Group Theory

Zambelli Lorenzo
BSc Applied Mathematics

September 2021-October 2021

1 Introduction

As the name of the course suggest, gruop is the central notion of this course. The first abstract definition of this concept was formulated by the German mathematician W.F.A. von Dyck (1856– 1934). Algebra courses starting from abstract definitions of this kind were started in Gottingen around 1920, notably by the famous female mathematician Emmy Noether (1882–1935). A young student from Amsterdam, B.L. van der Waerden, attended her courses. He extended his algebra knowledge with the help of Emil Artin (1898–1962) in Hamburg. In 1928, only 25 years old, Van der Waerden was appointed mathematics professor in Groningen where he wrote what is probably the most influential textbook on abstract algebra to date. It appeared in 1930 and completely adopts the abstract definition/theorem/proof style. The book made Van der Waerden, who died in 1996, world famous. Due to Noether's and Artin's lectures and Van der Waerden's recording of this, abstract algebra is still taught all over the world essentially exclusively in this style.

2 Modular Arithmetic

Definition 1 (II.1.1) *Let N be a positive integer. Two intergers a, b are called congruent modulo N if $N \mid a - b$. This denoted by $a \equiv b \mod N$. We call N the modulus.*

Lemma 2 (II.1.2) *Let $a, b, c \in \mathbb{Z}$. Then the following assertions hold.*

- *(Reflexivity) We have $a \equiv a \mod N$*
- *(Symmetry) We have $a \equiv b \mod N$ if and only if $b \equiv a \mod N$*
- *(Transitivity) If $a \equiv b \mod N$ and $b \equiv c \mod N$, then $a \equiv c \mod N$*

Definition 3 (II.1.3) *For $a \in \mathbb{Z}$ the residue class of a modulo N is defined as*

$$\{b \in \mathbb{Z} \mid b \equiv a \mod N\} = a \mod N$$

We also write $\overline{a}$ for $a \mod N$. If $b \in a \mod N$, then we call b a representative for $a \mod N$

Lemma 4

1. *We have $a \mod N = \{a + Nk \mid k \in \mathbb{Z}\}$*
2. *The sets $a \mod N$ for distinct $0 \leq a < N$ are all distinct*

We denote the set of residue classes modulo N by $\mathbb{Z}/N\mathbb{Z} = \{\overline{0}, \overline{1}, ..., \overline{N-1}\}$

Lemma 5 (II.1.5) *For $a, b \in \mathbb{Z}$ one has $\overline{a} = \overline{b}$ modulo N if and only if $a \equiv b \mod N$*

Theorem 6 (II.1.6) *Let $\overline{a_1}, \overline{a_2}, \overline{b_1}, \overline{b_2}$ be residue classes modulo N, where $a_1, a_2, b_1, b_2 \in \mathbb{Z}$. Suppose $\overline{a_1} = \overline{b}$ and $\overline{b_1} = \overline{b_2}$. Then*

$$\overline{a_1 + b_1} = \overline{a_2 + b_2} \quad \textit{and} \quad \overline{a_1 b_1} = \overline{a_2 b_2}$$

Definition 7 (II.1.7) *(Adding and multiplying residue classes) We denote the set of residue classes modulo N by $\mathbb{Z}/N\mathbb{Z}$. For $\overline{a}, \overline{b} \in \mathbb{Z}/N\mathbb{Z}$ we define*

$$\overline{a} + \overline{b} = \overline{r_1 + r_2} \quad \textit{and} \quad \overline{a} \cdot \overline{b} = \overline{r_1 \cdot r_2}$$

with r_1, r_2 be arbitrary elements in $\overline{a}, \overline{b}$ respectively.

Definition 8 (II.2.1) *A residue class $a \mod N$ is called unit modulo N if there exists a residue class $b \mod N$ such that*

$$(a \mod N) \cdot (b \mod N) = 1 \mod N$$

The subset of $\mathbb{Z}/N\mathbb{Z}$ consisting of all units modulo N is denoted as $(\mathbb{Z}/N\mathbb{Z})^\times$

Definition 9 (II.2.4) *(Euler totient function or Euler's phi function) The number of elements of $(\mathbb{Z}/N\mathbb{Z})^\times$ is denoted by $\varphi(N)$*

Corollary 10 (II.2.5) *The number $\varphi(N)$ equals the number of integers $a \in \mathbb{Z}$ with $1 \leq a \leq N$ and $\gcd(a, N) = 1$. In particular, a positive integer p is prime if and only if $\varphi(p) = p - 1$*

Theorem 11 (II.2.3) *Let $a \in \mathbb{Z}$. Then $a \mod N \in (\mathbb{Z}/N\mathbb{Z})^\times$ if and only if $\gcd(a, N) = 1$*

Theorem 12 (II.2.6)

1. *If $a \mod N$ and $b \mod N$ are units modulo N, then so is their product*
2. *If $a \mod N \in (\mathbb{Z}/N\mathbb{Z})^\times$, then a residue class $b \mod N$ such that $(a \mod N) \cdot (b \mod N) = 1 \mod N$ is also a unit modulo N*
3. *For each $a \mod N \in (\mathbb{Z}/N\mathbb{Z})^\times$ there is a unique class $b \mod N \in (\mathbb{Z}/N\mathbb{Z})^\times$ with $(a \mod N) \cdot (b \mod N) = 1 \mod N$*

