Course 6

1.9 Isomorphism theorems for groups

Theorem 1.9.1 (The First Isomorphism Theorem) *Let $f : G \to G'$ be a group homomorphism. Then:*
(i) $\mathrm{Ker} f \trianglelefteq G$;
(ii) $G/\mathrm{Ker} f \simeq \mathrm{Im} f$.

Proof. Let us denote $K = \mathrm{Ker} f$.

(i) We have already seen that $K = \mathrm{Ker} f \leq G$. Now let $x \in G$ and $n \in K$. Then $f(n) = 1'$, so that

$$f(x^{-1} \cdot n \cdot x) = f(x^{-1}) \cdot f(n) \cdot f(x) = (f(x))^{-1} \cdot 1' \cdot f(x) = 1' .$$

Hence $x^{-1} \cdot n \cdot x \in K$. It follows that $K \trianglelefteq G$.

(ii) Define
$$\overline{f} : G/K \to \mathrm{Im} f \text{ by } \overline{f}(xK) = f(x) ,\ \forall x \in G .$$

Let us prove first that $\overline{f}$ is well-defined, that is, it does not depend on the choice of representatives. Indeed, we have

$$xK = yK \Longrightarrow x^{-1} \cdot y \in K \Longrightarrow f(x^{-1} \cdot y) = 1' \Longrightarrow$$
$$\Longrightarrow f(x^{-1}) \cdot f(y) = 1' \Longrightarrow (f(x))^{-1} \cdot f(y) = 1' \Longrightarrow f(x) = f(y) .$$

By the definition of the operation on the quotient group G/K we have

$$\overline{f}((xK)(yK)) = \overline{f}((xy)K) = f(x \cdot y) = f(x) \cdot f(y) = \overline{f}(xK)\overline{f}(yK) ,$$

for every $x, y \in G$, hence $\overline{f}$ is a group homomorphism.

Now let $x, y \in G$ be such that $\overline{f}(xK) = \overline{f}(yK)$. Then $f(x) = f(y)$, whence $(f(x))^{-1} \cdot f(y) = 1'$. It follows that $f(x^{-1} \cdot y) = 1'$, that is, $x^{-1} \cdot y \in K$. Then $xK = yK$. Therefore, $\overline{f}$ is injective.

Clearly, $\overline{f}$ is surjective and consequently, $\overline{f}$ is a group isomorphism. □

Example 1.9.2 (a) Let $n \in \mathbb{N}$ and $f : \mathbb{Z} \to \mathbb{Z}_n$ be defined by $f(x) = \widehat{x}$. Then f is a group homomorphism between $(\mathbb{Z}, +)$ and $(\mathbb{Z}_n, +)$, $\mathrm{Ker} f = \{x \in \mathbb{Z} \mid \hat{x} = \hat{0}\} = n\mathbb{Z}$ and $\mathrm{Im} f = \mathbb{Z}_n$. By the First Isomorphism Theorem we have $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$.

(b) The groups $(\mathbb{Q}^*/\{-1, 1\}, \cdot)$ and $(\mathbb{Q}^*_+, \cdot)$ are isomorphic.

We are looking for a group homomorphism $f : \mathbb{Q}^* \to \mathbb{Q}^*_+$ which allows us to get the required isomorphism directly form the First Isomorphism Theorem.

We may try $g : \mathbb{Q}^* \to \mathbb{Q}^*_+$ defined by $g(x) = x^2$, $\forall x \in \mathbb{Q}^*$. Then g is a group homomorphism, $\mathrm{Ker} g = \{x \in \mathbb{Q}^* \mid g(x) = 1\} = \{-1, 1\}$, but $\mathrm{Im} f \neq \mathbb{Q}^*_+$.

Let us now consider $f : \mathbb{Q}^* \to \mathbb{Q}^*_+$ defined by $f(x) = |x|$, $\forall x \in \mathbb{Q}^*$. Then it is easy to see that f is a group homomorphism and $\mathrm{Im} f = \mathbb{Q}^*_+$. Moreover, $\mathrm{Ker} f = \{x \in \mathbb{Q}^* \mid f(x) = 1\} = \{-1, 1\}$. Hence by Theorem 1.9.1, there exists a group isomorphism $\overline{f} : \mathbb{Q}^*/\{-1, 1\} \to \mathbb{Q}^*_+$, that is defined by $\overline{f}(x\{-1, 1\}) = f(x) = |x|$, $\forall x \in \mathbb{Q}^*$.

