Fall 2024

Summary: Groups

1 Definition and first examples

Definition 1.1. A *group* is a set G with a binary operation (multiplication) $\cdot : G \times G \to G$ satisfying the axioms:

1. the group operation is associative: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
2. there exists an identity element $e \in G$ such that $a \cdot e = e \cdot a = a$ for any $a \in G$
3. for each $a \in G$ there exists the inverse element $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Definition 1.2. A group G is *finite* if the set G is finite.

Definition 1.3. A group G is *abelian* (commutative) if $a \cdot b = b \cdot a$ for all $a, b \in G$.

Definition 1.4. If G is finite as a set, then the *order of the group* G is the number of elements in G. Notation: $|G|$.

Definition 1.5. *Generators* of a group G form a subset $S \subset G$ such that any element of G can be written as a product of the elements in S.

Definition 1.6. Any equation satisfied by the generators is a *relation* in G.

Definition 1.7. A *presentation of G in terms of generators and relations* is the expression

$$\langle S \mid R_1, R_2, \dots R_k \rangle$$

where S is a set of generators of G and $R_1, R_2, \dots R_k$ are the relations satisfied by the elements in S such that any other relation follows from these.

Definition 1.8. Let g be an element in the group G. The smallest positive integer n such that $g^n = 1$, if it exists, is called the *order of the element g in G* and denoted $o(g)$. If there is no such integer, then we say that g is of infinite order (this implies that the group G is infinite).

2 Group homomorphisms. Subgroups and normal subgroups.

Definition 2.1. A map $\phi : G \to H$ between two groups is a *group homomorphism* if

$$\phi(x \cdot_G y) = \phi(x) \cdot_H \phi(y)$$

for any $x, y \in G$.

Definition 2.2. A *group isomorphism* is a homomorphism $\phi : G \to H$ that is a bijection between the sets G and H.

Definition 2.3. A *group endomorphism* is a homomorphism $\phi : G \to G$. A *group automorphism* is an isomorphism $\phi : G \to G$.

Definition 2.4. The *kernel* of a homomorphism $\phi : G \to H$ is the set of all elements $g \in G$ such that $\phi(g) = 1_H$: $\mathrm{Ker}\phi = \{g \in G \ : \phi(g) = 1\}$. The image of a homomorphism $\phi : G \to H$ is the set $\mathrm{Im}\phi = \{h \in H \mid \exists g \in G \ : \phi(g) = h\}$.

Remark 2.5. If G is presented in terms of generators and relations, to check if a given map $\phi : G \to H$ is a group homomorphism, it suffices to check that the images of the generators of G in H satisfy the relations for the generators in G.

Definition 2.6. A *subgroup* $H \subset G$ is a nonempty subset of G that forms a group with respect to the group operation in G. In particular, $1 \in H$ and for any $a, b, \in H$, we have $a \cdot b \in H$.

Definition 2.7. A subgroup $H \subset G$ is *normal* if $ghg^{-1} \in H$ for any $g \in G, h \in H$. Notation: $H \lhd G$.

Proposition 2.8. *If G is abelian, any subgroup is normal in G: $H \subset G \implies H \lhd G$.*

Proposition 2.9. *Let $\phi : G \to H$ be a group homomorphism. Then*

1. *The image of ϕ is a subgroup in H: $\phi(G) \subset H$.*
2. *The kernel of ϕ is a normal subgroup in G: $\mathrm{Ker}\phi \lhd G$.*

3 The dihedral group D_n.

Definition 3.1. The *dihedral group* D_n, $n \geq 3$ is the group of rigid symmetries of a flat regular n-gon. The group operation is composition.

Proposition 3.2. *The dihedral group D_n is a non-abelian group of order $2n$. It has the following presentation in generators and relations:*

$$D_n = \langle r, s \mid r^n = 1,\ s^2 = 1,\ srs = r^{-1} \rangle.$$

4 Cosets. Lagrange's theorem.

Definition 4.1. Let $H \subset G$ be a subgroup. A *left coset* with respect to H in G is the subset of element of G defined as follows:

$$gH = \{gh, h \in H\}.$$

Proposition 4.2. *Let H be a subgroup of G.*

1. *Two cosets xH and yH are either equal, or disjoint.*
2. *Any element $g \in G$ belongs to an H-coset.*
3. *If H is finite, $|xH| = |yH|$ for any $x, y \in G$.*

Theorem 4.3. *(Lagrange's Theorem). Let G be a finite group, and $H \subset G$ a subgroup. Then the order of H divides the order of G.*

Definition 4.4. In the conditions of Lagrange's theorem, the number $[G : H] = |G|/|H|$ is called the *index of H in G*. It equals to the number of left H-cosets in G.

