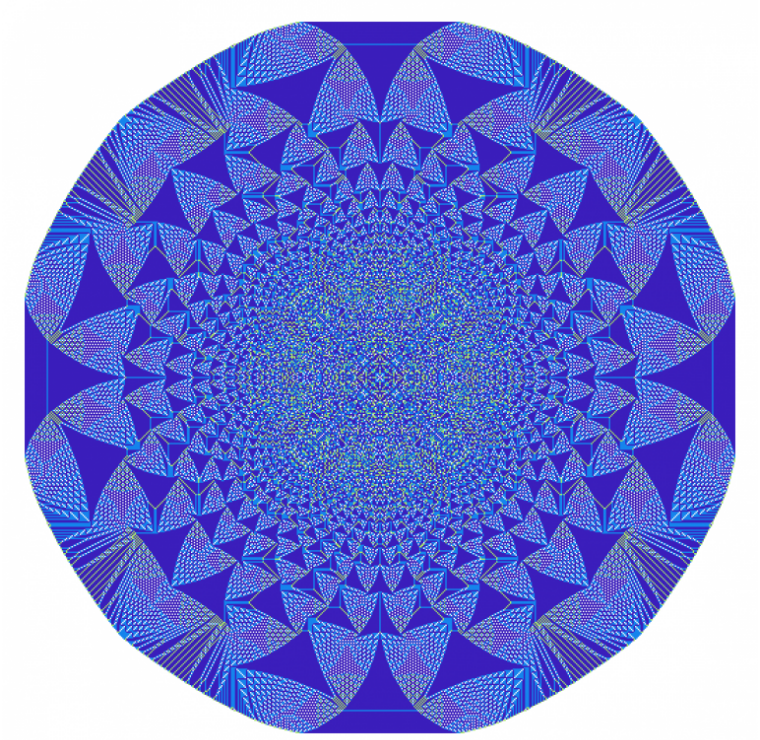
Jonas Hübotter
based on lectures of Frank Himstedt



Abstract Algebra

Contents. Groups, homomorphisms, cyclic groups, Sylow theorems, and solvable groups. Rings, ideals, polynomial rings, irreducibility of polynomials. Fields, field extensions, Galois theory, solvable polynomials.

Illustration is due to Katherine E. Stange.
Contributions are welcome at `https://github.com/jonhue/algebra`.

ACKNOWLEDGEMENT

The contents of this summary are based on the "Algebra" lecture given by Frank Himstedt at the Technical University of Munich in fall of 2020.

Contents

Part I

Groups

1
Groups and Homomorphisms

1.1 Groups

Definition 1.1 (Semigroup, Monoid, and Group)**.**

(a) A set G with a mapping $\cdot$ on G (that is, $\cdot : G \times G \to G$) is named
- *semigroup* if $\forall a, b, c \in G.\ (a \cdot b) \cdot c = a \cdot (b \cdot c)$; — *associativity*
- *monoid* if it is a semigroup and $\exists e \in G.\ \forall a \in G.\ e \cdot a = a \cdot e = a$; — e is called *neutral element*
- *group* if it is a monoid and $\forall a \in G.\ \exists a' \in G.\ a \cdot a' = a' \cdot a = e$. — a' is the *inverse element* of a

(b) A group $(G, \cdot)$ is named *abelian* or *commutative* if the group operation $\cdot$ is commutative under elements of G,

$$\forall a, b \in G. \quad a \cdot b = b \cdot a. \tag{1.1}$$

We denote groups by $(G, \cdot)$. If the group operation $\cdot$ is clear from context, we refer to the group simply as G. Subsequently, we also write ab instead of $a \cdot b$.

Remark 1.2. Let G be a group. Then,

(a) there is exactly one neutral element $e \in G$ and for every $a \in G$ there is exactly one inverse element $a' \in G$, which we call a^{-1};
(b) the mapping on G, which we refer to by $\cdot$, may be resembled by any symbol;
(c) if G is abelian, often
- $+$ is used instead of $\cdot$,
- 0 is used instead of e, and
- $-a$ is used instead of a^{-1}.

Example 1.3: Semigroups, monoids, and groups

	$(\mathbb{N}, +)$	$(\mathbb{N}_0, +)$	$(\mathbb{Z}, +)$	$(\mathbb{Z}, \cdot)$	$(\mathbb{Q} \setminus \{0\}, \cdot)$
semigroup	yes	yes	yes	yes	yes
monoid	no	yes	yes	yes	yes
group	yes	no	yes	no	yes

Example 1.4: General linear and special linear group

The *general linear group* $\mathrm{GL}_n(K)$ is the group of invertible[1] $n \times n$ linear maps over a field[2] K,

$$\mathrm{GL}_n(K) \doteq \{\boldsymbol{A} \in K^{n\times n} \mid \det \boldsymbol{A} \neq 0\}. \tag{1.2}$$

The *special linear group* $\mathrm{SL}_n(K)$ is the group of normed linear maps over the field K,

$$\mathrm{SL}_n(K) \doteq \{\boldsymbol{A} \in K^{n\times n} \mid \det \boldsymbol{A} = 1\}. \tag{1.3}$$

The group operation of $\mathrm{GL}_n(K)$ and $\mathrm{SL}_n(K)$ is matrix multiplication. Their neutral element is the identity matrix $\boldsymbol{I}$, and the inverse elements are the matrix inverses $\boldsymbol{A}^{-1}$.

[1] Recall from linear algebra that a matrix $\boldsymbol{A}$ is invertible iff $\det \boldsymbol{A} \neq 0$.

[2] A *field* is a set of elements with well-defined operations for addition, subtraction, multiplication, and division. We give a formal definition in definition 15.1. Examples of fields are the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, and the complex numbers $\mathbb{C}$.

Example 1.5: Abelian groups

- $(\mathbb{Z}, +)$
- $(\mathbb{Q}, +)$
- $(\mathbb{R}, +)$
- $(\mathbb{R} \setminus \{0\}, \cdot)$

Example 1.6: Symmetric group

The *symmetric group* S_n is the group of bijections on the set $[n]$,

$$S_n \doteq \{\sigma : [n] \to [n] \mid \sigma \text{ is bijective}\}, \tag{1.4}$$

with the function composition "$\circ$" as mapping.