Theorem 1.9.3 (The Second Isomorphism Theorem) *Let $(G, \cdot)$ be a group and let $H, N \leq G$. If $N \trianglelefteq < H \cup N >$, then:*
(i) $< H \cup N >= H \cdot N = N \cdot H$;
(ii) $H \cap N \trianglelefteq H$;
(iii) $H/(H \cap N) \simeq (H \cdot N)/N$.

Proof. (i) We show that $H \cdot N$ is the smallest subgroup of G containing $H \cup N$. This will imply that $H \cdot N =< H \cup N >$.

Obviously, $H \cdot N \neq \emptyset$, since $1 \in H \cdot N$. Let $x, y \in H \cdot N$. Then $x = h_1 \cdot n_1$ and $y = h_2 \cdot n_2$ for some $h_1, h_2 \in H$ and $n_1, n_2 \in N$. Since $N \trianglelefteq < H \cup N >$, it follows that

$$x \cdot y^{-1} = h_1 \cdot n_1 \cdot (h_2 \cdot n_2)^{-1} = h_1 \cdot n_1 \cdot n_2^{-1} \cdot h_2^{-1} \in H \cdot N .$$

Hence $H \cdot N \leq G$.

Clearly, $H \subseteq H \cdot N$ and $N \subseteq H \cdot N$. Now since $H \cdot N \leq G$ and $H \cup N \subseteq H \cdot N \subseteq < H \cup N >$, it follows that $H \cdot N =< H \cup N >$. Similarly, $N \cdot H =< H \cup N >$.

(ii) and (iii) Let $i : H \to H \cdot N$ be the inclusion group homomorphism and let $p : H \cdot N \to (H \cdot N)/N$ be the natural projection defined by $p(x) = xN$, $\forall x \in H \cdot N$, which is again a group homomorphism. Now consider the group homomorphism $f = p \circ i : H \to (H \cdot N)/N$, that is defined by $f(h) = hN$, $\forall h \in H$. Then f is clearly surjective, hence $\mathrm{Im} f = (H \cdot N)/N$. We have

$$\mathrm{Ker} f = \{h \in H \mid f(h) = N\} = \{h \in H \mid hN = N\} = \{h \in H \mid h \in N\} = H \cap N\,.$$

By Theorem 1.9.1, it follows that $H \cap N \trianglelefteq H$ and $\overline{f} : H/(H \cap N) \to (H \cdot N)/N$ defined by

$$\overline{f}(h(H \cap N)) = f(h) = hN\,,\ \forall h \in H\,,$$

is a group isomorphism. □

Theorem 1.9.4 (The Third Isomorphism Theorem) *Let $(G, \cdot)$ be a group and let $N, N' \trianglelefteq G$ be such that $N \subseteq N'$. Then:*

(i) $N'/N \trianglelefteq G/N$;

(ii) $(G/N)/(N'/N) \simeq G/N'$.

Proof. (i) and (ii) Let $f : G/N \to G/N'$ be defined by $f(xN) = xN'$. Let us prove that f is well-defined, that is, it does not depend on the choice of representatives. Indeed, we have

$$xN = yN \Longrightarrow x \in yN \text{ and } y \in xN \Longrightarrow xN' \subseteq yNN' \subseteq yN' \text{ and } yN' \subseteq xNN' \subseteq xN' \Longrightarrow xN' = yN'.$$

By the definition of the operations on the quotient groups G/N and G/N' we have

$$f((xN)(yN)) = f((x \cdot y)N) = (x \cdot y)N' = (xN')(yN') = f(xN)f(yN)\,,$$

for every $x, y \in G$, hence f is a group homomorphism.