Theorem 13 (II.2.10) *(Euler) For all $a \mod N \in (\mathbb{Z}/N\mathbb{Z})^\times$ one has*

$$(a \mod N)^{\varphi(N)} = 1 \mod N$$

Corollary 14 (II.2.11 Fermat's Little theorem) *If p is prime, then $(a \mod p)^p = a \mod p$ for every $a \in \mathbb{Z}$*

2.1 The Chinese Remainder Theorem

Theorem 15 (II.3.4 The Chinese remainder theorem) *Let N, M be positive integers with $\gcd(N, M) = 1$. The map*

$$f : \mathbb{Z}/NM\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/M\mathbb{Z}$$
$$a \mod NM \mapsto (a \mod N, a \mod M)$$

is well-defined. this map is a group isomorphism. Moreover it induces a group isomorphism between $(\mathbb{Z}/NM\mathbb{Z})^\times$ and $(\mathbb{Z}/N\mathbb{Z})^\times \times (\mathbb{Z}/M\mathbb{Z})^\times$

Lemma 16 (II.3.1) *Suppose $N, M \in \mathbb{Z}$ are positive. The map*

$$f : \mathbb{Z}/NM\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/M\mathbb{Z}$$
$$a \mod N \mapsto a \mod M)$$

is well-defined if and only if $M|N$.
Here well-defined means that the image of $a \mod N$ does not depend on the choice of the representative in $a \mod N$. In other words, if $a \mod N = b \mod N$ then we have $a \mod M = b \mod M$ (if $N|b - a$ then $M|b - a$)

Corollary 17 (II.3.8) *Euler's totient function has the property $\varphi(NM) = \varphi(N) \cdot \varphi(M)$ for all positive coprime integers N, M.*

3 Groups

Definition 18 (III.1.1) *A group is a triple $(G, \cdot, e)$ where G is a set, $e \in G$, and $\cdot$ is a map from $G \times G$ to G, which we write as $(x, y) \to x \cdot y$, satisfying*

G1 (associativity) For all $x, y, z \in G$ we have $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
G2 (unit element) For all $x \in G$ we have $e \cdot x = x = x \cdot e$
G3 (inverses) For all $x \in G$ a $y \in G$ exists such that $x \cdot y = e = y \cdot x$
G4 (commutative or abelian) For all $x, y \in G$ we have $x \cdot y = y \cdot x$
The order of the group $(G, \cdot, e)$ is the number of elements in G. We call a group finite if it has finite order

Theorem 19 (III.1.6) *Let $(G, \cdot, e)$ be a group.*

1. *If $e' \in G$ satisfies $e'x = x$ or $xe' = x$ for some $x \in G$, then $e' = e$*
2. *For every $x \in G$ there is precisely one $y \in G$ with $xy = e = yx$*
3. *For any fixed $a \in G$, the map $\lambda_a : G \to G$; $x \to ax$ is a bijection from G to itself. Similarly, $\rho_a : G \to G$; $x \to xa$ is a bijection*

Definition 20 (III.1.7) *Let $(G, \cdot, e)$ be a group and $x \in G$. The element $y \in G$ such that $xy = e = yx$ is called the inverse of x in G. It is denoted by x^{-1}, by Theorem III.1.6 x^{-1} is unique and hence well-defined.*
In case of an abelian group G with group law denoted as $+$, this inverse element is called the opposite of x in G, and it is denoted as $-x$.

Corollary 21 (III.1.9) *Let G be a group and let $a, a_1, ..., a_n \in G$. Then we have*

1. $(a^{-1})^{-1} = a$
2. $(a_1 \cdots a_n)^{-1} = a_n^{-1} \cdot a_{n-1}^{-1} \cdots a_1^{-1}$
3. $(a^n)^{-1} = (a^{-1})^n$

3.1 Subgroups

Definition 22 (III.2.1) *Let $G = (G, \cdot, e)$ be a group. A group H is called subgroup of G if H is a subset of G, and the unit element and the group law of H and G are the same. In this case e write $H \leq G$. We call H a proper subgroup if H is a proper subset of G.*

Theorem 23 (III.2.3) *(Subgroup criterion) Let $(G, \cdot, e)$ be a group and $H \subset G$. Then H forms a subgroup of G if and only if*

H1 $e \in H$
H2 *For all $x, y \in H$ also $x \cdot y \in H$*
H3 *For all $x \in H$ also $x^{-1} \in H$*

Theorem 24 (III.2.8 Theorem of Lagrange) *If H is a subgroup of a finite group G, then the order of H is a divisor of the order of G, i.e, $\#H | \#G$*

Definition 25 (III.2.9) *Let x be an element of a group G. Then we define the order of x, notation $\mathrm{ord}(x)$, as follows. If an integer $m > 0$ exists with $x^m = e$, then $\mathrm{ord}(x)$ is defined to be the smallest such m. Otherwise, we set $\mathrm{ord}(x) = \infty$*

Theorem 26 (III.2.11) *Let G be a group and an element $x \in G$. Then the following statements hold true:*

1. $\mathrm{ord}(x) = \mathrm{ord}(x^{-1})$
2. *If $\mathrm{ord}(x) < \infty$, then $\langle x \rangle = \{x, x^2, ..., x^{\mathrm{ord}(x)} = e\}$*
3. *$\mathrm{ord}(x) = \# \langle x \rangle$, i.e. the order of the subgroup generated by x is the order of x*
4. *if $\#G < \infty$, then also $\mathrm{ord}(x) < \infty$ and moreover $\mathrm{ord}(x) | \#G$*
5. *If $x^n = e$, then $\mathrm{ord}(x) | n$*