Elements of the symmetric group $\sigma \in S_n$ are called *permutations*. The neutral element of the symmetric group is the identity id, which maps each input to itself.

There are multiple ways of representing permutations. Perhaps the most natural representation of $\sigma \in S_n$ is a mapping in *two-line notation*,

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}, \tag{1.5}$$

or in *one-line notation* by simply omitting the first line,

$$\sigma = (\sigma(1)\ \sigma(2)\ \cdots\ \sigma(n)). \tag{1.6}$$

An alternative characterization of a permutation is as a product of (disjoint) cycles. A *cycle* $\rho \in S_n$ is a permutation that maps a subset of numbers $\{i_1, i_2, \ldots, i_r\} \subseteq [n]$ in a cyclic fashion. That is,

$$\rho(i_1) = i_2, \quad \rho(i_2) = i_3, \quad \cdots \quad \rho(i_{r-1}) = i_r, \quad \rho(i_r) = i_1, \tag{1.7}$$

leaving all other $j \in [n]$ fixed. We denote such a cycle by

$$\rho = (i_1\ i_2\ \cdots\ i_r). \tag{1.8}$$

A cycle of length r, is also called *r-cycle*. 2-cycles are called *transpositions*.

Every permutation $\sigma \in S_n$ can be written as a "product" (i.e., composition),

$$\sigma = \rho_1 \cdots \rho_s, \tag{1.9}$$

where ρ_i are cycles with pairwise disjunct elements. This is also known as the *cycle notation* of σ. Note that the ordering of $\rho_1, \ldots \rho_s$ does not matter, as their elements are disjoint.

The cycle lengths $r_1, \ldots, r_s$ (in descending order) of $\rho_1, \ldots, \rho_s$ are the *cycle type* of σ.

Remark 1.7. The symmetric group is not abelian.
Proof. We have $(1\ 2)(2\ 3) = (2\ 3\ 1)$ and $(2\ 3)(1\ 2) = (1\ 3\ 2)$. □

Lemma 1.8 (Notation and Rules)**.** *Let $(G, \cdot)$ be a group.*

(a) For $a \in G, n \in \mathbb{N}_0$, we write
- $a^n \doteq \underbrace{a \cdot a \cdots a}_{n \text{ many}}$,
- $a^0 \doteq e$, *and*
- $a^{-n} \doteq \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{n \text{ many}}$.

(b) $\forall a, b \in G.\ \forall m, n \in \mathbb{Z}$.
- *(i)* $(a^{-1})^{-1} = a$
- *(ii)* $a^m \cdot a^n = a^{m+n}$, $(a^m)^n = a^{m \cdot n}$
- *(iii)* $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$

Proof of (b)(iii). $(a \cdot b) \cdot b^{-1} \cdot a^{-1} = a \cdot \underbrace{(b \cdot b^{-1})}_{=e} \cdot a^{-1} = a \cdot a^{-1} = e$. □

Definition 1.9 (Subgroup)**.** A subset $U \subseteq G$ is called a *subgroup* of a group G (denoted $U \leq G$) if U itself is a group with mapping $\cdot$. That is, U is a subgroup iff

(a) $e \in U$; — U contains the neutral element
(b) $\forall a, b \in U.\quad a \cdot b \in U$; and — the mapping $\cdot$ is closed wrt. U

(c) $\forall a \in U.\quad a^{-1} \in U.$ — the mapping $(\dots)^{-1}$ is closed wrt. U

Associativity follows from G being a group.

Example 1.10: Subgroups

- $\{e\}, G \leq G$ (*trivial subgroups*)
- $\mathrm{SL}_n(K) \leq \mathrm{GL}_n(K)$
- Let $2\mathbb{Z} \doteq \{2m \mid m \in \mathbb{Z}\}$, then $(2\mathbb{Z}, +) \leq (\mathbb{Z}, +)$

Remark 1.11. If $\{U_i\}_{i \in I}$ are subgroups of G, then $\bigcap_{i \in I} U_i \leq G$.

Definition 1.12 (Generated Subgroup)**.** For any $M \subseteq G$,

$$\langle M \rangle \doteq \bigcap_{\substack{U \leq G \\ M \subseteq U}} U \leq G, \tag{1.10}$$

by remark 1.11

is the *subgroup generated by* M. In particular, $\langle M \rangle$ is the "smallest" subgroup that includes M.

Lemma 1.13. *For $M \neq \emptyset$, we have*

$$\langle M \rangle = \{a_1 \cdot a_2 \cdots a_n \mid n \in \mathbb{N}, a_i \in M \text{ or } a_i^{-1} \in M\}. \tag{1.11}$$

Proof (sketch). Let $N \doteq \{a_1 \cdot a_2 \cdots a_n \mid n \in \mathbb{N}, a_i \in M \text{ or } a_i^{-1} \in M\}$.

- $\langle M \rangle \subseteq N$: $N \leq G$ and $M \subseteq N \implies \langle M \rangle \subseteq N$
- $N \subseteq \langle M \rangle$: if $U \leq G$ with $M \subseteq U$, then U includes all of these products $\implies N \subseteq U \implies N \subseteq \langle M \rangle$ □

using that $\langle M \rangle$ is the smallest subgroup including M

Example 1.14: Generated subgroup

$$S_3 = \{\mathrm{id}, \underbrace{(1\ 2)}_{\tau_1}, \underbrace{(1\ 3)}_{\tau_2}, \underbrace{(2\ 3)}_{\tau_3}, \underbrace{(1\ 2\ 3)}_{\sigma_1}, \underbrace{(1\ 3\ 2)}_{\sigma_2}\} = \langle\{\underbrace{(1\ 2)}_{\tau_1}, \underbrace{(1\ 2\ 3)}_{\sigma_1}\}\rangle.$$

Definition 1.15 (Cyclic Group)**.** A group G is *cyclic* if $\exists a \in G$ with

$$G = \langle a \rangle \doteq \langle\{a\}\rangle = \{a^m \mid m \in \mathbb{Z}\}. \tag{1.12}$$

Such an $a \in G$, is called a *generator* of G.

