oplus \langle pa_r \rangle$ and P/pP is an elementary abelian p-group of rank r.

A direct sum of several cyclic groups of equal order p^n is a *homocyclic* group of exponent p^n. Such groups have quite a homogeneous structure.

Lemma 1.5. *Suppose that A is a homocyclic group of exponent p^n and rank r. Then*

(a) *$p^i A = \Omega_{n-i}(A)$ for all $i \leq n$;*

(b) *if $p^i a \in p^j A$ for $i \leq j \leq n$, then $a \in p^{j-i} A$;*

(c) *the mapping $x \to px$ induces isomorphisms of the sections $p^i A / p^{i+1} A$, $i = 0, 1, \dots, n-1$;*

(d) *if $p^i B \geq p^j A$ for a subgroup $B \leq A$, then $B \geq p^{j-i} A$ unless $j \geq n$;*

(e) *if $p^k A \geq B$, then $\Omega_k(A/B)$ is a homocyclic group of exponent p^k and rank r;*

(f) *if $A \geq B \geq p^k A$, then $B/p^{n-k}B$ is a homocyclic group of exponent p^{n-k} and rank r.*

Proof. Let $A = \langle a_1 \rangle \oplus \cdots \oplus \langle a_r \rangle$ where $|a_i| = p^n$ for all i. Every element $a \in A$ has a unique representation $a = \sum_{i=1}^{r} u_i a_i$ where $a_i \in \mathbb{Z}/p^n\mathbb{Z}$. It follows

that $a \in p^s A \Leftrightarrow p^s | u_i$ for all i, and $p^s | |a| \Leftrightarrow p^{n-s} | u_i$ for all i. Hence (a) and (b) follow. It also follows that $|p^i A| = p^{r(n-i)}$ and hence $|p^i A / p^{i+1} A| = p^r$ for all $i \leq n-1$. Since the mapping $x \to px$ obviously induces a homomorphism of $p^{i-1}A/p^i A$ onto $p^i A/p^{i+1}A$, this is actually an isomorphism.

To prove (d), choose k such that $B \geq p^k A$, but $B \not\geq p^{k-1}A$. The mapping $x \to px$ induces an isomorphism of $p^{k-1}A/p^k A$ onto $p^k A/p^{k+1}A$ which maps $B \cap p^{k-1}A$ onto $pB \cap p^k A$; hence $p^i B \not\geq p^{k-1+i}A$ as long as $k-1+i < n$. If $p^i B \geq p^j A$ for $j \leq n$, it follows that $j \geq k+i$ so that $B \geq p^k A \geq p^{i-j}A$.

(e) The factor-group $A/B = \langle g_1 \rangle \oplus \cdots \oplus \langle g_r \rangle$ is a direct sum of r cyclic p-groups of orders $|g_i| = p^{k_i} \geq p^k$, since $A/p^k A$ is a homomorphic image of A/B. Hence

$$\Omega_k(A/B) = \left\langle p^{k_1-k} g_1 \right\rangle \oplus \cdots \oplus \left\langle p^{k_r-k} g_r \right\rangle$$

is a homocyclic group of exponent p^k and rank r.

(f) We have $B \geq \left\langle p^k a_1 \right\rangle \oplus \cdots \oplus \left\langle p^k a_r \right\rangle$; and hence $B = \langle g_1 \rangle \oplus \cdots \oplus \langle g_r \rangle$ is a direct sum of r cyclic groups of order $\geq p^{n-k}$ each. Then $B/p^{n-k}B = \langle g_1 \rangle / \left\langle p^{n-k} g_1 \right\rangle \oplus \cdots \oplus \langle g_r \rangle / \left\langle p^{n-k} g_r \right\rangle$ is a homocyclic group of exponent p^{n-k} and rank r. □

Lemma 1.6. (a) *Suppose that B is a homocyclic subgroup of exponent p^n of an abelian group A of the same exponent p^n. Then $A = B \oplus C$ for some $C \leq A$.*

