MATH 433
Applied Algebra

Lecture 30:
Direct product of groups.
Quotient group.

Direct product of binary structures

Given nonempty sets G and H, the Cartesian product $G \times H$ is the set of all ordered pairs (g, h) such that $g \in G$ and $h \in H$. Suppose $*$ is a binary operation on G and $\star$ is a binary operation on H. Then we can define a binary operation $\bullet$ on $G \times H$ by

$$(g_1, h_1) \bullet (g_2, h_2) = (g_1 * g_2,\ h_1 \star h_2).$$

Proposition 1 The operation $\bullet$ is fully (resp. uniquely, well) defined if and only if both $*$ and $\star$ are.

Proposition 2 The operation $\bullet$ is associative (resp. commutative) if and only if both $*$ and $\star$ are.

Proposition 3 A pair (e_G, e_H) is the identity element in $G \times H$ if and only if e_G is the identity element in G and e_H is the identity element in H.

Proposition 4 $(g', h') = (g, h)^{-1}$ in $G \times H$ if and only if $g' = g^{-1}$ in G and $h' = h^{-1}$ in H.

Direct product of groups

Given nonempty sets G and H, the Cartesian product $G \times H$ is the set of all ordered pairs (g, h) such that $g \in G$ and $h \in H$. Suppose $*$ is a binary operation on G and $\star$ is a binary operation on H. Then we can define a binary operation $\bullet$ on $G \times H$ by

$$(g_1, h_1) \bullet (g_2, h_2) = (g_1 * g_2,\ h_1 \star h_2).$$

Theorem The set $G \times H$ with the operation $\bullet$ is a group if and only if both $(G, *)$ and $(H, \star)$ are groups.

The group $G \times H$ is called the **direct product** of the groups G and H. Usually the same notation (multiplicative or additive) is used for all three groups:

$$(g_1, h_1)(g_2, h_2) = (g_1 g_2,\ h_1 h_2) \text{ or}$$
$$(g_1, h_1) + (g_2, h_2) = (g_1 + g_2,\ h_1 + h_2).$$

Similarly, we can define the direct product $G_1 \times G_2 \times \cdots \times G_n$ of any finite collection of groups $G_1, G_2, \ldots, G_n$.

Example. $\mathbb{Z}_2 \times \mathbb{Z}_3$ (with addition in $\mathbb{Z}_2$ and $\mathbb{Z}_3$).

The group consists of 6 elements. It is Abelian since $\mathbb{Z}_2$ and $\mathbb{Z}_3$ are both Abelian. The identity element is $([0]_2, [0]_3)$. Let $g = ([1]_2, [1]_3)$. Then $2g = g + g = ([0]_2, [2]_3)$, $3g = ([1]_2, [0]_3)$, $4g = ([0]_2, [1]_3)$, $5g = ([1]_2, [2]_3)$, and $6g = ([0]_2, [0]_3)$. It follows that $\mathbb{Z}_2 \times \mathbb{Z}_3$ is a cyclic group, $\mathbb{Z}_2 \times \mathbb{Z}_3 = \langle g \rangle$.

Theorem If g has finite order in a group G and h has finite order in a group H, then (g, h) has finite order in $G \times H$ equal to $\operatorname{lcm}\big(o(g), o(h)\big)$. [*Hint:* $(g, h)^n = (g^n, h^n)$.]

Theorem The direct product of nontrivial cyclic groups is cyclic if and only if they are all finite and their orders are pairwise coprime.

For example, groups $\mathbb{Z}_3 \times \mathbb{Z}_5$, $\mathbb{Z}_4 \times \mathbb{Z}_{15}$, and $\mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_7$ are cyclic while groups $\mathbb{Z}_4 \times \mathbb{Z}_6$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$, $\mathbb{Z}_3 \times \mathbb{Z}$, and $\mathbb{Z} \times \mathbb{Z}$ are not.

Quotient space

Let X be a nonempty set and $\sim$ be an equivalence relation on X. Given an element $x \in X$, the **equivalence class** of x, denoted $[x]_\sim$ or simply $[x]$, is the set of all elements of X that are **equivalent** (i.e., related by $\sim$) to x:

$$[x]_\sim = \{y \in X \mid y \sim x\}.$$

Theorem Equivalence classes of the relation $\sim$ form a partition of the set X.

The set of all equivalence classes of $\sim$ is denoted $X/\sim$ and called the **quotient space** (or **factor space**) of X by the relation $\sim$.

In the case when the set X carries some structure (algebraic, geometric, analytic, etc.), this structure may (or may not) induce an analogous structure on the quotient space $X/\sim$.

Examples of quotient spaces

- $X = \mathbb{Z}$, $x \sim y$ if and only if $x \equiv y \mod n$.