Example 1.16: Cyclic groups

- $\langle i \rangle = \{i^m \mid m \in \mathbb{Z}\}$ is a cyclic subgroup of $(\mathbb{C} \setminus \{0\}, \cdot)$,

$$\begin{aligned}\langle i \rangle &= \{\dots, \underbrace{i^{-2}}_{=-1}, \underbrace{i^{-1}}_{=-i}, 1, i, \underbrace{i^2}_{=-1}, \underbrace{i^3}_{=-i}, \underbrace{i^4}_{=1}, \underbrace{i^5}_{=i}, \dots\} \\ &= \{1, i, -1, -i\}.\end{aligned}$$

- $(\mathbb{Z}, +) = \langle 1 \rangle = \{\dots, -2, -1, 0, 1, 2, \dots\}$ is cyclic

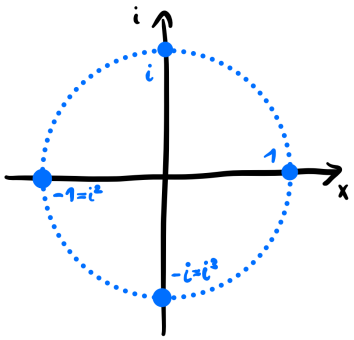


Figure 1.1: An illustration of the cyclic subgroup $\langle i \rangle$ in the complex plane.

Definition 1.17 (Order)**.** Let G be a group.

(a) The cardinality $|G| \in \mathbb{N} \cup \{\infty\}$ is called *order* of the group G.
(b) For any $a \in G$, $o(a) \doteq |\langle a \rangle|$ is the *order* of the element a.

If $|G| < \infty$, G is called *finite*.

Lemma 1.18. *If $k \doteq o(a) < \infty$, we have*

(a) $o(a) = \min\{j \in \mathbb{N} \mid a^j = e\}$;
(b) $\langle a \rangle = \{e, a, a^2, \ldots, a^{k-1}\}$; *and*
(c) For any $j \in \mathbb{Z}$, $a^j = e \iff o(a) \mid j$.[3]

[3] We use $a \mid b$ to denote that a divides b.

Proof. We write $m \doteq \min\{j \in \mathbb{N} \mid a^j = e\}$.

- $\underline{\{e, a, a^2, \ldots, a^{m-1}\} \subseteq \langle a \rangle}$: Let us fix an arbitrary $j \in \mathbb{N}$. We have,

$$\begin{aligned} o(a) = |\langle a \rangle| < \infty &\implies \exists j' > j.\ a^j = a^{j'} && \text{as the order of } a \text{ is finite} \\ &\implies a^{j'-j} = e && \text{by multiplying from the right with } a^{-j} \\ &\implies m \text{ exists and } \{e, a, a^2, \ldots, a^{m-1}\} \subseteq \langle a \rangle. && \text{as } j' - j \in \mathbb{N} \text{ is again a natural number} \end{aligned}$$

- $\underline{\langle a \rangle \subseteq \{e, a, a^2, \ldots, a^{m-1}\}}$: We fix any $n \in \mathbb{Z}$. Then, by *long division*, there exist $q, r \in \mathbb{Z}$ and $0 \leq r < m$ with $n = q \cdot m + r$. This yields,

$$a^n = a^{q \cdot m + r} = \underbrace{(a^m)^q}_{=e} \cdot a^r = a^r \in \{e, a, a^2, \ldots, a^{m-1}\}.$$

This proves that $m = o(a)$ and $\langle a \rangle = \{e, a, a^2, \ldots, a^{m-1}\}$. It also follows that

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

Remark 1.19. For a finite cyclic group $\langle a \rangle = \{e, a, a^2, \ldots, a^{k-1}\}$ of order k, we have $a^{k-j} = a^{-j}$.

Example 1.20: Order

- Let us consider $\mathrm{GL}_2(\mathbb{R})$. Then,

$$\begin{aligned} \boldsymbol{A} = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} &\implies \forall n \in N.\ \boldsymbol{A}^n = \begin{bmatrix} 2^n & 0 \\ 0 & 2^n \end{bmatrix} \neq \boldsymbol{I} \\ &\implies o(\boldsymbol{A}) = \infty, \\ \boldsymbol{B} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} &\implies \boldsymbol{B}^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \\ &\qquad \boldsymbol{B}^3 = -\boldsymbol{B} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \boldsymbol{B}^4 = (\boldsymbol{B}^2)^2 = \boldsymbol{I} \\ &\implies o(\boldsymbol{B}) = 4. \end{aligned}$$

- $|S_n| = |\{\sigma : [n] \to [n] \mid \sigma \text{ is bijective}\}| = n!$

Example 1.21: Subgroups of S_3

Let us find the subgroups of

$$S_3 = \{\mathrm{id}, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}.$$

We immediately obtain the trivial subgroups $\{\mathrm{id}\}$ and S_3 or order 1 and 6, respectively. It is a simple exercise to confirm the following cyclic subgroups:

- $\langle(1\,2)\rangle = \{\mathrm{id}, (1\,2)\}$
- $\langle(1\,3)\rangle = \{\mathrm{id}, (1\,3)\}$
- $\langle(2\,3)\rangle = \{\mathrm{id}, (2\,3)\}$
- $\langle(1\,2\,3)\rangle = \langle(1\,3\,2)\rangle = \{\mathrm{id}, (1\,2\,3), (1\,3\,2)\}$

The first three subgroups generated by 2-cycles are of order 2, the last subgroup generated by the 3-cycles is of order 3.

Observe that the subgroup orders are divisors of the group order. This is not coincidental, we will make this precise in the following. In doing so, we will also find that our list of subgroups of S_3 was indeed exhaustive.

The subgroup structure of a group G can be graphically represented in a *subgroup graph*. Subgroups of G are represented as vertices. Groups U and V are connected if $U \leq V$ and there exists no subgroup "between" U and V. An example is given in fig. 1.2.

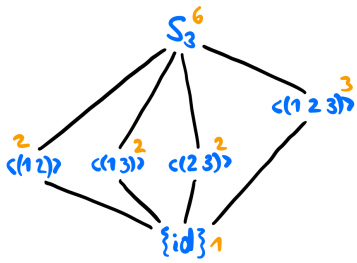


Figure 1.2: Subgroup graph of the symmetric group S_3. The order of the subgroups is shown in orange.

Definition 1.22 (Cosets and Index)**.** Let $U \leq G$ be a subgroup.