The function f is clearly surjective, hence $\mathrm{Im} f = G/N'$. We have

$$\mathrm{Ker} f = \{xN \in G/N \mid f(xN) = N'\} = \{xN \in G/N \mid xN' = N'\} = \{xN \in G/N \mid x \in N'\} = N'/N\,.$$

By Theorem 1.9.1, it follows that $N'/N \trianglelefteq G/N$ and $\overline{f} : (G/N)/(N'/N) \to G/N'$ defined by

$$\overline{f}(xN(N'/N)) = f(xN) = xN'\,,\ \forall x \in G\,,$$

is a group isomorphism. □

Example 1.9.5 Consider the abelian group $(\mathbb{Z}, +)$. Let $m, n \in \mathbb{N}$ be such that $m|n$. Then we have $N = n\mathbb{Z} \subseteq m\mathbb{Z} = N'$. By the third isomorphism theorem we have $(\mathbb{Z}/n\mathbb{Z})/(m\mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}_m$. Hence the factor groups of $\mathbb{Z}_n \simeq \mathbb{Z}/n\mathbb{Z}$ are isomorphic to $\mathbb{Z}_m$ for $m \in \mathbb{N}$ with $m|n$.

1.10 Permutation groups

Recall that if M is a set, then $S_M = \{f : M \to M \mid f \text{ is bijective}\}$ is a group with respect to the composition of functions, called the *symmetric group* of M. If $|M| = n$, then S_M is identified with the permutation group of n elements and is denoted by S_n.

A very important result is the following theorem, that tells us that it is enough to study symmetric (permutation) groups in order to know the structure of any other group.

Theorem 1.10.1 (Cayley) *Every group is isomorphic to a subgroup of a symmetric group.*

Proof. Let $(G, \cdot)$ be a group and consider the symmetric group S_G. For every $a \in G$, define

$$t_a : G \to G \text{ by } t_a(x) = a \cdot x\,, \quad \forall x \in G\,.$$

Let us prove that $t_a \in S_G$, that is, t_a is bijective. If $x_1, x_2 \in G$ such that $t_a(x_1) = t_a(x_2)$, then $a \cdot x_1 = a \cdot x_2$, whence $x_1 = x_2$. Thus, t_a is injective. Furthermore, $\forall y \in G$, $\exists x = a^{-1} \cdot y \in G$ such that $t_a(x) = a \cdot x = y$. Thus, t_a is surjective, so that t_a is bijective.

We may now define

$$f : G \to S_G \text{ by } f(a) = t_a\,,\ \forall a \in G\,.$$

Let us show that f is an injective group homomorphism.

Let $a, b \in G$. We prove that $f(a \cdot b) = f(a) \circ f(b)$, or equivalently $t_{ab} = t_a \circ t_b$. But this holds since $\forall x \in G$,

$$t_{a \cdot b}(x) = (a \cdot b) \cdot x = a \cdot (b \cdot x) = t_a(b \cdot x) = t_a(t_b(x)) = (t_a \circ t_b)(x)\,.$$

Therefore, f is a group homomorphism.

If $a, b \in G$ such that $f(a) = f(b)$, then $t_a = t_b$. It follows that $t_a(1) = t_b(1)$, that is, $a = b$. Hence f is injective. Then $\mathrm{Ker}\, f = \{1\}$.

By the First Isomorphism Theorem, it follows that $G/\{1\} \simeq G/\mathrm{Ker}\, f \simeq \mathrm{Im} f$. But

$$G/\{1\} = \{x \cdot \{1\} \mid x \in G\} = \{\{x\} \mid x \in G\} \simeq G.$$

Hence we have $G \simeq \mathrm{Im} f$. But $\mathrm{Im} f \leq S_G$, so that we are done. $\square$

Remark 1.10.2 If $\sigma \in S_n$ and $\sigma(1) = i_1, \ldots, \sigma(n) = i_n$, then we denote $\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}$. The composition of $\sigma_1 \circ \sigma_2 \in S_n$ is also denoted by $\sigma_1\sigma_2$ and is called the *product* of σ_1 and σ_2. For $\sigma \in S_n$ and $k \in \mathbb{N}$, we denote $\sigma^k = \underbrace{\sigma \circ \cdots \circ \sigma}_{k \text{ times}}$.

Definition 1.10.3 A permutation $\sigma \in S_n$ is called *cycle* (or *circular permutation*) of length k if there exist k distinct numbers $i_1, \ldots, i_k \in \{1, \ldots, n\}$ such that $\sigma(i_1) = i_2, \ldots, \sigma(i_{k-1}) = i_k, \sigma(i_k) = i_1$ and $\sigma(i) = i$ for every $i \in \{1, \ldots, n\} \setminus \{i_1, \ldots, i_k\}$. In this case we denote $\sigma = (i_1 i_2 \ldots i_k)$. A cycle of length 2 is called *transposition.*

For $\sigma \in S_n$ and $x \in \{1, \ldots, n\}$ we call the *orbit* of x under σ the set $\mathcal{O}_x = \{\sigma^k(x) \mid k \in \mathbb{N}\}$.