Definition 27 (III.2.13 Product of groups) *Given two groups $(G_1, *, e_1)$ and $(G_2, @, e_2)$, the product set*

$$G_1 \times G_2 = \{(g_1, g_2) : g_1 \in G_1, g_2 \in G_2\}$$

can be given the structure of a group as follows. The unit element is the pair (e_1, e_2). The group las is given by

$$(x_1, x_2) \circ (y_1, y_2) = (x_1 * y_1, x_2 @ y_2)$$

Definition 28 (Cyclic) *A group G is called cyclic if $G = \langle g \rangle$ for some $g \in G$. The element g is called a generator of G*

Proposition 29 *If G is a finite group and $g \in G$, then G is cyclic and generated by g if and only if $\mathrm{ord}(g) = \#G$*

3.2 Homomorphisms

Definition 30 (III.3.1) *Let $(G_1, @, e_1)$ and $(G_2, *, e_2)$ be groups. A homomorphism from G_1 to G_2 is a map $f : G_1 \to G_2$ satisfying $f(x@y) = f(x) * f(y)$ for all $x, y \in G_1$.*

- *An isomorphism from G_1 to G_2 is a bijective homomorphism. We call G_1 and G_2 isomorphic, and write $G_1 \cong G_2$ if an isomorphism from G_1 to G_2 exists*

Theorem 31 (III.3.3) *Given a homomorphism $f : (G_1, \square, e_1) \to (G_1, *, e_2)$, the following holds true:*

1. $f(e_1) = e_2$
2. *If $x \in G_1$, then we have $f(x^{-1}) = (f(x))^{-1}$*
3. *If f is an isomorphism, then so is the inverse of f*
4. *If $g : (G_2, *, e_2) \to (G_3, @, e_3)$ is a homomorphism as well, then so is the composition $g \circ f$*

Theorem 32 (III.3.4) *Let $f : (G_1, \circ, e_1) \to (G_2, *, e_2)$ a homomorphism and let $H_i \leq G_i$ be subgroups for $i = 1, 2$. Then $f(H_1)$ is a subgroup of G_2, and $f^{-1}(H_2)$ is a subgroup of G_1*

Definition 33 (III.3.5) *If $f : (G_1, \square, e_1) \to (G_2, *, e_2)$ is a homomorphism, then the kernel of f, denoted by $\ker(f)$, is defined as*

$$\ker(f) = \{x \in G_1 \mid f(x) = e_2\}$$

Theorem 34 (III.3.6) *Let $f : (G_1, \square, e_1) \to (G_2, *, e_2)$ be a homomorphism. Then*

1. $\ker(f)$ *is a subgroup of G_1;*
2. *f is injective if and only if* $\ker(f) = e_1$

Let $G_1, \cdot, e_1)$ and $G_2, *, e_2)$ be two groups. Let $f : G_1 \to G_2$ be an isomorphism, meaning:

- f is a homomorphism
- f is a bijection

The following properties hold:

1. G_1 is abelian if and only if G_2 is abelian
2. If $x \in G_1$ is of order k then $f(x)$ is of order k
3. $\#G_1 = \#G_2$. Moreover, if $H \leq G_1$ is of order k then the subgroup $f(H)$ is of order k

4 Group of Permutations

Let Σ be a non-empty set. Let S_Σ be a set of all bijections from Σ to Σ. Then S_Σ is a group with respect to composition of maps

Definition 35 (IV.1.1) *The group $(S_\Sigma, \circ, id_\Sigma)$ is called symmetric group on the set Σ*

Theorem 36 (IV.1.3) *Suppose that $f : \Sigma \to \Sigma'$ is a bijection and $g : \Sigma' \to \Sigma$ is its inverse. Then S_Σ and $S_{\Sigma'}$ are isomorphic; and explicit isomorphism $\varphi : S_\Sigma \to S_{\Sigma'}$ is given by $\varphi(\sigma) = f \circ \sigma \circ g$, with as inverse $\psi : S_{\Sigma'} \to S_\Sigma$ given by $\psi(\tau) = g \circ \tau \circ f$*

Theorem 37 (IV.1.4 Caayley's theorem) *Every group G is isomorphic to a subgroup of S_G*

4.1 Permutations on n integers

Let Σ be a finite set of integers

Definition 38 (IV.2.1) *The symmetric group on n integers, denoted by S_n, is defined as the group $S_{1,2,\ldots,n}$. Elements of this group are called permutations. The group S_n is also called the permutation group on n elements*

Corollary 39 (IV.2.2) *A finite group G is isomorphic to a subgroup of $S_{1,\ldots,n}$*

Theorem 40 (IV.2.3) *The group S_n consists of $n!$ elements*

Definition 41 (IV.2.4) *A permutation $\sigma \in S_n$ is called a cycle of length k (or a k-cycle), if there exist k distinct integers $a_1, \ldots, a_k \in \{1, \ldots, n\}$ such that $\sigma(a_i) = a_{i+1}$ for $1 \leq i < k$ and $\sigma(a_k) = a_1$ and $\sigma(x) = x$ for $x \notin \{a_1, \ldots, a_k\}$. Such a permutation is denoted by $\sigma(a_1a_2\ldots a_k)$. A 2-cycle is also called a transposition.*
If two cycles $(a_1a_2\ldots a_k)$ and $(b_1b_2\ldots b_l)$ satisfy $\{a_1a_2\ldots a_k\} \cap \{b_1b_2\ldots b_l\} = \emptyset$ they are disjoint