Corollary 4.5. *In a finite group, the order of any element divides the order of the group.*

Corollary 4.6. *Let G be a finite group, and $g \in G$ an element. Then $g^{|G|} = 1$.*

Corollary 4.7. *Let G be a finite group of prime order, $|G| = p$. Then G is cyclic (= there exists $x \in G$ such that $G = \{1, x, x^2, \ldots x^{p-1}\}$.)*

5 Applications of Lagrange's theorem in arithmetic.

Definition 5.1. The *group of units* in $\mathbb{Z}/n\mathbb{Z}$ is the group of all invertible elements in $\mathbb{Z}/n\mathbb{Z}$ with respect to multiplication. It is denoted $((\mathbb{Z}/n\mathbb{Z})^*, \cdot)$.

Proposition 5.2. *Let $[a]_n \in \mathbb{Z}/n\mathbb{Z}$, $[a]_n \neq [0]_n$. Then $[a]_n$ is a unit in $\mathbb{Z}/n\mathbb{Z}$ if and only if $\gcd(a, n) = 1$. In particular, $|((\mathbb{Z}/n\mathbb{Z})^*, \cdot)| = \varphi(n)$, where $\varphi(n)$ is the Euler's totient function of n.*

Theorem 5.3. *(Fermat's Little Theorem (FLT)). Let p be a prime, and $a \in \mathbb{Z}$ such that p does not divide a. Then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Theorem 5.4. *(Euler's Theorem). Let $a, n \in \mathbb{Z}^+$, such that $\gcd(a, n) = 1$. Then*

$$a^{\varphi(n)} \equiv 1 \pmod{n},$$

where $\varphi(n)$ is Euler's totient function of n.

Remark 5.5. For a prime p, the group $((\mathbb{Z}/p\mathbb{Z})^*, \cdot)$ is cyclic of order $p - 1$.

6 Quotient group.

Proposition 6.1. *Let G be a group, and $N \lhd G$ a normal subgroup. The set of left N-cosets in G is a group under the operation*

$$(xN)(yN) = (xyN).$$

Definition 6.2. Let $N \lhd G$. Then the group of left N-cosets in G is called the *quotient group* and denoted G/N.

Proposition 6.3. *Let $\phi : G \to H$ be a group homomorphism. Then $G/\mathrm{Ker}\phi \simeq \mathrm{Im}\phi$.*

7 The symmetric group S_n

Definition 7.1. Let G be a finite group and E a finite set. We say that *G acts on E* (by permutations) if for all $x \in E$ and $g \in G$ the element $g \cdot x \in E$ is defined, such that

1. $1 \cdot x = x \quad \forall x \in E$,
2. $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x) \quad \forall g_1, g_2 \in G, \quad \forall x \in E$.

Definition 7.2. Let G act on the set E. The *orbit* of $x \in E$ is the set

$$\mathrm{Orb}_x = \{g \cdot x,\ g \in G\}.$$

The orbits of size 1 are called the *fixed points* of the action.

Definition 7.3. The *symmetric group* of order n is the group of all permutations (bijective maps) of $n \geq 1$ ordered elements:

$$\rho : \{1, 2, \dots n\} \to \{1, 2, \dots n\},$$

where $\rho(i) = k \in \{1, 2, \dots n\}$ and $i \neq j \implies \rho(i) \neq \rho(j)$. The product in S_n is the composition of permutations. The neutral element is the trivial permutation. The inverse element for such that $\rho(i) = k$ is $\rho^{-1}(k) = i$ for all $i, k \in \{1, \dots n\}$. The group is denoted S_n. We have $|S_n| = n!$, the number of all permutations of n elements.

Definition 7.4. Let $\sigma \in S_n$ be a permutation and consider the subgroup $\langle\sigma\rangle \subset S_n$ generated by σ. If the action of $\langle\sigma\rangle$ by permutations of the set of n elements contains exactly one nontrivial orbit with $k > 1$ elements (and possibly some fixed points), then $\sigma \in S_n$ is called a *k-cycle*.

Definition 7.5. A 2-cycle is called a *transposition*.

Notation 7.6. Let $\pi \in S_n$ be a k-cycle, and $x \in \{1, 2, \dots n\}$ a number in the nontrivial orbit of π. Then in the *cycle notation* we represent π as follows: $\pi = (x, \pi(x), \pi^2(x), \dots \pi^{k-1}(x))$.

Definition 7.7. Two cycles $\pi_1, \pi_2 \in S_n$ are *disjoint* if their nontrivial orbits do not intersect.