Two permutations $\sigma_1, \sigma_2 \in S_n$ are called *disjoint* if for every $i \in \{1, \ldots, n\}$ we have at least one of the equalities $\sigma_1(i) = i$ and $\sigma_2(i) = i$.

Remark 1.10.4 (1) We have $(i_1\ i_2\ \ldots\ i_k) = (i_2\ i_3\ \ldots\ i_k\ i_1) = \cdots = (i_k\ i_1\ \ldots\ i_{k-1})$.

(2) If $\sigma \in S_n$ is a cycle of length k, then $\mathrm{ord}\,\sigma = k$. In particular, every transposition has order 2.

Example 1.10.5 (a) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix} = (1\ 3\ 4)$ is a cycle of length 3.

We have $\mathcal{O}_1 = \mathcal{O}_3 = \mathcal{O}_4 = \{1, 3, 4\}$, $\mathcal{O}_2 = \{2\}$ and $\mathcal{O}_5 = \{5\}$.

(b) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{pmatrix}$ is not a cycle.

We have $\mathcal{O}_1 = \mathcal{O}_4 = \{1, 3\}$, $\mathcal{O}_2 = \mathcal{O}_4 = \{2, 4\}$ and $\mathcal{O}_5 = \{5\}$. We may write $\sigma = (1\ 3)(2\ 4)$. The cycles corresponding to the orbits are disjoint.

(c) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 4 & 5 \end{pmatrix} = (2\ 3)$ is a transposition.

Theorem 1.10.6 *Let $\sigma_1, \sigma_2 \in S_n$ be disjoint. Then $\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1$.*

Proof. Since σ_1, σ_2 are disjoint, for every $i \in \{1, \ldots, n\}$ we have 3 cases:

Case I. $\sigma_1(i) = \sigma_2(i) = i$. Then $(\sigma_1 \circ \sigma_2)(i) = (\sigma_2 \circ \sigma_1)(i)$.

Case II. $\sigma_1(i) = i$ and $\sigma_2(i) \neq i$. Since σ_2 is injective, it follows that $\sigma_2(\sigma_2(i)) \neq \sigma_2(i)$. Since σ_1, σ_2 are disjoint, we must have $\sigma_1(\sigma_2(i)) = \sigma_2(i)$. Then $(\sigma_1 \circ \sigma_2)(i) = \sigma_2(i) = (\sigma_2 \circ \sigma_1)(i)$.

Case III. $\sigma_1(i) \neq i$ and $\sigma_2(i) = i$. This is similar to Case II. $\square$

Theorem 1.10.7 *Every permutation $e \neq \sigma \in S_n$ may be written as a product of disjoint cycles of length at least 2, uniquely up to the order of the factors.*

Proof. Let $e \neq \sigma \in S_n$. Let $\sigma_1, \dots, \sigma_k$ be the cycles obtained from the orbits of σ. We claim that $\sigma = \sigma_1 \dots \sigma_k$. Let $x_1 \in \{1, \dots, n\}$ and $\sigma(x_1) = x_2$. If σ_i is the cycle containing x_1, we may write $\sigma = (x_1\ x_2\ \dots\ x_r)$. All the other cycles except for σ_i do not contain $x_1, x_2, \dots, x_r$, hence these elements remain fixed by the other cycles. Hence $(\sigma_1 \dots \sigma_k)(x_1) = x_2 = \sigma(x_1)$. It follows that $\sigma = \sigma_1 \dots \sigma_k$. □

Corollary 1.10.8 *Every cycle $(i_1\ i_2\ \dots\ i_k)$ of length k can be written as a product of transpositions, namely $(i_1\ i_k)(i_1\ i_{k-1}) \dots (i_1\ i_2)$. Hence every permutation $e \neq \sigma \in S_n$ may be written as a product of transpositions.*

Example 1.10.9 We have $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix} = (1\ 2\ 5)(3\ 4)$ and $\sigma = (1\ 5)(1\ 2)(3\ 4) = (1\ 3)(3\ 4)(4\ 5)(2\ 4)(1\ 4)$, hence the decomposition of a permutation as a product of transpositions is not unique in general.