(a) For $a \in G$,

$$aU \doteq \{a \cdot u \mid u \in U\}, \tag{1.13}$$
$$Ua \doteq \{u \cdot a \mid u \in U\}, \tag{1.14}$$

are the left and right *coset* of U in G, respectively.

(b) The *index* $[G : U] \doteq |\{aU \mid a \in G\}|$ of U in G is defined as the number of cosets of U in G.[4]

[4] The number of left cosets is identical to the number of right cosets.

Lemma 1.23. *For all $a, b \in G$, we have*

(a) $aU = U \iff a \in U$
(b) $aU = bU \iff a^{-1}b \in U$
(c) $aU \cap bU \neq \emptyset \iff aU = bU$
(d) $G = \bigcup_{a \in G} aU$
(e) $|aU| = |U|$

Proof of (e). $U \to aU, u \mapsto a \cdot u$ is a bijective mapping. Hence, domain and codomain are of the same size. □

Theorem 1.24 (Lagrange's Theorem)**.** *If G is a finite group and $U \leq G$ is some subgroup, then*

$$|G| = |U| \cdot [G : U]. \tag{1.15}$$

In particular, $|U|$ and $[G : U]$ are divisors of $|G|$.

Proof. Let $r \doteq [G : U]$. Then we can write G as a disjoint union of cosets,

$$G = a_1 U \cup a_2 U \cup \cdots \cup a_r U.$$

We have,

$$|G| = \sum_{i=1}^{r} |a_i U| = r \cdot |U| = [G : U] \cdot |U|. \qquad \square$$

using that $|a_i U| = |U|$ by lemma 1.23.(e)

Corollary 1.25. *Let G be a finite group. Then we have for any $a \in G$,*

(a) $o(a) \mid |G|$
(b) $a^{|G|} = e$ *(*Fermat's little theorem*)*

Proof.

(a) By Lagrange's theorem, $|\langle a \rangle| \mid |G|$.
(b) By lemma 1.18.(c), $a^{|G|} = e \iff o(a) \mid |G|$. $\square$

Corollary 1.26. *Let G be a group such that $|G| = p$ where p is prime. Then, G is cyclic.*

Proof.

$$\begin{aligned} |G| > 1 &\implies \exists a \in G \setminus \{e\} \\ &\implies 1 \neq |\langle a \rangle| \mid |G| && \text{using that } o(a) \geq 2 \text{ if } a \neq e \text{ and Lagrange's theorem} \\ &\implies |\langle a \rangle| = p = |G|. && \text{using that } |G| \text{ only has divisors 1 and } p \end{aligned}$$

Therefore, $\langle a \rangle = G$. $\square$

Example 1.27: Subgroups of S_3 (continued)

We will now see that S_3 has exactly four non-trivial subgroups, proving that we have found all subgroups of S_3 in example 1.21.

Let $U \leq S_3$ be a non-trivial subgroup. By Lagrange's theorem, we have $|U| \mid |S_3| = 3! = 6$. As we have excluded the trivial subgroups $\{\mathrm{id}\}$ and S_3, we know that $|U| \neq 1, 6$. This leaves us with $|U| \in \{2, 3\}$.

Observe that 2 and 3 are prime, hence, by corollary 1.26 U must be cyclic. Recall that we have already enumerated all (four) cyclic subgroups of S_3 in example 1.21.

1.2 Homomorphisms

We will now consider two groups $(G, \cdot)$ and $(H, \cdot)$. To understand the relationship between G and H, it is useful to look at mappings between the two groups. A special mapping that (as we will see) preserves the structure of a group, is the group homomorphism.

Definition 1.28 ((Group) Homomorphism)**.**

(a) The mapping $\varphi : G \to H$ is called a *(group) homomorphism* if

$$\forall a, b \in G. \quad \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b). \tag{1.16}$$

The homomorphism $\psi : G \to G$ is called *endomorphism* of G.

(b) The set of elements that are mapped to the neutral element e_H,

$$\ker \varphi \doteq \{a \in G \mid \varphi(a) = e_H\} \subseteq G, \tag{1.17}$$

is called the *kernel* of φ.

(c) The set of elements in the codomain H that φ maps to,

$$\operatorname{im} \varphi \doteq \{\varphi(a) \mid a \in G\} \subseteq H, \tag{1.18}$$

is called the *image* of φ.

Example 1.29: Homomorphisms

- $\varphi : G \to H, a \mapsto e_H$ is the *trivial homomorphism*
- For any field K, $\det : \mathrm{GL}_n(K) \to K \setminus \{0\}, \boldsymbol{A} \mapsto \det \boldsymbol{A}$ is a homomorphism due to the multiplicativity of the determinant.[5] We have for its kernel,

$$\ker \det = \{\boldsymbol{A} \in \mathrm{GL}_n(K) \mid \det \boldsymbol{A} = 1\} = \mathrm{SL}_n(K). \tag{1.19}$$

- Let us consider the *sign* of a permutation,

$$\operatorname{sgn} : S_n \to \{-1, 1\}, \sigma \mapsto (-1)^{N(\sigma)}, \tag{1.20}$$

where $N(\sigma)$ is the number of inversions in σ. An *inversion* in σ is a pair of elements that is out of order. More formally,

$$N(\sigma) = |\{(i, j) \mid i < j \text{ and } \sigma(i) > \sigma(j)\}|. \tag{1.21}$$

For an r-cycle the sign reduces to,

$$\operatorname{sgn} \underbrace{(i_1 \ \cdots \ i_r)}_{r\text{-cycle}} = (-1)^{r-1}. \tag{1.22}$$

It can be shown that sgn is a homomorphism, that is,

$$\forall \sigma, \tau \in S_n. \quad \operatorname{sgn}(\sigma \circ \tau) = \operatorname{sgn} \sigma \cdot \operatorname{sgn} \tau. \tag{1.23}$$

[5] Recall that $\det(\boldsymbol{A} \cdot \boldsymbol{B}) = \det \boldsymbol{A} \cdot \det \boldsymbol{B}$.

The kernel of sgn is the set of permutations with positive sign,

$$\ker \operatorname{sgn} = \{\sigma \in S_n \mid \operatorname{sgn} \sigma = 1\} \doteq A_n. \tag{1.24}$$

This set forms again a group, which is known as the *alternating group* A_n.