Proposition 7.8. *Disjoint cycles commute in S_n.*

Theorem 7.9. *Any permutation in S_n is a product of disjoint cycles, uniquely up to the order of the factors.*

Proposition 7.10. *Let $\pi, \rho \in S_n$. The cycle decomposition of $\pi\rho\pi^{-1}$ is obtained from that of ρ by replacing each integer i in the disjoint cycle decomposition of ρ by the integer $\pi(i)$.*

Proposition 7.11. *Every k-cycle in S_n is a product of $(k-1)$ transpositions. In particular,*

$$(12 \dots k) = (1k)(1\ \ k-1) \dots (13)(12).$$

Caution: The decomposition of a permutation as a product of *disjoint cycles* is unique. The transpositions in the Proposition above are *not* disjoint.

Corollary 7.12. *The group S_n is generated by the transpositions $\{(ij)\}_{1 \leq i < j \leq n}$*

Proposition 7.13. *No permutation in S_n can be written both as a product of an odd number of transpositions and as a product of an even number of transpositions.*

Definition 7.14. A permutation is *odd* if it is a product of an odd number of transpositions, and *even* if it is a product of an even number of transpositions. A transposition is an odd permutation.

Proposition 7.15. *The set A_n of all even permutations form a normal subgroup in S_n of index 2: $[S_n : A_n] = 2$.*

8 The orbit-stabilizer theorem.

Let G be a finite group acting on a finite set E. Then the orbit of $x \in E$ is the set $\mathrm{Orb}_x = \{g \cdot x \in G\}$ (see Definitions 7.1 7.2).

Definition 8.1. Let G act on the set E. The *stabilizer* of $x \in E$ is

$$\mathrm{Stab}_x = \{g \in G \,|g \cdot x = x\}.$$

Proposition 8.2. *Let G act on the set E. The stabilizer Stab_x of an element $x \in E$ is a subgroup in G.*

Proposition 8.3. *Let G act on the set E. Two orbits of the G-action Orb_x and Orb_y either coincide, or do not intersect. In particular, E splits as a disjoint union of orbits of G-action: $E = \cup_i \mathrm{Orb}_{x_i}$.*

Theorem 8.4. *(The Ortbit-Stabilizer theorem). Let a finite group G act on a finite set E. Then for any element $x \in E$, the number of elements in the orbit of x under the G-action equals to the index of the stabilizer subgroup of x in G:*

$$|\mathrm{Orb}_x| = [G : \mathrm{Stab}_x].$$

9 Conjugacy classes and the class equation

Definition 9.1. Let G be a group acting on itself by conjugations: $g \cdot x = gxg^{-1}\ \forall x \in G, g \in G$. Then an orbit of $x \in G$ is called the *conjugacy class* of x in G and denoted C_x, and the stabilizer of x with respect to this action is called the *centralizer* of $x \in G$ and denoted $G_x \subset G$.

Proposition 9.2. *The elements $g_1 \in S_n$ and $g_2 \in S_n$ belong to the same conjugacy class in S_n if and only if they decompose as a product of disjoint cycles of the same lengths. The set of lengths of cycles in a disjoint cycle decomposition of an element $g \in S_n$ is called the cycle type of g. Conjugacy classes in S_n are in bijection with cycles types.*

Definition 9.3. The *center* $Z(G)$ of the group G is the set of elements that commute with any element in G:

$$Z(G) = \{x \in G \mid xg = gx\ \forall g \in G\}.$$

Theorem 9.4. *(The class equation). Let G be a finite group, and let $Z(G)$ be its center, and $\{x_i\}_{i=1}^m$ a set of representatives the conjugacy classes $\{C_{x_i}\}_{i=1}^m$ containing more than one element each. Let G_{x_i} be the stabilizer subgroup for x_i. Then*

$$|G| = |Z(G)| + \sum_{i=1}^{m} |C_{x_i}| = |Z(G)| + \sum_{i=1}^{m} [G : G_{x_i}].$$

10 Direct product of groups

Definition 10.1. Let G, H be groups. The *direct product* $G \times H$ is the group whose elements are pairs $G \times H = \{(g,h) \mid g \in G, h \in H\}$ with the multiplication $(g_1,h_1)\cdot(g_2,h_2) = (g_1g_2, h_1h_2)$ for any $g_1, g_2 \in G, H_1, h_2 \in H$.

It is easy to check that $(1_G, 1_H) \in G \times H$ is the identity element, and $(g,h)^{-1} = (g^{-1}, h^{-1})$.

Proposition 10.2. *Properties of the direct product:*

(a) $G \times H \simeq H \times G$

(b) $G \times H$ *is abelian if an only if* G *and* H *are both abelian*

(c) $\{(1,h\}_{h\in H} \subset G \times H$ *is a subgroup isomorphic to* H*, and* $\{(g,1\}_{g\in G} \subset G \times H$ *is a subgroup isomorphic to* G

(d) For the cyclic groups, $C_n \times C_m \simeq C_{mn}$ *if and only If* $\gcd(n,m) = 1$

(e) Suppose that $H, K \subset G$ *are two subgroups such that (a)* $H \cap K = \{1\}$*, (b)* $\forall h \in H, k \in K$, $hk = kh$*, (c)* G *is spanned by the products* $\{hk\}_{h\in H, k\in K}$*. Then* $G \simeq H \times K$.

