INTRODUCTION TO ALGEBRA — HANDOUT 9

Proposition 1. Let G and H be two groups. Then $G \times H$ is a group with

$$(g_1, h_1) \cdot (g_2, h_2) := (g_1 \cdot g_2, h_1 \cdot h_2).$$

This group is called the **direct product** of G and H.

Proof. It is straightforward to show the associativity. The identity of $G \times H$ is (e_g, e_h), and the inverse of (g, h) is (g^{-1}, h^{-1}). $\square$

Example 1. $\mathbb{R} \times \mathbb{R}$, $\mathbb{Z}_2 \times \mathbb{Z}_2$ or $\mathbb{Q} \times \mathbb{Z}_2$.

Proposition 2. $G' = \{(g, e_h) : g \in G\}$ and $H' = \{(e_g, h) : h \in H\}$ are two subgroups of $G \times H$ isomorphic to G and H, and they have the following properties

(1) $G' \cap H' = \{e\}$;
(2) $G \times H = G'H'$, i.e., for all $a \in G \times H$, there are $g \in G'$ and $h \in H'$ such that $a = gh$;
(3) $G' \lhd G \times H$ and $H' \lhd G \times H$ (or equivalently $gh = hg$ for all $g \in G'$ and $h \in H'$);

Definition 1. If two subgroups N_1 and N_2 of a group G have the properties of Proposition 2, then G is called the **internal direct product** of N_1 and N_2.

Lemma 1. $\mathbb{Z}_{mn}$ is isomorphic to $\mathbb{Z}_m \times \mathbb{Z}_n$ iff m and n are relative primes, i.e., their greatest common divisor is 1.

Example 2.

- $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$.
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \ncong \mathbb{Z}_4$.

Theorem 1. Every finitely generated abelian group can be decomposed as

$$\mathbb{Z}^n \times \mathbb{Z}_{p_1^{n_1}} \times \ldots \times \mathbb{Z}_{p_k^{n_k}},$$

where $p_1, \ldots, p_k$ are prime numbers. This decomposition is unique up to ordering.

Example 3.

- $\mathbb{Z}_{42} \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_7$,
- $\mathbb{Z}_{12} \cong \mathbb{Z}_3 \times \mathbb{Z}_4 \ncong \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

Example 4. $\langle \mathbb{Q}, + \rangle$ is not finitely generated.

Definition 2. A group G is called **Boolean group** if $a^2 = e$ for all $a \in G$.

Exercise 1. Show that

- every Boolean group is commutative, and
- every finite Boolean group has 2^n elements for some natural number n.

Proposition 3. Let $\langle B, \wedge, \vee, ^-, 0, 1 \rangle$ be a Boolean algebra. Then B is a Boolean group with the symmetric difference $x \triangle y := (\bar{x} \wedge y) \vee (x \wedge \bar{y})$.

Proof. Associativity: calculation. Identity is 0 and $x \triangle x = 0$. $\square$

Definition 3. Theory T said to be **interpretable** in S if every basic concept of T can be defined explicitly in S such that the translation of the axioms of T are theorems in S.

Example 5. By Proposition 3, the theory of Boolean groups is interpretable in the theory of Boolean algebras.

Proposition 4. The theory of Boolean algebras is not interpretable in the theory of Boolean Groups.