- Within the group $(\mathbb{Z}, +)$, $\varphi : \mathbb{Z} \to \mathbb{Z}, m \mapsto 2m$ is an endomorphism.

Lemma 1.30 (Properties of Homomorphisms). *Let $\varphi : G \to H$ be a homomorphism. Then,*

(a) $\varphi(e_G) = e_H$
(b) $\forall g \in G.\ \varphi(g^{-1}) = \varphi(g)^{-1}$
(c) $\ker \varphi \leq G$ *and* $\operatorname{im} \varphi \leq H$
(d) φ *injective* $\iff \ker \varphi = \{e_G\}$
(e) if $\psi : H \to K$ is a homomorphism, then $\psi \circ \varphi : G \to K$ is a homomorphism

Proof.

(a) We have $\varphi(e_G) = \varphi(e_G \cdot e_G) = \varphi(e_G) \cdot \varphi(e_G)$, using the compatibility of a homomorphism with the group structure (1.16). By multiplying with $\varphi(e_G)^{-1}$ from one side, we obtain that this statement is true if and only if $\varphi(e_G) = e_H$.

(b) Again, using the homomorphism property, we have,

$$e_H = \varphi(e_G) = \varphi(g \cdot g^{-1}) = \varphi(g) \cdot \varphi(g^{-1}).$$

By multiplying from the left with $\varphi(g)^{-1}$, we obtain that this statement is true if and only if $\varphi(g)^{-1} = \varphi(g^{-1})$.

(c) Let us confirm the properties of subgroups for $\ker \varphi \leq G$. The proof is analogous for $\operatorname{im} \varphi \leq H$. By definition 1.9, we need to show,

(i) $e_G \in \ker \varphi$ follows immediately from (a)
(ii) $\forall a, b \in \ker \varphi.\ \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) = e_H \cdot e_H = e_H$. Therefore, $\ker \varphi$ is closed under the group operation, $a \cdot b \in \ker \varphi$.
(iii) $\forall a \in \ker \varphi.\ \varphi(a^{-1}) = \varphi(a)^{-1} = e_H^{-1} = e_H$. Therefore, $\ker \varphi$ is closed under inversion, $a^{-1} \in \ker \varphi$.

$\implies \ker \varphi \leq G$.

(d) • "$\Rightarrow$": Let φ be injective. We want to show that $\ker \varphi = \{e_G\}$. Note that (a) already implies $\{e_G\} \subseteq \ker \varphi$. To show $\ker \varphi \subseteq \{e_G\}$, let $a \in \ker \varphi$. Then,

$$\varphi(a) = e_H \overset{(a)}{=} \varphi(e_H).$$

As φ is injective, it follows that $a = e_H$.

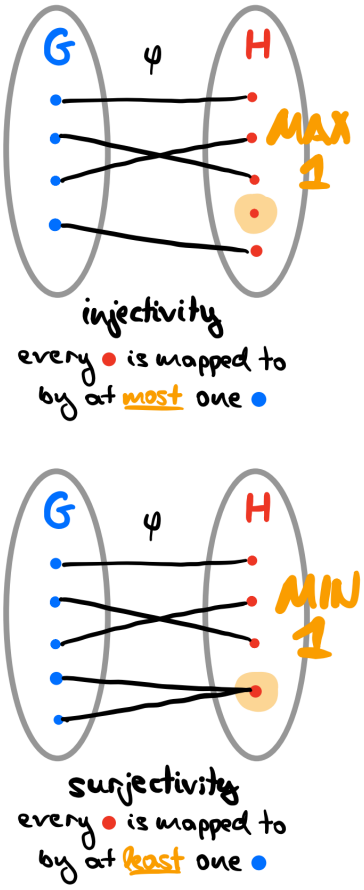


Figure 1.3: An illustration of *injectivity* and *surjectivity*. When a function φ is injective, $\varphi(a) = \varphi(b)$ implies $a = b$. We call a function *bijective* is it is both injective and surjective, i.e., a one-to-one mapping.

- "$\Leftarrow$": Let $\ker \varphi = \{e_G\}$. We want to show that φ is injective. Let $a, b \in G$ with $\varphi(a) = \varphi(b)$. By multiplying from the right with $\varphi(b)^{-1}$, we obtain,

$$e_H = \varphi(a) \cdot \varphi(b)^{-1} = \varphi(a) \cdot \varphi(b^{-1}) = \varphi(a \cdot b^{-1}).$$

  As the kernel of φ only contains e_G, we follow,

$$e_G = a \cdot b^{-1} \overset{\cdot b}{\Longrightarrow} a = b \implies \varphi \text{ injective.}$$

(e) Let $a, b \in G$. Then,

$$\begin{aligned}(\psi \circ \varphi)(a \cdot b) &= \psi(\varphi(a \cdot b)) = \psi(\varphi(a) \cdot \varphi(b)) && \text{using that } \varphi \text{ is a homomorphism} \\ &= \psi(\varphi(a)) \cdot \psi(\varphi(b)) = (\psi \circ \varphi)(a) \cdot (\psi \circ \varphi)(b). \square && \text{using that } \psi \text{ is a homomorphism}\end{aligned}$$

Definition 1.31 (Isomorphism)**.**

(a) The mapping $\varphi : G \to H$ is called an *isomorphism* if φ is a homomorphism and bijective. The isomorphism $\psi : G \to G$ is called an *automorphism* of G.

(b) G and H are called *isomorphic* (denoted $G \cong H$) if there exists an isomorphism $\varphi : G \to H$.

(c) $\mathrm{Aut}(G) \doteq \{\psi : G \to G \mid \psi \text{ automorphism}\}$ forms a group under function composition "$\circ$". This group is called the *automorphic group* of G.

Remark 1.32. If $\varphi : G \to H$ is an isomorphism, then $\varphi^{-1} : H \to G$ is an isomorphism.

Example 1.33: Isomorphisms

- Given a group G and an arbitrary element $g \in G$,

$$i_g : G \to G, x \mapsto g \cdot x \cdot g^{-1}, \tag{1.25}$$

  is the *inner automorphism* of the so-called *conjugating element* g. This isomorphism corresponds to the conjugation group action (also called *(left) conjugation* by g), which we will encounter again in chapter 4.
- $\exp : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot), x \mapsto e^x$ is an isomorphism.[6]

[6] exp is a homomorphism due to $e^{x+y} = e^x e^y$. As exp is strictly monotonically increasing, it is bijective.

