MATH 415

Modern Algebra I

Lecture 9: Direct product of groups. Factor groups.

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 $G_1, G_2, \ldots, G_n$.

Examples.

- $\mathbb{Z}_2 \times \mathbb{Z}_3$ (with $+_2$ in $\mathbb{Z}_2$ and $+_3$ in $\mathbb{Z}_3$).

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

- $\mathbb{Z}_2 \times \mathbb{Z}_2$ (with $+_2$ in $\mathbb{Z}_2$).

The group consists of 4 elements. Each of the three nonzero elements $(1,0)$, $(0,1)$ and $(1,1)$ has order 2. It follows that the direct product is not a cyclic group. Note that the sum of any two of the three nonzero elements equals the third one. Hence $\mathbb{Z}_2 \times \mathbb{Z}_2$ is a model of the Klein 4-group.

Theorem Let $G_1, G_2, \dots, G_k$ be groups and suppose g_i is an element of finite order n_i in G_i, $1 \leq i \leq k$. Then the element $g = (g_1, g_2, \dots, g_k)$ has finite order in $G_1 \times G_2 \times \cdots \times G_k$ equal to $\mathrm{lcm}(n_1, n_2, \dots, n_k)$.

Proof: Let us use multiplicative notation for all groups. It follows from the definition of the direct product that $g^n = (g_1^n, g_2^n, \dots, g_k^n)$ for any integer $n > 0$. Hence g^n is the identity element in the direct product if and only if each g_i^n is the identity element in G_i. For the latter, we need n to be divisible by each n_i. The least number with this property is $\mathrm{lcm}(n_1, n_2, \dots, n_k)$.

Corollary The direct product $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$ is a cyclic group if and only if the numbers $n_1, n_2, \dots, n_k$ 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 $\mathbb{Z}_4 \times \mathbb{Z}_6$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ are not.

Corollary The direct product $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$ is a cyclic group if and only if the numbers $n_1, n_2, \ldots, n_k$ are pairwise coprime.

Proof: A finite group is cyclic if and only if it has an element of the same order as the order of the group. Consider an arbitrary element $g = (g_1, g_2, \ldots, g_k)$ of the direct product. Let m_i be the order of g_i in the group G_i, $1 \leq i \leq k$. By the theorem, the order of g equals $\operatorname{lcm}(m_1, m_2, \ldots, m_k)$. By Lagrange's Theorem, each m_i (the order of the element g_i) divides n_i (the order of the group $\mathbb{Z}_{n_i}$). It follows that $\operatorname{lcm}(m_1, m_2, \ldots, m_k)$ divides $\operatorname{lcm}(n_1, n_2, \ldots, n_k)$. Moreover, if $g = (1, 1, \ldots, 1)$ then $m_i = n_i$ for all i so that the order of g is exactly $\operatorname{lcm}(n_1, n_2, \ldots, n_k)$. We conclude that $\operatorname{lcm}(n_1, n_2, \ldots, n_k)$ is the largest possible order for an element in our direct product. Thus the direct product is a cyclic group if and only if $\operatorname{lcm}(n_1, n_2, \ldots, n_k) = n_1 n_2 \ldots n_k$, which happens exactly when the numbers $n_1, n_2, \ldots, n_k$ are pairwise coprime.

Factor 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 **factor space** (or **quotient 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 factor space $X/\sim$.

Examples of factor spaces

- $X = G$, a group; $x \sim y$ if and only if $x = yh$ for some $h \in H$, where H is a fixed subgroup.

Equivalence class of an element $g \in G$ is a left coset of the subgroup H, $[g]_\sim = gH$. The factor space $G/\sim$ is the set of all left cosets of H in G. It is usually denoted G/H.

- $X = G$, a group; $x \sim y$ if and only if $x = hy$ for some $h \in H$, where H is a fixed subgroup.

Equivalence class of an element $g \in G$ is a right coset of the subgroup H, $[g]_\sim = Hg$. The factor space $G/\sim$ is the set of all right cosets of H in G. It is often denoted $H\backslash G$.

- $X = G$, a group; $x \sim y$ if and only if $x \in KyH = \{kyh : h \in H, k \in K\}$, where H and K are fixed subgroups.

In this example, $[g]_\sim = KgH$ (a **double coset**). The factor space $G/\sim$ is usually denoted $K\backslash G/H$.

Factor 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 factor 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 **factor group** (or **quotient 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 factor space $G/\!\sim$ is also the factor group). 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 $H \trianglelefteq G$.

Factor group

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

Theorem Assume that the factor space $G/\!\sim$ is also a factor 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 a factor group.

Alternative construction of the factor group

Suppose G is a group (with multiplicative notation). For any $X, Y \subset G$ let $XY = \{xy \mid x \in X,\ y \in Y\}$. This "multiplication of sets" is a well-defined operation on $\mathcal{P}(G)$, the set of all subsets of G. The operation is associative: $(XY)Z = X(YZ)$ for any sets $X, Y, Z \subset G$. Indeed,

$$(XY)Z = \{(xy)z \mid x \in X,\ y \in Y,\ z \in Z\},$$
$$X(YZ) = \{x(yz) \mid x \in X,\ y \in Y,\ z \in Z\}.$$

Proposition If H is a normal subgroup of G, then for all $a, b \in G$ we have $(aH)(bH) = (ab)H$ in the sense of the above definition.

Alternative construction of the factor group

Suppose G is a group (with multiplicative notation). For any sets $X, Y \subset G$ let $XY = \{xy \mid x \in X,\ y \in Y\}$.

Proposition If H is a normal subgroup of G, then for all $a, b \in G$ we have $(aH)(bH) = (ab)H$ in the sense of the above definition.

Proof. In terms of multiplication of sets, any coset gH can be written as $\{g\}H$. Therefore $(aH)(bH) = (\{a\}H)(\{b\}H)$. By associativity, this is the same as $\{a\}(H\{b\})H$. Now $H\{b\}$ is the right coset Hb. Since the subgroup H is normal, we have $Hb = bH = \{b\}H$. Again by associativity,

$$(aH)(bH) = \{a\}(\{b\}H)H = (\{a\}\{b\})(HH).$$

Clearly, $\{a\}\{b\} = \{ab\}$. It remains to show that $HH = H$. Indeed, $HH \subset H$ since the subgroup H is closed under the operation. Conversely, $H = \{e\}H \subset HH$.