(b) *Suppose that U is a homocyclic abelian group of exponent p^n and U/B is a homocyclic group of the same exponent p^n for some $B \leq U$. Then $U = B \oplus C$ for some $C \leq U$.*

(c) *Suppose that U is a homocyclic abelian group of exponent p^n and $U = V \oplus W$; then V and $U/V \cong W$ are homocyclic groups of exponent p^n.*

Proof. (a) Induction on $|A|$. Suppose that $\Omega_1(A) \not\leq B$; then there is $c \in A \setminus B$ such that $pc = 0$ and hence $B \cap \langle c \rangle = 0$. Then the image $\overline{B}$ of B in $\overline{A} = A/\langle c \rangle$ is isomorphic to B. By the induction hypothesis $\overline{A} = \overline{B} \oplus \overline{C}$ for some $\overline{C} \leq \overline{A}$. Let C be the full preimage of $\overline{C}$; we claim that $A = B \oplus C$. Indeed, $A = B + C$ and $B \cap C \leq B \cap \langle c \rangle = 0$. It remains to prove that if $\Omega_1(A) \leq B$, then $B = A$. We use induction on k to prove that if $p^k a = 0$, then $a \in B$; for $k = 1$ this is true by the assumption $\Omega_1(A) \leq B$. For $k > 1$ we have $p^{k-1}a \in \Omega_1(A) \leq B$; since B is homocyclic of the same exponent as A, there is $b \in B$ such that $p^{k-1}b = p^{k-1}a$, whence $p^{k-1}(b-a) = 0$. By the induction hypothesis $b - a \in B$, whence $a \in B$.

(b) Let $U/B = \langle \bar{a}_1 \rangle \oplus \cdots \oplus \langle \bar{a}_k \rangle$ with $|\bar{a}_i| = p^n$ for all i. Choose some preimages a_i of the $\bar{a}_i$; then $|a_i| = p^n$ for all i since p^n is the exponent of U. We claim that $U = B \oplus C$ where $C = \langle a_1 \rangle + \cdots + \langle a_k \rangle$. Since $U = B + C$, we need only to show that $B \cap C = 0$. If $\sum_{i=1}^k k_i a_i \in B$, then $\sum_{i=1}^k k_i \bar{a}_i = 0$, whence $p^n | k_i$ for all i, since U/B is homocyclic of exponent p^n. But then

$\sum_{i=1}^{k} k_i a_i = 0$ too.

(c) Both V and W are direct sums of cyclic p-groups; together, these decompositions form a decomposition of $U = V \oplus W$ into the direct sum of cyclic groups. Since the set of the orders of the summands is unique by the Structure Theorem, both V and W must be homocyclic of exponent p^n. □

The assertion (a) can be used to prove the existence part of the Structure Theorem for abelian p-groups.

Homomorphisms and automorphisms. Recall that a mapping φ of a group G into another group is a homomorphism if φ preserves the group operation: $(ab)^\varphi = a^\varphi b^\varphi$ (it follows that $(a^{-1})^\varphi = (a^\varphi)^{-1}$ and $1^\varphi = 1$). The set $\operatorname{Ker}\varphi = \{g \in G \mid g^\varphi = 1\}$ is always a normal subgroup of G, the *kernel* of φ. If $N \trianglelefteq G$, then $g \to gN$ is the so-called *natural homomorphism* of G onto the factor-group G/N. Congruences mod N denote equalities of the images in G/N of elements or subsets:

$$a \equiv b \,(\mathrm{mod}\, N) \;\Leftrightarrow\; aN = bN; \qquad A \equiv B \,(\mathrm{mod}\, N) \;\Leftrightarrow\; AN = BN.$$

Let φ be a homomorphism of a group G with kernel $N = \operatorname{Ker}\varphi$. The Homomorphism Theorems state that

- φ is a composition of the natural homomorphism of G onto G/N and some isomorphism of G/N onto G^φ;
- $H \to H^\varphi$ is a bijection of the set of all subgroups containing N and the set of subgroups of G^φ, and $N \le H \trianglelefteq G \Leftrightarrow H^\varphi \trianglelefteq G^\varphi$;
- for any subgroup $K \le G$ the full preimage of K^φ is KN; if $L \trianglelefteq K$, then $L^\varphi \trianglelefteq K^\varphi$ and $K^\varphi/L^\varphi \cong K/L(N \cap K)$; in particular, $K^\varphi \cong K/(K \cap N)$, and if $N \le M \trianglelefteq L$, then $L^\varphi/M^\varphi \cong L/M$.