2
Normal Subgroups and Quotient Groups

Let $(G, \cdot)$ be a group. In this chapter we will see that the coset structure of a group can itself be represented as a group.

Definition 2.1 (Normal Subgroup)**.** A subgroup $N \leq G$ is called *normal* (denoted $N \trianglelefteq G$) if

$$\forall a \in G. \quad aNa^{-1} \subseteq N. \tag{2.1}$$

Remark 2.2. The condition from eq. (2.1) is equivalent to,

$$\forall a \in G. \quad aNa^{-1} = N. \tag{2.2}$$

Proof (sketch). This follows directly from using eq. (2.1) for $a \in G$ and $a^{-1} \in G$. This yields $a^{-1}Na \subseteq N$. By multiplying from the left with a and from the right with a^{-1}, we obtain $N \subseteq aNa^{-1}$. □

Example 2.3: Normal subgroups

- the trivial subgroups $\{e\}$ and G are also normal, $\{e\}, G \trianglelefteq G$
- the *center*,

$$Z(G) \doteq \{a \in G \mid \forall x \in G.\, ax = xa\} \trianglelefteq G, \tag{2.3}$$

  is a normal subgroup of G.

Lemma 2.4 (Sufficient Conditions for Normal Subgroups)**.**

(a) If $\varphi : G \to H$ is a homomorphism, then $\ker \varphi \trianglelefteq G$.
(b) Every subgroup $U \leq G$ with index $[G : U] = 2$ is a normal subgroup of G.
(c) If U is the only subgroup of order $m < \infty$ of G, then $U \trianglelefteq G$.
(d) If G is abelian, then all subgroups of G are normal.

Proof (sketches).

(a) We have already seen in lemma 1.30.(c) that $\ker \varphi \leq G$. We have,

$$\forall a \in G, x \in \ker \varphi. \quad \varphi(axa^{-1}) = \varphi(a) \cdot \underbrace{\varphi(x)}_{=e_H} \cdot \varphi(a)^{-1} = e_H.$$

Thus, $a \cdot \ker\varphi \cdot a^{-1} \subseteq \ker\varphi$ and $\ker\varphi \trianglelefteq G$.

(c) For all $a \in G$, we have $aUa^{-1} = i_a(U)$ where i_a is the inner automorphism. As automorphisms are bijective, they map a subgroup to a subgroup of the same order. Therefore, $i_a(U) = U$, assuming that U is the only subgroup of order $m < \infty$. Using remark 2.2 completes the proof.

(d) Follows immediately from the definition of normal subgroups by applying commutativity. □

Example 2.5: Normal subgroups (continued)

- $A_n \trianglelefteq S_n$ as $A_n = \ker \operatorname{sgn}$, see eq. (1.24)
- $\mathrm{SL}_n(\mathbb{R}) \trianglelefteq \mathrm{GL}_n(\mathbb{R})$ as $\mathrm{SL}_n(\mathbb{R}) = \ker\det$, see eq. (1.19)
- $\mathrm{Inn}(G) \doteq \{i_g \mid g \in G\}$ known as the *inner automorphism group* is a normal subgroup of the automorphism group, $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$
- For the symmetric group S_3, we have the normal subgroups
  - $\{e\}, G \trianglelefteq G$
  - $A_3 = \langle(1\,2\,3)\rangle \trianglelefteq G$

  by lemma 2.4.(c). Simple calculations confirm that the subgroups of order 2 are not normal.

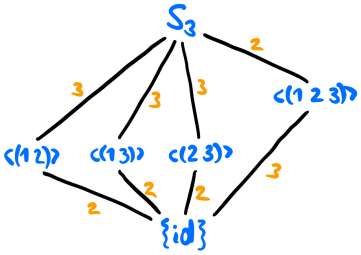


Figure 2.1: Subgroup graph of the symmetric group S_3. The index of the subgroups is shown in orange.

Theorem 2.6 (Quotient Group). *Let $N \trianglelefteq G$. Then the set*

$$G/N \doteq \{aN \mid a \in G\} \tag{2.4}$$

is a group under the operation,

$$aN \cdot bN \doteq (a \cdot b)N \quad \forall a, b \in G. \tag{2.5}$$

G/N is called the quotient group *G modulo N.*

Thus, the quotient group is the group of (left) cosets of a normal subgroup. In particular, if G is finite, we have,

$$|G/N| = [G : N] = \frac{|G|}{|N|}, \tag{2.6}$$

due to the definition of the index and Lagrange's theorem.

Proof. In proving that G/N is a group, we will see why we need the restriction of normal subgroups.

- First, we need to show that the group operation (2.5) is well-defined.[1] Let us fix $a_1, a_2, b_1, b_2 \in G$ such that $a_1N = a_2N$ and $b_1N = b_2N$. We need to show $a_1b_1N = a_2b_2N$.

[1] By *well-defined*, we mean that a function maps the same input to the same output.

As N contains the neutral element e, we know $a_1 \in a_1 N$ and $a_2 \in a_2 N$. Therefore, $\exists n \in N.\ a_1 = a_2 n$ and, analogously, $\exists \tilde{n} \in N.\ b_1 = b_2 \tilde{n}$. We have,

$$a_1 b_1 = a_2 n b_2 \tilde{n} = a_2 b_2 (b_2^{-1} n b_2 \tilde{n}).$$

Using that N is normal, $b_2^{-1} n b_2 \in N$. Then, as N is a subgroup, we also have $b_2^{-1} n b_2 \tilde{n} \in N$. This shows that $a_1 b_1 N = a_2 b_2 N$.

- $eN = N$ is the neutral element.
- The group operation is closed under G/N by definition.
- $(aN)^{-1} = a^{-1} N$ clearly is the inverse of aN.

$\implies G/N$ is a group. □

Example 2.7: Residue classes

We will consider the quotient group $\mathbb{Z}/n\mathbb{Z}$ of the group $(\mathbb{Z}, +)$ for any fixed $n \in \mathbb{N}_0$. We write,

$$n\mathbb{Z} \doteq \langle n \rangle = \{n \cdot k \mid k \in \mathbb{Z}\}. \tag{2.7}$$

Observe that the left cosets are of the form

$$a + n\mathbb{Z} = \{a + n \cdot k \mid k \in \mathbb{Z}\}. \tag{2.8}$$

They are also called *residue classes* modulo n.