Theorem 42 (IV.2.6) *Every $\sigma \in S_n$ can be written as a product $\sigma = \sigma_1 \cdots \sigma_r$ where the σ_i are pairwise disjoint cycles. A part from the order of the σ_i, this persentation is unique*

Theorem 43 (IV.2.8) *Let $\sigma = (i_1i_2\ldots i_k) \in S_n$ be a $k-$cycle. Then we have*

1. $\sigma^{-1} = (i_ki_{k-1}\ldots i_1)$
2. $\mathrm{ord}(\sigma) = k$
3. *if $\sigma_1, \ldots, \sigma_r$ are pairwise disjoint cycles, then $(\sigma_1\ldots\sigma_r)^n = \sigma_1^n\ldots\sigma_r^n$ for all $n \in \mathbb{Z}$*
4. *If σ_i has length l_i $(i = 1, \ldots, r)$, then $\mathrm{ord}(\sigma_1\ldots\sigma_r) = lcm(l_1, \ldots, l_r)$*

Lemma 44 *Let σ be a permutation of S_n and let $x \in \{1, 2, \ldots, n\}$. Then there exists an integer k such that $\sigma^k(x) = x$. If k is the smallest such integer then the elements in $\{x, \sigma(x), \ldots, \sigma^{k-1}(x)\}$ are all distinct*

Theorem 45 (IV.2.11) *Every permutation $\sigma \in S_n$ can be written as a product of transpositions $(2 - cycles)$*

4.2 Even and odd permutations

Definition 46 (Notation IV.3.1) *1. For $n \geq 2$ write $X := \{(i,j) \in \mathbb{Z} \times \mathbb{Z} \,|\, 1 \leq i < j \leq n\}$*

2. For $\sigma \in S_n$ define

$$\begin{aligned} f_\sigma &: X \to X \\ (i,j) &\mapsto (\min\{\sigma(i), \sigma(j)\}, \max\{\sigma(i), \max(j)\} \end{aligned}$$

3. finally define

$$\begin{aligned} h_\sigma &: X \to \mathbb{Q} \\ (i,j) &\mapsto \frac{\sigma(j) - \sigma(i)}{j - i} \end{aligned}$$

Lemma 47 (IV.3.2) *Let $n \geq 2$. Then the following holds:*

1. *For $\sigma, \tau \in S_n$ one has $f_{\sigma\tau} = f_\sigma \circ f_\tau$*
2. *The map f_σ is a bijection on X*
3. *We have $\prod_{(i,j)\in X} h_\sigma(i,j) = \pm 1$*

Definition 48 (IV.3.3) *We define the sign of a permutation $\sigma \in S_n$ by*

$$\epsilon(\sigma) = \prod_{(i,j)\in X} h_\sigma(i,j) = \prod_{1 \leq 1 < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i} = \pm 1$$

We call σ even if $\epsilon(\sigma) = 1$ and odd otherwise.

Theorem 49 (IV.3.5) *The sign $\epsilon : S_n \to \{+1, -1\}$ is a homomorphism*

Lemma 50 (IV.3.6) *1. We have $\rho \circ (a_1 a_2 ... a_l) \circ \rho^{-1} = (\rho(a_1)\rho(a_2)...\rho(a_l))$ for any $\rho \in S_n$ and any $l-$cycle $(a_1 a_2 ... a_l) \in S_n$*

2. Every transposition is odd

Corollary 51 (IV.3.7) *1. An l-cycle σ has sign $\epsilon(\sigma) = (-1)^{l-1}$*

2. If σ is a product of cycles of lenghts $l_1, ..., l_r$ then $\epsilon(\sigma) = (-1)^{\sum_{i=1}^{r}(l_i - 1)}$

3. A permutation σ is even if and only if σ can be written as a product of an even number of $2 - $cycles

4.3 The alternating group

Definition 52 (IV.4.1) *For $n \geq 1$ the alternating group is the subgroup of S_n consosting of all even permutations. We denote it by A_n*

Theorem 53 (IV.4.3) *For $n \geq 2$ the group A_n consists of $n!/2$ elements*

Theorem 54 (IV.4.4) *For $n \geq 3$ the elements of A_n can be written as products of $3-$cycles*

5 Some groups of matrices

Definition 55 (V.1.1) *The set of all linear maps* $\varphi : \mathbb{R}^n \to \mathbb{R}^n$ *satisfying* $\langle v, w\rangle = \langle \varphi(v), \varphi(w)\rangle$ *for all* $v, w \in V$, *is denoted by* $O(\mathbb{R}^n, \langle\cdot,\cdot\rangle)$.

Theorem 56 (V.1.2) *The set* $O(\mathbb{R}^n, \langle\cdot,\cdot\rangle)$ *is a group with respect to the composition of linear maps*

Definition 57 (V.1.4)

1. *The orthogonal group*

$$O(n) = \{A \in GL_n(\mathbb{R}) \,|\, A * A = I\}$$

2. *The unitary group*

$$U(n) = \{A \in GL_n(\mathbb{C}) \,|\, A * A = I\}$$

3. *The special orthogonal group*

$$SO(n) = \{A \in GL_n(\mathbb{R}) \,|\, A * A = I \;\; and \;\; \det(A) = 1\}$$

4. *The special unitary group*

$$SU(n) = \{A \in GL_n(\mathbb{C}) \,|\, A * A = I \;\; and \;\; \det(A) = 1\}$$

Remark: In $O(2)$ we have the following matrices

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \left\{ \underbrace{\begin{bmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{bmatrix}}_{\text{rotations}} \right\} \cup \underbrace{\left\{ \begin{bmatrix} \cos\phi & \sin\phi \\ \sin\phi & -\cos\phi \end{bmatrix} \right\}}_{\text{refelctions w.r.t a line origin}}$$

Instead, in $SO(2)$ we just have the rotations.