We now prove a very useful though simple lemma.

Lemma 1.7. *If φ is a homomorphism of a group G, then $\langle M\rangle^\varphi = \langle M^\varphi\rangle$ for any subset $M \subseteq G$.*

Proof. We know that $\langle M\rangle = \{m_1^{\varepsilon_1} \cdots m_s^{\varepsilon_s} \mid m_i \in M,\ \varepsilon_i = \pm 1\}$. Since φ is a homomorphism, $(m_1^{\varepsilon_1} \cdots m_s^{\varepsilon_s})^\varphi = (m_1^\varphi)^{\varepsilon_1} \cdots (m_s^\varphi)^{\varepsilon_s}$ for every such a product. Hence $\langle M\rangle^\varphi$ coincides with the set of the products $(m_1^\varphi)^{\varepsilon_1} \cdots (m_s^\varphi)^{\varepsilon_s}$ which is exactly $\langle M^\varphi\rangle$. □

A homomorphism of a group into itself is an *endomorphism*. A subgroup $H \le G$ is said to be *fully invariant*, if $H^\psi \le H$ for every endomorphism ψ of G. Lemma 1.7 implies that $\Omega_1(P)$ is a fully invariant subgroup in any p-group P, since elements of order p are mapped to elements of order dividing p by any

endomorphism. Similarly, G^n is a fully invariant subgroup for any $n \in \mathbb{N}$. If a Sylow p-subgroup is unique, then it is fully invariant; this happens, for example, in abelian groups.

An isomorphism of a group onto itself is an *automorphism*; all automorphisms of a group G form the group $\operatorname{Aut} G$ as a subgroup of $\mathbb{S}_G$ (that is, with respect to composition of mappings). For any given $g \in G$, the mapping $\tau_g : x \to g^{-1}xg = x^g$ is the *inner automorphism* induced by g.

A subgroup H of a group G is said to be *characteristic* in G, if it is invariant under all automorphisms of G, that is, if $H^\varphi = H$ for every $\varphi \in \operatorname{Aut} G$. Similarly to Lemma 1.2, it is sufficient to require $H^\varphi \leq H$ for all $\varphi \in \operatorname{Aut} G$. Clearly, a characteristic subgroup is normal, since it is in particular invariant under all inner automorphisms of G. A section M/N is called characteristic, if both M and N are characteristic subgroups. Every fully invariant subgroup is, of course, characteristic. (So the examples above, $\Omega_1(P)$, G^n, a unique Sylow subgroup, are all characteristic subgroups.) The converse may not be true, for example, $Z(G)$ is always a characteristic subgroup, but need not be fully invariant (Exercise 1.3).

In general, a normal subgroup of a normal subgroup may not be normal in the whole group; for example, the subgroup $A = \langle (12)(34) \rangle$ of order 2 in $\mathbb{S}_4$ is normal in the subgroup $B = \langle (12)(34), (13)(24) \rangle$ of order 4 which, in turn, is normal in $\mathbb{S}_4$, but $A \not\trianglelefteq \mathbb{S}_4$.

Lemma 1.8. (a) *If C is a characteristic subgroup of N and N is a normal subgroup of a group G, then C is also normal in G.*

(b) *If, in addition, N is characteristic in G, then C is characteristic in G.*

(c) *If C is fully invariant in N and N is fully invariant in G, then C is fully invariant in G.*

Proof. (a) For every $g \in G$ the restriction $\tau_g|_N$ of the inner automorphism τ_g to N is an automorphism of N since $N^{\tau_g} = N$, and $\tau_g|_N$ preserves the operations since $\tau_g \in \operatorname{Aut} G$. Then $C^g = C^{\tau_g} = C$, since C is characteristic in N.