11 Classification of finite abelian groups.

Definition 11.1. A group G is *simple* if it has no nontrivial ($\neq \{1\}$) proper ($\neq G$) normal subgroups.

Theorem 11.2. *(Cauchy). If G is a finite abelian group and a prime p divides the order of G, then G contains an element of order p.*

Corollary 11.3. *If G is a finite abelian simple group, then G is isomorphic to a cyclic group of prime order.*

To classify all finite abelian groups we will use direct products to build more complicated groups out of smaller groups.

Definition 11.4. Let n be a positive integer. A *partition* of n is a set of positive integers $i_1 \geq i_2 \geq \ldots \geq i_k \geq 1$ such that $i_1 + i_2 + \ldots + i_k = n$.

Proposition 11.5. *Let G be an abelian group of prime power order, $|G| = p^n$. Then G is isomorphic to a direct product of cyclic groups $G = C_{p^{i_1}} \times C_{p^{i_2}} \times \ldots \times C_{p^{i_k}}$, where $(i_1 \geq i_2 \geq \ldots i_k)$ is a partition of n. Different partitions of n correspond to non-isomorphic abelian groups.*

Proposition 11.6. *Let G be a finite abelian group, and $|G| = p_1^{n_1} \ldots p_r^{n_r}$ is the prime factorization of $|G|$ (here p_i are all distinct primes). Then G is isomorphic to a direct product of abelian groups of orders $p_1^{n_1}, p_2^{n_2}, \ldots p_r^{n_r}$:*

$$G \simeq G_{p_1^{n_1}} \times G_{p_2^{n_2}} \times \ldots G_{p_r^{n_r}}.$$

Theorem 11.7. *(Classification of finite abelian groups). Let G be a finite abelian group. Then G is isomorphic to a direct product of cyclic groups with prime power orders:*

$$G \simeq C_{p_1^{a_1}} \times C_{p_2^{a_2}} \times \ldots C_{p_m^{a_m}},$$

where $\{p_1, \ldots p_m\}$ are primes, not necessarily distinct, and $|G| = p_1^{a_1} p_2^{a_2} \ldots p_m^{a_m}$.

Definition 11.8. The numbers $(p_1^{a_1}, p_2^{a_2}, \ldots, p_m^{a_m})$ are called the *elementary divisors* of G.

Theorem 11.9. *Let G be a finite abelian group. Then G is isomorphic to a direct product of cyclic groups with consecutively dividing orders:*

$$G \simeq C_{d_1} \times C_{d_2} \times \ldots C_{d_k},$$

where $d_k | d_{k-1}$, $d_{k-1} | d_{k-2}$ and so on, $d_2 | d_1$, and $|G| = d_1 d_2 \ldots d_k$.

Definition 11.10. The numbers $(d_k, d_{k-1}, \ldots d_2, d_1)$ are called the *invariant factors* of G.

Example 11.11. Let G be an abelian group, $|G| = 360 = 2^3 \cdot 3^2 \cdot 5$. The partitions of the power of 2 are $(3), (2, 1), (1, 1, 1)$. The partitions of the power of 3 are $(2), (1, 1)$. According to Theorem 11.7, we have the following list of unisomorphic abelian groups of order 360:

$$C_8 \times C_9 \times C_5, \quad C_8 \times C_3 \times C_3 \times C_5, \quad C_4 \times C_2 \times C_9 \times C_5, \quad C_4 \times C_2 \times C_3 \times C_3 \times C_5,$$

$$C_2 \times C_2 \times C_2 \times C_9 \times C_5, \quad C_2 \times C_2 \times C_2 \times C_3 \times C_3 \times C_5.$$

The elementary divisors are $(8, 9, 5), (8, 3, 3, 5), (4, 2, 9, 5), (4, 2, 3, 3, 5), (2, 2, 2, 9, 5), (2, 2, 2, 3, 3, 5)$. Let us collect the powers of distinct primes to rewrite the same list of groups according to Theorem 11.9:

$$C_{360}, \quad C_{120} \times C_3, \quad C_{180} \times C_2, \quad C_{60} \times C_6, \quad C_{90} \times C_2 \times C_2, \quad C_{30} \times C_6 \times C_2.$$

The invariant factors of G are $(360), (120, 3), (180, 2), (60, 6), (90, 2, 2), (30, 6, 2)$.