To specify $\mathbb{Z}/n\mathbb{Z}$, we are interested in finding when $a + n\mathbb{Z} = b + n\mathbb{Z}$ holds. We have,

$$a + n\mathbb{Z} = b + n\mathbb{Z} \overset{1.23.(b)}{\iff} a - b \in n\mathbb{Z} \overset{1.13}{\iff} n \mid a - b. \tag{2.9}$$

Equivalently to $n \mid a - b$, we say that a is *congruent* b modulo n (denoted $a \equiv b \mod n$). For $n > 0$ this is equivalent to a and b having the same residue $r \in \{0, 1, \ldots, n-1\}$ when dividing by n.

From now on, we will assume $n > 0$. We denote elements by

$$\overline{a} \doteq a + n\mathbb{Z}, \tag{2.10}$$

where a is referred to as the *representative* of $\overline{a}$. It follows that,

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}. \tag{2.11}$$

By theorem 2.6, $\mathbb{Z}/n\mathbb{Z}$ with the mapping "+" is a cyclic group of order n. It is often denoted by

$$Z_n \doteq \mathbb{Z}/n\mathbb{Z} = \langle \overline{1} \rangle. \tag{2.12}$$

As an example, consider $Z_8 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}\}$. We have,

- $\overline{2} + \overline{5} = \overline{7}$,
- $\overline{2} + \overline{6} = \overline{8} = \overline{0}$, and
- $\overline{-6} = \overline{2}$.

Definition 2.8 (Cokernel)**.** The *cokernel* of a homomorphism $\varphi : G \to H$ is the quotient group $H / \operatorname{im} \varphi$.

Example 2.9: Outer automorphism group

Automorphisms that are not inner automorphisms are called *outer automorphisms*. The *outer automorphism group* is the group of cosets of the inner automorphism group with respect to outer automorphisms,

$$\operatorname{Out}(G) \doteq \operatorname{Aut}(G)/\operatorname{Inn}(G). \tag{2.13}$$

Let us define the homomorphism $\sigma : G \to \operatorname{Aut}(G), g \mapsto i_g$. It can be shown that

- $\ker \sigma = Z(G)$,
- $\operatorname{im} \sigma = \operatorname{Inn}(G)$, and
- the cokernel of σ is $\operatorname{Out}(G) = \operatorname{Aut}(G)/\operatorname{Inn}(G)$.

3
Homomorphism and Isomorphism Theorems

In this chapter, we will discuss tools to show that two groups are isomorphic.

Theorem 3.1 (Homomorphism Theorem)**.** *Let $\varphi : G \to H$ be a group homomorphism. Then,*

$$\overline{\varphi} : G/\ker\varphi \to \operatorname{im}\varphi, \quad a\ker\varphi \mapsto \varphi(a) \tag{3.1}$$

is an isomorphism. Especially, $G/\ker\varphi \cong \operatorname{im}\varphi$.

Proof.

- We will first show that $\overline{\varphi}$ is well-defined. For any $a, b \in G$,

$$\begin{aligned}
& a\ker\varphi = b\ker\varphi \\
\iff\quad & a^{-1}b \in \ker\varphi && \text{by lemma 1.23.(b)} \\
\iff\quad & \varphi(a^{-1}b) = e_H && \text{using the definition of the kernel (1.17)} \\
\iff\quad & \varphi(a)^{-1}\varphi(b) = e_H && \text{using that } \varphi \text{ is a homomorphism (1.16)} \\
\iff\quad & \varphi(a) = \varphi(b) \\
\iff\quad & \overline{\varphi}(a\ker\varphi) = \overline{\varphi}(b\ker\varphi). && \text{using the definition of } \overline{\varphi}
\end{aligned}$$

  The direction "$\Rightarrow$" shows that $\overline{\varphi}$ is well-defined. Note that "$\Leftarrow$" shows that $\overline{\varphi}$ is injective.
- Next, we show that $\overline{\varphi}$ is a homomorphism. For any $a, b \in G$,

$$\begin{aligned}
\overline{\varphi}(a\ker\varphi \cdot b\ker\varphi) &= \overline{\varphi}(ab\ker\varphi) && \text{using the operation of the quotient group (2.5)} \\
&= \varphi(ab) && \text{using the definition of } \overline{\varphi} \\
&= \varphi(a)\cdot\varphi(b) && \text{using that } \varphi \text{ is a homomorphism (1.16)} \\
&= \overline{\varphi}(a\ker\varphi)\cdot\overline{\varphi}(b\ker\varphi). && \text{using the definition of } \overline{\varphi}
\end{aligned}$$

- Finally, we observe that $\overline{\varphi}$ is surjective. That is, for any $a \in \operatorname{im}\varphi$, we have that $a\ker\varphi \in G/\ker\varphi$. □

Example 3.2: Homomorphism theorem

We have already seen in example 1.29 that for any field K, $\det : \mathrm{GL}_n(K) \to K \setminus \{0\}$ is a homomorphism with $\ker \det = \mathrm{SL}_n(K)$. Thus, by the homomorphism theorem,

$$\mathrm{GL}_n(K)/\mathrm{SL}_n(K) \cong K \setminus \{0\}. \tag{3.2}$$

Theorem 3.3 (Correspondence Theorem)**.** *The mapping,*

$$f : \{U \leq G \mid N \subseteq U\} \to \{V \leq G/N\}, \quad U \mapsto U/N, \tag{3.3}$$

is an inclusion-preserving[1] *bijection and fore every* $U \leq G$*,*

$$U \trianglelefteq G \iff U/N \trianglelefteq G/N. \tag{3.4}$$

A sketch of the correspondence theorem is given in fig. 3.1.

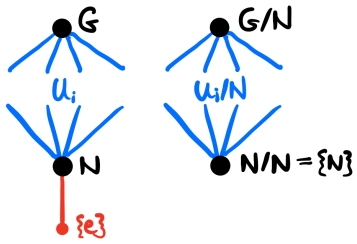


Figure 3.1: Sketch of the correspondence of subgroups U_i "between" G and N and the subgroups U_i/N "between" G/N and N/N.