Definition 58 (V.2.1) *An isometry on* $\mathbb{R}^n$ *is a map* $\varphi : \mathbb{R}^n \to \mathbb{R}^n$ *with the property* $d(u, v) = d(\varphi(u), \varphi(v))$ *for all* $u, v \in \mathbb{R}^n$

Remark: the map does not have to be linear.
Composition of isometries is an isometry.
exemples: rotations, reflections, translations

Theorem 59 (V.2.3)

1. *An isometry on* $\mathbb{R}^n$ *mapping* $0 \in \mathbb{R}^n$ *to 0 is linear*
2. *The linear isometries on* $\mathbb{R}^n$ *are exactly the elements of* $O(\mathbb{R}^n, \langle,\rangle) = O(n)$
3. *Every isometry can be written as a composition of a translation and a linear isometry*
4. *Isometry are invertible*

Remark:

- The set of all Isometries on $\mathbb{R}^n$ is a group with respect to the composition of maps

- The set of all linear isometries on $\mathbb{R}^n$ is a subgroup of the group of all isometries

Definition 60 (V.2.4) *The symmetry group of a subset $F \subset \mathbb{R}^n$ is defined as the group of all isometries on $\mathbb{R}^n$ mapping F to F*

Theorem 61 (V.2.5) *If $F \subset \mathbb{R}^n$, $a \in \mathbb{R}_{>0}$ and φ is a isometry on $\mathbb{R}^n$, then the symmetry group of $a\varphi(F)$ and of F are isomorphic*

Remark: this theorem says that, up to isomorphism, the symmetry group of a set is not affected by the position of the set or the scaling of the set in $\mathbb{R}^n$, but only by the shape of the set

5.1 The dihedral groups

Definition 62 (V.3.1) *The symmetry group of a circle is called the infinite dihetral group. This group is denoted by D_∞*

Theorem 63 (V.3.2)

- *The group D_∞ is isomorphic to $O(2)$*
- *The subset $R \subset D_\infty$ of all rotations is a subgroup of D_∞ that is isomorphic to $SO(2)$*
- *if $\sigma \in D_\infty$ is any reflection, then*

$$D_\infty = R \sqcup \sigma \cdot R$$

Taking σ the reflection across the y-axis, we have $\sigma\rho\sigma = \rho^{-1}$ for any $\rho \in R$

Definition 64 (V.3.3) *The symmetry group of F_n is called the $n - th$ dihedral group D_n*

Theorem 65 (V.3.4)

- *The group D_n contains the rotation ρ by an angle $2\pi/n$ and the reflection σ in the y-axis. Every element of D_n can be written in a unique way as ρ^k or $\sigma\rho^k$, for some $0 \leq k < n$*
- *The group D_n consistes of $2n$ elements. It is abelian if and only if $n = 2$*
- *one has $\operatorname{ord}(\rho) = n$ and $\operatorname{ord}(\sigma\rho^k) = 2$, so in particular $\rho^n = \sigma^2 = id$. Moreover, $\sigma\rho\sigma = \rho^{-1}$*
- *The subgroup R_n of D_n consisting of all rotations is isomorphic to $\mathbb{Z}/n\mathbb{Z}$*

6 Conjugation

Definition 66 (VI.1.1) *Let G is a group and $a \in G$. Then the map*

$$\begin{aligned} \gamma_a : G &\to G \\ g &\mapsto aga^{-1} \end{aligned}$$

is a bijection and called the conjugation by a

Theorem 67 (VI.1.2) *Let G be a group and let $a, b \in G$*

1. *The conjugation γ_a by a is an isomorphism*
2. *the conjugations γ_a, γ_b satisfy $\gamma_a\gamma_b = \gamma_{ab}$*
3. *The inverse of γ_a is $\gamma_{a^{-1}}$*
4. *If H is a subgroup of G, then so is $\gamma_a(H) = aHa^{-1}$, and $H \cong aHa^{-1}$*

Definition 68 (VI.1.5) *Two elements x, y in a group G are called conjugate if a conjugation γ_a for some $a \in G$ exists with $\gamma_a(x) = y$*
The conjugacy class of $x \in G$ dfiend as the subset of G given by

$$C_x = \{y \in G |\, \text{there exists } a \in G \text{ with } \gamma_a(x) = y$$

Remark: A group G is commutative if and only if $C_g = \{g\}$ for every element $g \in G$

Theorem 69 *Let G be a group and let $x, y, z \in G$*

1. *The element x is conjugate to iteself, so $x \in C_x$*
2. *If x is conjugate to y, then also y is conjugate to x (so $x \in C_x$ implies $y \in C_x$)*
3. *if $x \in C_y$ and $y \in C_z$, then $x \in C_z$*

Corollary 70 (VI.1.9) *every group G is the disjoint union of conjugacy classes. In other words, every elements of G lies in some C_x, and if there is an element in both C_x and C_y, then $C_x = C_y$*

