In this lecture, we meet two concepts that help us study groups and their properties. The objective is not only to learn this concepts, but mainly to use them to study the principal objects of group theory.

1. Homomorphisms and isomorphisms

When studying an algebraic structure, we are not only interested in the objects that possess this structure, but also in the morphisms between objects of the same type that preserve such structure. This is true through out all branches of mathematics.

In the case of group theory, the objects are groups and the structure preserving maps are called group-homomorphisms.

Let $(G, \cdot)$ and $(H, *)$ be groups.

Definition 1.1. A group-homomorphism from G to H is a map $\varphi\colon G \to H$ such that

$$\varphi(a \cdot b) = \varphi(a) * \varphi(b)$$

for all $a, b \in G$.

Remark 1.1.1. From now and on, we omit the adjective "group" in "group-homomorphism", since we will be working only on the realm of group theory (**Grp**).

Note that φ transforms a product $a \cdot b$ (using the operation of G) into the product $\varphi(a) * \varphi(b)$ (using the operation of H). This is why we say φ preserves the structure: it takes a product in G and maps it to a product in H. In this case (of groups) there are no more structure to be preserved.

However, the definition above just guarantees that the structure is preserved in one direction only: from G to H. If, in addition, it is possible to preserve the structure the other way around, we obtain a more interesting type of map: an *isomorphism*.

Definition 1.2. An **isomorphism** is a bijective homomorphism.

Thus, an isomorphism $\varphi\colon G \to H$ is just a homomorphism that has inverse $\varphi^{-1}\colon H \to G$. In this case, G and H are said to be of the same isomorphism type, or *isomorphic* for short. We write $G \cong H$. You may ask *isn't it necessary that the inverse be a homomorphism also (so that the structure is preserved the other way around)?* And it turns out that *no*, because it follows straight from the definition. (Why?)

Exercise 1. Prove φ^{-1} is a homomorphism if φ is an isomorphism.

Exercise 2. Prove $\cong$ is an equivalence relation (over which set?)

Lemma 1.3. *If $\varphi\colon G \to H$ is an isomorphism, then*

(i) $|G| = |H|$

(ii) *G is Abelian if and only if H is Abelian*

(iii) *φ preserves the order of elements, that is, $|x| = |\varphi(x)|$.*

Example 1. (i) Let us prove $(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$. Define $\psi\colon \mathbb{R} \to \mathbb{R}^+ : x \mapsto \exp(x)$. Notice

$$\psi(x+y) = \exp(x+y) = \exp(x)\cdot\exp(y) = \psi(x)\cdot\psi(y).$$

Since ψ is injective and surjective (facts known from elementary calculus), ψ is an isomorphism. (Are there any other maps that show $(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$?)

(ii) If X and Y have the same cardinality, then $S_X \cong S_Y$. Indeed, if $\omega\colon X \to Y$ is a bijection (recall the definition of cardinality), and given any $\alpha \in S_X$, the map $\omega \circ \alpha \circ \omega^{-1}\colon Y \to Y$ is also a bijection. Thus, define $\varphi\colon S_X \to S_Y$ by $\varphi(\alpha) = \omega \circ \alpha \circ \omega^{-1}$ for every $\alpha \in S_X$. Diagramatically, we have

$$X \xhookrightarrow{\alpha} X \xhookrightarrow{\omega} Y \xhookrightarrow{\omega\circ\alpha\circ\omega^{-1}} Y\ .$$

Since

$$\varphi(\alpha\circ\beta) = \omega\circ(\alpha\circ\beta)\circ\omega^{-1} = (\omega\circ\alpha\circ\omega^{-1})\circ(\omega\circ\beta\circ\omega^{-1}) = \varphi(\alpha)\circ\varphi(\beta),$$

φ is a homomorphism. The reader must easily verify that φ is an isomorphism.

(iii) The groups S_3 and $\mathbb{Z}/6\mathbb{Z}$ are not isomorphic as one is Abelian and the other is not. This follows from Theorem 1.3.