Equivalence class of an integer m is the congruence class modulo n, $[m]_\sim = [m]_n = m + n\mathbb{Z}$. The quotient space $\mathbb{Z}/\!\sim$ is $\mathbb{Z}_n$.

- $X = G$, a group; $x \sim y$ if and only if $x \in yH$, where H is a subgroup.

Equivalence class of an element $g \in G$ is the coset of the subgroup H, $[g]_\sim = gH$. The quotient space $G/\!\sim$ is the set of all cosets of H in G. In this example, the quotient space is usually denoted G/H.

Remark. The first example is a particular case of the second, when $G = \mathbb{Z}$ and $H = n\mathbb{Z}$. Hence $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$.

Quotient group

Let G be a nonempty set with a binary operation $*$. Given an equivalence relation $\sim$ on G, we say that the relation $\sim$ is **compatible** with the operation $*$ if for any $g_1, g_2, h_1, h_2 \in G$,

$$g_1 \sim g_2 \text{ and } h_1 \sim h_2 \implies g_1 * h_1 \sim g_2 * h_2.$$

If this is the case, we can define an operation on the quotient space $G/\sim$ by $[g] \star [h] = [g * h]$ for all $g, h \in G$. Compatibility is required so that the operation $\star$ is defined uniquely: if $[g'] = [g]$ and $[h'] = [h]$ then $[g' * h'] = [g * h]$.

If the operation $*$ is associative (resp. commutative), then so is $\star$. If e is the identity element for $*$, then its equivalence class $[e]$ is the identity element for $\star$. If $h = g^{-1}$ in $(G, *)$, then $[h] = [g]^{-1}$ in $(G/\sim, \star)$.

Thus, if $(G, *)$ is a group then $(G/\sim, \star)$ is also a group called the **quotient group** (or **factor group**). Moreover, if the group $(G, *)$ is Abelian then so is $(G/\sim, \star)$.

Question. When is an equivalence relation $\sim$ on a group G compatible with the operation?

Let G be a group and assume that an equivalence relation $\sim$ on G is compatible with the operation (so that the quotient space $G/{\sim}$ is also the quotient group). What can we derive from this? For simplicity, let us use multiplicative notation.

Lemma 1 The equivalence class of the identity element is a subgroup of G.

Proof. Let $H = [e]_\sim$ be the equivalence class of the identity element e. We need to show that **(i)** $e \in H$, **(ii)** $h_1, h_2 \in H \implies h_1 h_2 \in H$, and **(iii)** $h \in H \implies h^{-1} \in H$.

By reflexivity, $e \sim e$. Hence $e \in H$. Further, if $h_1, h_2 \in H$, then $h_1 \sim e$ and $h_2 \sim e$. By compatibility, $h_1 h_2 \sim ee = e$ so that $h_1 h_2 \in H$. Next, if $h \in H$ then $h \sim e$. Also, $h^{-1} \sim h^{-1}$. By compatibility, $hh^{-1} \sim eh^{-1}$, that is, $e \sim h^{-1}$. By symmetry, $h^{-1} \sim e$ so that $h^{-1} \in H$.

Lemma 2 Each equivalence class is a left coset of the subgroup $H = [e]_\sim$.

Proof. We need to prove that $[g]_\sim = gH$ for all $g \in G$. We are going to show that $gH \subset [g]_\sim$ and $[g]_\sim \subset gH$.

Suppose $a \in gH$, that is, $a = gh$ for some $h \in H$. Then $g \sim g$ and $h \sim e$, which implies that $gh \sim ge = g$. Hence $a \in [g]_\sim$. Conversely, suppose $a \in [g]_\sim$. We have $a = ea = (gg^{-1})a = g(g^{-1}a)$. Since $g^{-1} \sim g^{-1}$ and $a \sim g$, it follows that $g^{-1}a \sim g^{-1}g = e$. Hence $g^{-1}a \in H$ so that $a = g(g^{-1}a) \in gH$.

Lemma 3 Each equivalence class is a right coset of the subgroup $H = [e]_\sim$.

Proof. Analogous to the proof of Lemma 2.

Definition. A subgroup H of a group G is called **normal** if $gH = Hg$ for all $g \in G$, that is, each left coset of H is also a right coset. *Notation:* $H \triangleleft G$ or $H \trianglelefteq G$.

Quotient group

Question. When is an equivalence relation $\sim$ on a group G compatible with the operation?

Theorem Assume that the quotient space $G/\sim$ is also the quotient group. Then
(i) $H = [e]_\sim$, the equivalence class of the identity element, is a subgroup of G,
(ii) $[g]_\sim = gH$ for all $g \in G$,
(iii) $G/\sim = G/H$,
(iv) the subgroup H is **normal**, which means that $gH = Hg$ for all $g \in G$.

Theorem If H is a normal subgroup of a group G, then G/H is indeed the quotient group.