Remark: let $\sigma \in S_n$, lets n_i be the leingths of the disjoints cycles σ_i with $n_1 \leq n_2 \leq \cdot \leq n_s$, then $[n_1, n_2, \cdots, n_s]$ is the cycle type of σ

Claim: Let $\sigma \in S_n$ be of cycle type $[n_1, n_2, ..., n_s]$ Then

$$\begin{aligned} C_\sigma &= \{\varphi_\tau(\sigma) = \tau\sigma\tau^{-1} : \tau \in S_n\} \\ &= \{\tau \in S_n : \tau \text{ has cycle type } [n_1, n_2, ..., n_s]\} \end{aligned}$$

Claim: Denote the conjugacy classes of permutation of cycle type $[n_1, n_2, ..., n_s]$ by $C_{[n_1,...,n_s]}$. Then

$$S_n = \bigcup C_{[n_1,...,n_s]}$$

where the union runs over all possible ordered interges $1 \leq n_1 \leq \cdots \leq n_s \leq n$ suhc that $n = n_1 + \cdots + n_s$. Note that we can also write $S_n = \bigcup C_\sigma$ where σ's are permutations in S_n with pairwise distinct cycle types.

Theorem 71 (VI.1.13) *If G is a group and $a \in G$, then*

$$N(a) = \{g \in G \,|\, \gamma_g(a) = a\}$$

is a subgroup of G. If G is finite, then

$$\#G = \#C_a \cdot \#N(a)$$

This group is called the centralizer of a

6.1 Index

Definition 72 (VI.2.1) *For H a subgroup of a group G, a left coset of H in G is any subset of the form gH; for $g \in G$.*
The set consisting of all left cosets of H in G is denoted by $G/H := \{gH : g \in G\}$

Definition 73 *The index of H in G is defiend as the number of disjoint left cosets of H in G and denoted by $[G : H]$. If the index is not finite then we write $[G : H] = \infty$*

Theorem 74 *If G is a finite group, then $[G : H]$ is finite for all subgroups H. Moreover, we have*

$$\#G = [G : H] \cdot \#H$$

6.2 Action, Orbit, Stabilizer

Definition 75 (VI.3.1) *Let $(G, *)$ be a group and X a nonempty set. A group action of G on X is a map*

$$\begin{aligned} G \times X &\to X \\ (g, x) &\mapsto g \cdot x \end{aligned}$$

satisfying

A1 $e \cdot x = x$ *for every* $x \in X$ *(here* $e \in G$ *is the identity element)*

A2 $(g * h) \cdot x = g \cdot (h \cdot x)$ *for all* $g, h \in G$ *and all* $x \in X$

we say that G acts on X or X is a G-set

Theorem 76 (VI.3.3)
1. *an action of the group $(G, *)$ on a set X induces the homomorphism*

$$\begin{aligned} f : G &\to S_X = \{\text{bijections from } X \text{ to } X\} \\ g &\mapsto f(g) \end{aligned}$$

such that $f(g)(x) = gx$

2. *If $f : G \to S_X$ is any homomorphism, then $gx = f(g)(x)$ (for $g \in G$ and $x \in X$) defines an action of G on X*

Definition 77 (VI.3.5) *Let the group G act on the set X. Let $x \in X$. Then, the stabilizer of x in G, denoted by G_x or $Stab_G(x)$ is*

$$G_x = \{g \in G : gx = x\} \subseteq G$$

Theorem 78 (VI.3.7)
1. *G_x is a subgroup of G*
2. *For $x \in X$ and $g \in G$, one has $G_{gx} = gG_xg^{-1}$*

Definition 79 (VI.3.5) *Let the group G act on the set X. Let $x \in X$. Then, the orbit of x under G, denoted by Gx, is*

$$Gx = \{gx : g \in G\} \subseteq X$$

Theorem 80 (VI.3.7) *For $x, y \in X$ one has*

$$Gx = Gy \Leftrightarrow y \in Gx$$
$$Gx \cap Gy = \emptyset \Leftrightarrow y \notin Gx$$

Corollary 81 (VI.3.8) *Any G-set X is a disjoint union of orbits:*

$$X = \bigcup_{x \in X} Gx$$

Definition 82 (VI.3.5) *Let the group G act on the set X. Then, the action of G on X is called faithful if for every distinct pair $g, h \in G$ there exits $y \in X$ such that $g \cdot y \neq h \cdot y$. We also say that G acts faithfully on X.*

Remark: Faitfulness is equivalent to say that different group elements $g, h \in G$ induces different bijections $f(g), f(h) \in S_X$:

$$\begin{aligned} f : G &\to S_X \\ g &\mapsto f(g) \end{aligned}$$

with $f(g)(y) = g \cdot y \neq h \cdot y = f(h)(y)$ for some $y \in X$

Theorem 83 (VI.3.7) *The action of G on X is faithful $\Leftrightarrow$ The homomorphism $f : G \to S_X$ given by $f(g)(x) = g \cdot x$ is injective*

Definition 84 (VI.3.5) *Let the group G act on the set X. Then, the action of G on X is called transitive if for every pair $x_1, x_2 \in X$ there exists $g \in G$ with $gx_1 = x_2$. We say that G acts transitively on X*

Theorem 85 (VI.3.7) *The following are equivalent*

- *G acts transitively on X*
- *$Gx = X$ for some $x \in X$*
- *$Gx = X$ for all $x \in X$*