(b) If N is characteristic in G, then $\alpha|_N \in \operatorname{Aut} N$ for every $\alpha \in \operatorname{Aut} G$ for similar reasons, and hence $C^\alpha = C$ since C is characteristic in N.

(c) For any endomorphism φ of G its restriction to N is an endomorphism of N; hence C is φ-invariant. □

Lemma 1.9. *For any subgroup $H \leq G$, $C_G(H)$ is a normal subgroup of $N_G(H)$ and $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\operatorname{Aut} H$.*

Proof. For every $g \in N_G(H)$, the restriction $\tau_g|_H$ is an automorphism of H since $N^g = N$. The mapping $\vartheta : g \to \tau_g|_H$ is a homomorphism of $N_G(H)$ into $\operatorname{Aut} H$ since $(x^{g_1})^{g_2} = x^{g_1 g_2}$ for any $x \in H$ so that $(g_1 g_2)^\vartheta = g_1^\vartheta g_2^\vartheta$. An element $g \in N_G(H)$ belongs to the kernel of ϑ if and only if $\tau_g|_H = 1_H \Leftrightarrow x^g = x$

for every $x \in H$, that is, $g \in C_G(H)$. By the Homomorphism Theorems, $N_G(H)/\mathrm{Ker}\,\vartheta = N_G(H)/C_G(H) \cong N_G(H)^\vartheta \leq \mathrm{Aut}\,H$. □

Lemma 1.10. *If H is a normal (or characteristic) subgroup of G, then both $N_G(H)$ and $C_G(H)$ are normal (or characteristic) subgroups of G.*

Proof. The proof is left as an exercise for the reader. □

Commutators and commutator subgroups. We define recursively *commutators of weight* $1, 2, \ldots$ in variables $x_1, x_2, \ldots$ as formal bracket expressions. The letters $x_1, x_2, \ldots$ are commutators of weight 1; if c_1 and c_2 are commutators of weight w_1 and w_2, then $[c_1, c_2]$ is a commutator of weight $w_1 + w_2$. The *multiweight* of a commutator is the collection of the partial weights in particular variables, which are defined recursively in an obvious way. For example, $[[x_1, x_2], x_1]$ is a commutator of weight 3, and of weight 1 in x_2 and of weight 2 in x_1. A commutator $[...[[a_1, a_2], a_3], \ldots, a_k]$ is called *simple* (or *left-normed*) and is denoted by $[a_1, a_2, \ldots, a_k]$.

The *commutator* $[a, b]$ of two elements in a group is defined to be $[a, b] = a^{-1}b^{-1}ab$; to avoid confusion, we had better say that $[a, b]$ is the value of the (formal) commutator $[x_1, x_2]$ on a, b. Then commutators of greater weight in the elements of a group are defined as the values of formal commutators on these elements. We may also use the same notions of weight and multiweight for these values. Commutators may be different as formal bracket structures, but their values, commutators in the group elements, may well be equal; for example, any commutator of weight ≥ 2 in the elements of an abelian group is trivial.

Lemma 1.11. *The following commutator formulae hold for any elements a, b, c in any group:*

(a) $a^b = a[a, b]$,

(b) $[ab, c] = [a, c]^b[b, c] = [a, c][a, c, b][b, c]$,

(c) $[a, bc] = [a, c][a, b]^c = [a, c][a, b][a, b, c]$,

(d) $[a, b]^{-1} = [b, a]$.

Proof. A direct verification, by expanding the commutators by definition; for example, in (b) we have $[ab, c] = (ab)^{-1}c^{-1}abc = b^{-1}a^{-1}c^{-1}abc$ on the left, $[a, c]^b[b, c] = b^{-1}[a, c]b[b, c] = b^{-1}a^{-1}c^{-1}acbb^{-1}c^{-1}bc = b^{-1}a^{-1}c^{-1}abc$ in the middle, and on the right $[a, c][a, c, b][b, c] = a^{-1}c^{-1}ac[a, c]^{-1}b^{-1}[a, c]bb^{-1}c^{-1}bc = a^{-1}c^{-1}acc^{-1}a^{-1}cab^{-1}a^{-1}c^{-1}acbb^{-1}c^{-1}bc = b^{-1}a^{-1}c^{-1}abc$, and all three results are the same. □