Definition 1.10.10 Let $\sigma \in S_n$ and $i, j \in \{1, \dots, n\}$ with $i \neq j$. We say that (i, j) is an *inversion* of σ if $i < j$ and $\sigma(i) > \sigma(j)$. We denote by $\operatorname{inv}(\sigma)$ the number of inversions of σ, and define $\varepsilon : S_n \to \{-1, 1\}$ by $\varepsilon(\sigma) = (-1)^{\operatorname{inv}(\sigma)}$. The number $\varepsilon(\sigma)$ is called the *signature* of σ. The permutation σ is called *even* (respectively *odd*) if $\varepsilon(\sigma) = 1$ (respectively $\varepsilon(\sigma) = -1$).

We denote by A_n the subset of S_n consisting of the even permutations.

Remark 1.10.11 (1) Every transposition is an odd permutation. Indeed, let

$$(i\ j) = \begin{pmatrix} 1 & \dots & i-1 & i & i+1 & \dots & j-1 & j & j+1 & \dots n \\ 1 & \dots & i-1 & j & i+1 & \dots & j-1 & i & j+1 & \dots n \end{pmatrix}.$$

Then $\operatorname{inv}(i\ j) = (j - i) + (j - i - 1) = 2(j - i) - 1$, hence $\varepsilon(i\ j) = -1$.

(2) A pair (i, j) is an inversion of σ if and only if $\frac{\sigma(j)-\sigma(i)}{j-i} < 0$. Then $\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j)-\sigma(i)}{j-i}$.

Theorem 1.10.12 *For $n \geq 2$, ε is a surjective group homomorphism between the groups $(S_n, \circ)$ and $(U_2 = \{-1, 1\}, \cdot)$. Moreover, $A_n \trianglelefteq S_n$ and $S_n/A_n \simeq U_2$.*

Proof. If $\sigma_1, \sigma_2 \in S_n$, then for every $i', j' \in \{1, \dots, n\}$, there exist unique $i, j \in \{1, \dots, n\}$ such that $i' = \sigma_2(i)$ and $j' = \sigma_2(j)$, because σ_2 is bijective. For every $\sigma_1, \sigma_2 \in S_n$ we have:

$$\begin{aligned} \varepsilon(\sigma_1 \circ \sigma_2) &= \prod_{1 \leq i < j \leq n} \frac{\sigma_1(\sigma_2(j)) - \sigma_1(\sigma_2(i))}{j - i} \\ &= \prod_{1 \leq i < j \leq n} \frac{\sigma_1(\sigma_2(j)) - \sigma_1(\sigma_2(i))}{\sigma_2(j) - \sigma_2(i)} \cdot \prod_{1 \leq i < j \leq n} \frac{\sigma_2(j) - \sigma_2(i)}{j - i} \\ &= \prod_{1 \leq i' < j' \leq n} \frac{\sigma_1(j') - \sigma_1(i')}{j' - i'} \cdot \prod_{1 \leq i < j \leq n} \frac{\sigma_2(j) - \sigma_2(i)}{j - i} = \varepsilon(\sigma_1) \cdot \varepsilon(\sigma_2), \end{aligned}$$

hence ε is a group homomorphism. Also, ε is surjective, because there exist even (the identical permutation) and odd permutations (any transposition). Hence $\operatorname{Im} \varepsilon = U_2$.

Since $\operatorname{Ker} \varepsilon = \{\sigma \in S_n \mid \varepsilon(\sigma) = 1\} = A_n$, the First Isomorphism Theorem implies that $A_n \trianglelefteq S_n$ and $S_n/A_n \simeq U_2$. □

Remark 1.10.13 (1) The group $(A_n, \circ)$ is called the *alternating group* of degree n. Since $|S_n : A_n| = |S_n/A_n| = |U_2| = 2$, we have $|A_n| = |S_n|/2 = n!/2$.

(2) If $\sigma \in S_n$ is even (respectively odd), then the number of transpositions in any decomposition of σ in product of transpositions is even (respectively odd).