Definition 86 (VI.3.5) *Let the group G act on the set X. Then, the element $x \in X$ is called a fixpoint of G if $Gx = \{x\}$, in other words, if $gx = x$ for every $g \in G$. The set of all fixpoints in X is denoted X^G, so*

$$X^G := \{y \in X : gy = y \text{ for all } g \in G\}$$

The action of G on X is called fixpoint free, if there are no fixpoints, i.e. $X^G = \emptyset$

Theorem 87 (VI.3.9) *Suppose G is a group and X is a G-set (G acts on X). Let $x \in X$. Then*

$$\begin{aligned} G/G_x &\to Gx \\ gG_x &\mapsto gx \end{aligned}$$

is a well-defined bijective map

Theorem 88 (Orbit-Stabilizer theorem) *For any G-set X and any $x \in X$ one has*

$$\#Gx = [G : G_x]$$

Definition 89 (VI.3.12) *Gievan a group G and a finite G set X, the permutation character of the action is the function $\chi : G \to \mathbb{Z}$ given by*

$$\chi(g) = \#\{x \in X : gx = x\}$$

Theorem 90 (VI.3.13) *Let G be a finite group acting on a finite G-set X. The number of orbits in X under G is given by*

$$\#orbits = \frac{1}{\#G} \sum_{g \in G} \chi(g)$$

6.3 Sylow Theory

Definition 91 (VI.4.1) *Let G be a finite group and let p be a prime dividing the order of G.*
Write $\#G = p^n \cdot m$, where $n \geq 1$ and $gcd(p, m) = 1$.
A Sylow p-group in G is a subgroup $H \subset G$ with $\#H = p^n$.
We define $n_p(G)$ to be the number of pairwise distinct Sylow p-groups in G

Theorem 92 (VI.4.3 Sylow Theorem) *Let G be a finite group and p be a prime dividing the order of G. Write $\#G = p^n \cdot m$ where $n \geq 1$ and $gcd(p, m) = 1$*

1. *The group G contains a Sylow p-group*
2. *We have $n_p(G) \equiv 1 \, mod \, p$ and $n_p(G) | m$*
3. *If H and H' are Sylow p-groups in G then*

   $$H' = \gamma_a(H) = aHa^{-1}$$

   for some $a \in G$

Theorem 93 (VI.4.7) *Suppose $p \neq q$ are primes with $p \not\equiv 1 \, mod \, q$ and $q \not\equiv 1 \, mod \, p$, and G is a group with $\#G = pq$ then $G \cong \mathbb{Z}/pq\mathbb{Z}$*

Claim: If G is a cyclic group of order n, then $G \cong \mathbb{Z}/n\mathbb{Z}$ if $G = \langle g \rangle$ then

$$G \to \mathbb{Z}/n\mathbb{Z} \quad (1)$$
$$g \mapsto 1 \, modn \quad (2)$$

is a isomorphism.

Theorem 94 (VI.4.9 Cauchy's Theorem) *If G is a finite group and if p is a prime dividing the order of G, then there exists $g \in G$ with $ord(g) = p$*

7 Normal Subgroups

Definition 95 (VII.1.1) *A subgroup H of a group G is called normal if*

$$H = aHa^{-1} \quad \text{for all } a \in G$$

In other words, a subgroup $H \leq G$ is normal if

$$aha^{-1} \in H \quad \text{for all } h \in H, a \in G$$

we denote it by $H \lhd G$

Claims:

- If G is abelian then all subgroups are normal
- For any $n \in \mathbb{Z}_{>0}$ the alternating group A_n is a normal subgroup in S_n

Theorem 96 *Let G be a finite group and $\#G = p^n m$ with p prime, $n \geq 1$ and $gcd(p, m) = 1$. Consider a Sylow p-group $H \leq G$. Then H is a normal if and only if there is only one Sylow p-group in G*

Theorem 97 (VII.1.8) *Let G be a group and let $H \leq G$ be a subgroup. The following statements are equivalent:*

1. *H is normal in G, i.e., $aHa^{-1} = H$ for all $a \in G$*
2. *every $a \in G$ satisfies $aH = Ha$*
3. *For all $a \in G$ we have $aHa^{-1} \subset H$*
4. *For all $a, b, c, d \in G$ with $aH = cH$ and $bH = dH$ we also have $abH = cdH$*

Lemma 98 (VII.1.7) *If H is a subgroup of a group G and if $a, b \in G$, then $aH = bH$ if and only if $b^{-1}a \in H$*

Theorem 99 (VII.1.9) *If G is a subgroup and if H is a subgroup of G with $[G : H] = 2$, then $H \leq G$ is normal*

Remark:$[G : H] = \#G/\#H$

7.1 Factor groups

Definition 100 *The set*

$$G/H = \{gH : g \in G\}$$

forms a group with respect to $aH \cdot bH = abH$ and the identity element is H whenever H is a normal subgroup. This group is called the factor group of G modulo H.