For two subsets M and N in a group G, we define the *mutual commutator subgroup* to be $[M, N] = \langle [m, n] \mid m \in M, n \in N \rangle$. Note that $[M, N] = [N, M]$, since $[n, m] = [m, n]^{-1}$ and the inverses of the elements generate the same

subgroup. If N, say, consists of one element n, we write simply $[M, n]$.

Lemma 1.12. *If M and N are subgroups of a group G, then $[M, N]$ is a normal subgroup of the group $\langle M, N\rangle$.*

Proof. It is clear that $[M, N] \leq \langle M, N\rangle$, so it suffices to prove that $\langle M, N\rangle \leq N_G([M, N])$; since $N_G([M, N])$ is a subgroup, it suffices to prove that both M and N are contained in $N_G([M, N])$. By symmetry, we need only show that $M \leq N_G([M, N])$. By Lemma 1.2, it suffices to show that $[M, N]^g \leq [M, N]$ for any $g \in M$. By Lemma 1.7, we need only prove that $[m, n]^g \in [M, N]$ for any $m \in M$, $n \in N$ (since $[M, N]$ is generated by the $[m, n]$). By Lemma 1.11(b), $[m, n]^g = [mg, n][g, n]^{-1} \in [M, N]$ because $mg \in M$ since M is a subgroup. □

Lemma 1.13. *If M is a subgroup of G, then $[M, g] = [M, \langle g\rangle]$ for any $g \in G$.*

Proof. Clearly, $[M, g] \leq [M, \langle g\rangle]$. We denote by a bar the image in $M/[M, g]$. For any $\overline{m} \in \overline{M}$, we have $[\overline{m}, \bar{g}] = 1$ which implies $\bar{g} \in C_{\overline{M}}(\overline{m})$. Since $C_{\overline{M}}(\overline{m})$ is a subgroup, $\bar{g}^k \in C_{\overline{M}}(\overline{m})$ for every $k \in \mathbb{Z}$. Hence $[m, g^k] \in [M, g]$ for all $m \in M$, $k \in \mathbb{Z}$, and therefore $[M, \langle g\rangle] \leq [M, g]$ since $[M, g]$ is a subgroup. □

For any homomorphism φ of a group G and any $a, b \in G$, we have

$$[a, b]^\varphi = [a^\varphi, b^\varphi], \qquad \text{whence} \quad [M, N]^\varphi = [M^\varphi, N^\varphi] \tag{1.14}$$

by Lemma 1.7. It follows that if both M and N are characteristic (or fully invariant, or normal) subgroups, then $[M, N]$ is also a characteristic (respectively, fully invariant, normal) subgroup.

The *derived subgroup* of a group G is defined to be $[G, G]$ (often denoted by G'). The derived subgroup is fully invariant, since G is. It is easy to see that $[G, G]$ is the smallest normal subgroup such that the factor-group is abelian.

Lemma 1.15. *For a normal subgroup N of a group G, the factor-group G/N is abelian if and only if $[G, G] \leq N$.*

Proof. For $x, y \in G$, let $\bar{x}$ and $\bar{y}$ denote their images in G/N (under the natural homomorphism). By (1.14), $\overline{[x, y]} = [\bar{x}, \bar{y}]$. Then G/N is abelian $\Leftrightarrow \overline{[x, y]} = [\bar{x}, \bar{y}] = 1$ for all $\bar{x}, \bar{y} \in G/N \Leftrightarrow [x, y] \in N$ for all $x, y \in G \Leftrightarrow [G, G] \leq N$. □

In fact, any subgroup containing $[G, G]$ is normal in G (Exercise 1.2).

We conclude this subsection with remarks on commutator subgroups. The same simple commutator notation is used for subgroups:

$$[A, B, C, \dots, Z] = [\dots[[A, B], C], \dots, Z].$$