[1] We say that a mapping $f : A \to B$ is *inclusion-preserving* if for any $a_1, a_2 \in A$ such that $a_1 \subseteq a_2$, we have $f(a_1) \subseteq f(a_2)$.

Theorem 3.4 (First Isomorphism Theorem)**.** *Let* $U \leq G$ *and* $N \trianglelefteq G$*. Then,*

(a) $UN \leq G$ *where* $UN \doteq \{x \cdot n \mid x \in U, n \in N\}$
(b) $U \cap N \trianglelefteq U$
(c) $UN/N \cong U/(U \cap N)$

A sketch of the correspondence theorem is given in fig. 3.2.

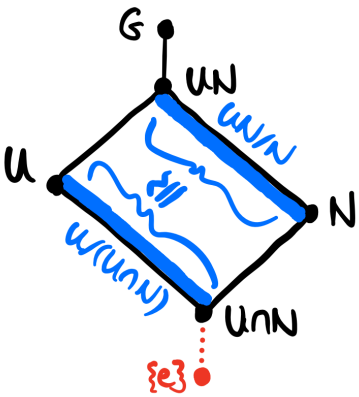


Figure 3.2: Sketch of the first isomorphism theorem.

Theorem 3.5 (Second Isomorphism Theorem)**.** *Let* $U, N \trianglelefteq G$ *with* $N \subseteq U$*. Then,* $(G/N)/(U/N) \cong G/U$*.*

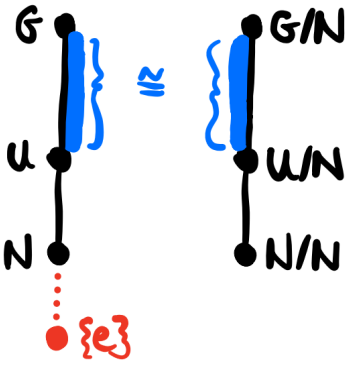


Figure 3.3: Sketch of the second isomorphism theorem..

4
Group Actions

5
Sylow Theorems

6
Direct Products and Abelian Groups

7
Solvable Groups

Part II

Rings

8
Rings and Ideals

9
Homomorphisms and Quotient Rings

10
Divisors in Integral Domains

11
Polynomial Rings

12
Factorial Rings

13
Euclidean Domains and Principal Ideal Domains

14
Irreducibility of Polynomials

Part III

Fields

15
Fields

Definition 15.1 (Field)**.**

16
Algebraic Field Extensions

17
Splitting Fields

18
Normal and Separable Field Extensions

19
Galois Theory

20
Finite Fields

21
Cyclotomic Fields

22
Solvable Polynomials

Summary of Notation

We follow these general rules:

- lowercase italic for indices i and scalar variables a
- uppercase italic bold for matrices $\boldsymbol{M}$
- uppercase italic for sets A

$\doteq$	equality by definition
$\mathbb{N}$	set of natural numbers $\{1, 2, \dots\}$
$\mathbb{N}_0$	set of natural numbers, including 0, $\mathbb{N} \cup \{0\}$
$[n]$	set of natural numbers from 1 to n, $\{1, 2, \dots, n-1, n\}$
$\mathbb{Z}$	set of integers $\{\dots, -2, 1, 0, 1, 2, \dots\}$
$\mathbb{R}$	set of real numbers
$\mathbb{C} = \mathbb{R}^2$	set of complex numbers
$A \cup B$	disjoint union of sets A and B
$f : A \to B$	function f from elements of set A to elements of set B
$a \mid b$	a is a divisor of b

GROUPS

$U \leq G$	U is a subgroup of G
$\langle M \rangle \leq G$	for $M \subseteq G$, the subgroup generated by M
$\langle a \rangle$	the cyclic group $\langle \{a\} \rangle$
$o(a)$	order of element a, $\lvert\langle a \rangle\rvert$
aU	left coset of $a \in G$ and $U \leq G$, $\{a \cdot u \mid u \in U\}$
Ua	right coset of $a \in G$ and $U \leq G$, $\{u \cdot a \mid u \in U\}$
$[G : U]$	index of $U \leq G$ in G, $\lvert\{aU \mid a \in G\}\rvert$
$\ker \varphi$	kernel of homomorphism $\varphi : G \to H$, $\{a \in G \mid \varphi(a) = e_H\} \subseteq G$
$\operatorname{im} \varphi$	image of homomorphism $\varphi : G \to H$, $\{\varphi(a) \mid a \in G\} \subseteq H$
$G \cong H$	G and H are isomorphic
$N \trianglelefteq G$	N is a normal subgroup of G
$\overline{a} = aN$	the (left) coset of some $a \in G$ in the context of the quotient group G/N
$\mathrm{GL}_n(K)$	*general linear group* over invertible linear maps $\boldsymbol{A} \in K^{n \times n}$, $\det \boldsymbol{A} \neq 0$
$\mathrm{SL}_n(K)$	*special linear group* over volume-preserving linear maps $\boldsymbol{A} \in K^{n \times n}$, $\det \boldsymbol{A} = 1$

S_n	*symmetric group* over bijections on $[n]$ (so-called permutations)
A_n	*alternating group* over bijections σ on $[n]$ with positive sign, $\operatorname{sgn}\sigma = 1$
$Z(G)$	*center* of group G, $\{a \in G \mid \forall x \in G.\ ax = xa\} \trianglelefteq G$
$\mathrm{Aut}(G)$	*automorphism group* over automorphisms on G
$\mathrm{Inn}(G)$	*inner automorphism group* over inner automorphisms on G
G/N	for some $N \trianglelefteq G$, *quotient group* G modulo N over (left) cosets of N
$n\mathbb{Z} = \langle n \rangle$	subgroup $n\mathbb{Z} \leq \mathbb{Z}$ of multiples of $n \in \mathbb{Z}$
$Z_n = \mathbb{Z}/n\mathbb{Z}$	quotient group $\mathbb{Z}$ modulo $n\mathbb{Z}$, $\langle \overline{1} \rangle = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$
$\mathrm{Out}(G)$	*outer automorphism group* over cosets of the inner automorphism group and outer automorphisms on G, $\mathrm{Aut}(G)/\mathrm{Inn}(G)$
i_g	*inner automorphism* of some conjugating element $g \in G$, $i_g : G \to G, x \to g \cdot x \cdot g^{-1}$

Index