Theorem 101 (VII.2.7) *If H is a normal subgroup of a group G, then the factor group G/H is abelian if and only if the element $a^{-1}b^{-1}ab$ is in H for all $a, b \in G$*

Theorem 102 (VII.2.9) *Let H be normal in a group G. The assignment*

$$\pi : G \to G/H \ : g \mapsto gH$$

defines a surjective homomorphism from G to G/H with $ker(\pi) = H$
The homomorphism ϕ is usually called the canonical homomorphism to a factor group

Theorem 103 (VII.2.11) *A subgroup H of a group G is normal if and only if H is the kernel of some homomorphism from G to another group*

7.2 Simple groups

Definition 104 (VII.3.1) *A group G is called simple if $\{e\}$ and G are the only normal subgroups in G.*

Proposition 105 *If G is a simple group, if G' is any group, and if $f : G \to G'$ a homomorphism, then either f is injective or f is the map sending every element of G to the unit element of G'*

8 Homomorphisms starting from a factor group

Let $\varphi : G/H \to G'$ be a homomorphis. Then

$$\psi : G \underset{\pi}{\to} G/H \underset{\varphi}{\to} G'$$

is a homomorphism since π is the canonical homomorphism and $\psi = \varphi \circ \pi$
Claim: $H \leq ker(\psi)$

Definition 106 (Criterion VIII.1.2) *Let H to be a normal subgroup of a group G, and consider an arbitrary group G'. Constructing a homomorphism $\varphi : G/H \to G'$ is done using the following recipe:*

1. *First find a homomorphism $\psi : G \to G'$ satisfying $H \subset ker(\psi)$*
2. *The homomorphism in 1. gives the well-defined map*

$$\begin{aligned} \varphi : G/H &\to G' \\ gH &\mapsto \psi(g) \end{aligned}$$

3. *The map $\varphi : G/H \to G'$ as in 2. is a homomorphism and we have $\psi = \varphi \circ \pi$, where π is the canonical homomorphism $G \to G/H$*

Theorem 107 (VIII.2.1 Homomorphism theorem) *If $\psi : G \to G'$ is a homomorphsim of groups, then $H = ker(\psi)$ is a normal subgroup of G and we have*

$$G/H \cong \psi(G) \leq G'$$

in particular, if ψ is surjective, then one has $G/H \cong G'$

Theorem 108 (VIII.2.4 Isomorphism Theorem) *Consider a group G, an arbitrary $H \leq G$, and a normal subgroup $N \leq G$. Then*

1. *$HN = \{hn | h \in H, n \in N\}$ is a subgroup of G*
2. *N is a normal subgroup of HN*
3. *$H \cap N$ is a normal subgroup of H*
4. *$H/(H \cap N) \cong HN/N$*

Theorem 109 (VIII.2.7 Second isomorphism theorem) *Consider a group G and a normal subgroup $N \leq G$*

1. *Every normal subgroup in G/N has the form H/N, with H a normal subgroup in G containing N*
2. *If $N \subset H$ for some normal subgroup H in G, then*

$$(G/N)/(H/N) \cong G/H$$

9 Finitely generated groups

Definition 110 (IX.1.1) *A group G is called finitely generated if there exist finitely many elements $g_1, ..., g_n \in G$ with the following property: Every $g \in G$ can be written as*

$$g = g_{i_1}^{\pm 1} \cdot \dots \cdot g_{i_t}^{\pm 1}$$

with indices $1 \leq i_j \leq n$ (note that is allowed here that $i_k = i_l$, in other words any g_i can be used multiple times)

Theorem 111 (IX.1.3) *Any finitely generated abelian group $(A, +, 0)$ is isomorphic to a factor group $\mathbb{Z}^n/H$ for some subgroup $H \leq \mathbb{Z}^n$*

9.1 Subgroups of $\mathbb{Z}^n$

Theorem 112 (IX.2.1) *If $H \leq \mathbb{Z}^n$ is a subgroup then $H \cong \mathbb{Z}^k$ for some k with $0 \leq k \leq n$*

Remark: An abelian group H is isomorphic to $\mathbb{Z}^k$ if and only if there exist $h_1, ..., h_k \in H$ such that every $h \in H$ can be written in a unique way as

$$h = m_1 h_1 + \dots + m_k h_k$$

A group H having this property is called a free abelian group (with basis $h_1, ..., h_k$).

Claim: By the previuos theorem, any subgroup of a finitely generated free abelian group is itself a finitely generated free abelian group.

Theorem 113 (IX.2.4) *We have $\mathbb{Z}^k \cong \mathbb{Z}^l$ if and only if $k = l$*

Corollary 114 (IX.2.5) *If $H \leq \mathbb{Z}^n$ is a subgroup then a unique integer k exists with $H \cong \mathbb{Z}^k$ (and this k satisfies $0 \leq k \leq n$)*

9.2 The structure of finitely generated abelian groups

Theorem 115 (IX.3.1 Structure theorem for finitely generated abelian groups) *For any finitely generated abelian group there exist a unique integer $r \geq 0$ and a unique (possibly empty) finite sequence $(d_1, ..., d_m)$ of integers $d_i > 1$ satisfying $d_m|d_{m-1}|...|d_1$ such that*

$$A \cong \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \ldots \mathbb{Z}/d_m\mathbb{Z}$$

Definition 116 (IX.3.2) *Given a finitely generated abelian group A, the integer r mentioned in the previous theorem is called the rank of A. The integres $d_1, ..., d_m$ are called the elementary divisors*

Theorem 117 (IX.3.4) *Given a subgroup $H \leq Z^n$ with $H \neq \{0\}$, there exists a basis $f_1, ..., f_n$ for $\mathbb{Z}^n$, an integer k with $1 \leq k \leq n$ and a sequence of integers $(d_1, ..., d_k)$ with $d_i > 0$ and $d_k|d_{k-1}|...|d_1$ such that $d_1 f_1, ..., d_k f_k$ is a basis of H.*

Definition 118 (IX.3.6) *Let A be an abelian group. The set*

$$A_{tor} = \{a \in A | ord(a) < \infty\}$$

is a subgroup of A called the torsion subgroup of A.