(iv) $(\mathbb{R}\setminus\{0\}, \cdot)$ and $(\mathbb{R}, +)$ are not isomorphic. The former has an element of order 2 and the latter does not have any element of order 2.

Exercise 3. (i) Provide an example of a group with only one element.

(ii) Prove S_3 is the unique nonabelian group of order 6 up to isomorphism.

(iii) Prove $A \times B \cong B \times A$ if A and B are any groups.

2. Subgroups

We now come to study of groups that live inside larger groups.

Let $(G, \cdot)$ be a group.

Definition 2.1. A group $(H, \cdot_H)$ is a **subgroup** of $(G, \cdot_G)$ if $H \subseteq G$ and $\cdot_H = \cdot_G$.

In other words, a subgroup of G is a subset of G that it together with the operation of G is itself a group.

If H is a subgroup of G we write $H \leq G$. As an exercise, prove $\leq$ is a partial order.

Example 2. (i) Under addition, $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R}$.

(ii) There are always two noninteresting subgroups of any group G, namely $\{1_G\}$ and G itself. We call the former the *trivial subgroup* of G.

(iii) If $G = D_{2n}$ is the dihedral group of order $2n$, let H be $\{1, r, r^2, \ldots, r^{n-1}\}$, the set of all rotations in G. Since the product of two rotations is again a rotation and the inverse of a rotation is also a rotation it follows that H is a subgroup of D_{2n} of order n.

The following result says that the subgroups of G are precisely the nonempty subsets of G that are closed under multiplication and inverses.

Lemma 2.2 (Subgroup criterion)**.** *A set H is a subgroup of G if and only if*

(i) $\varnothing \neq H \subseteq G$, *and*

(ii) $ab^{-1} \in H$ *for all* $a, b \in H$.

Proof. ($\Rightarrow$) This follows from the definition.

($\Leftarrow$) Suppose (i) and (ii) hold. Asociativity of the multiplication of G holds for any subset of G, so in particular it holds on H. Because H is nonempty, we can choose $x \in H$ and using the second condition we see $1_G = xx^{-1} \in H$. Further, if a is any element of H, (ii) implies $a^{-1} = 1_G a^{-1} \in H$. Thus H is closed under inverses. Finally, note H is closed under products since $ab = a(b^{-1})^{-1} \in H$ for any $a, b \in H$.

□

Exercise 4. Prove that if H is a nonempty finite subgroup of G that is closed under multiplication, then H is a subgroup of G.

2.1. Some important subgroups

Definition 2.3. Let G be a group and $A \subseteq G$.

(i) $C_G(A) = \{g \in G \mid gag^{-1} = a \text{ for all } a \in A\}$ is the **centralizer** of A.

(ii) $Z(G) = \{g \in G \mid ga = ag \text{ for all } a \in G\}$ is the center of G.

(iii) $N_G(A) = \{g \in G \mid gAg^{-1} = A\}$ is the normalizer of A, where $gAg^{-1} = \{gxg^{-1} \mid x \in A\}$.

In words, the centralizer of a subset S in a group G is the set of elements in G that commute with all elements of S. The normalizer is the set of elements that leave S fixed under conjugation. Both are subgroups of G.

Proposition 2.4.

(i) $C_G(A), N_G(A), Z(G) \leq G$

(ii) $C_G(G) = G$

(iii) $C_G(A) \leq N_G(A)$

Proof. (i) Let us prove $N_G(A) \leq G$. First note $N_G(A) \neq \varnothing$ as $1 \in N_G(A)$. Now let $x, y \in N_G(A)$. We have Using **??**, we get

(ii) The rest of the proof is trivial and is left to the reader.

Exercise. □

Exercise 5 (Classwork)**.** Assume the following to be true.

(i) If G is a group and $N \trianglelefteq G$, then $|H| \mid |G|$.

(ii) If $H \leq G$, then $H \leq N_G(H)$.

(iii) If $H \trianglelefteq G$, then $H = C_G(H)$ if and only if H is abelian.

Prove that if $G = S_3$ and $A = \{(1), (1\,2\,3), (1\,3\,2)\}$, then $C_G(A) = A$ and $N_G(A) = G$.