MATH 415

Modern Algebra I

Lecture 14: Factor groups (continued). Homomorphisms of groups.

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, $H = \{e\}H \subset HH$.

Homomorphism of groups

Definition. Let G and H be groups. A function $f : G \to H$ is called a **homomorphism** of groups if $f(g_1 g_2) = f(g_1) f(g_2)$ for all $g_1, g_2 \in G$.

Examples of homomorphisms:

- Residue modulo n of an integer.

For any $k \in \mathbb{Z}$ let $f(k)$ be the remainder of k under division by n. Then $f : \mathbb{Z} \to \mathbb{Z}_n$ is a homomorphism of the group $(\mathbb{Z}, +)$ onto the group $(\mathbb{Z}_n, +_n)$.

- Fractional part of a real number.

For any $x \in \mathbb{R}$ let $f(x) = \{x\} = x - \lfloor x \rfloor$ (fractional part of x). Then $f : \mathbb{R} \to [0, 1)$ is a homomorphism of the group $(\mathbb{R}, +)$ onto the group $([0, 1), +_1)$.

- Sign of a permutation.

The function $\operatorname{sgn} : S_n \to \{-1, 1\}$ is a homomorphism of the symmetric group S_n onto the multiplicative group $\{-1, 1\}$.

- Determinant of an invertible matrix.

The function $\det : GL(n, \mathbb{R}) \to \mathbb{R} \setminus \{0\}$ is a homomorphism of the general linear group $GL(n, \mathbb{R})$ onto the multiplicative group $\mathbb{R} \setminus \{0\}$.

- Linear transformation.

Any vector space is an abelian group with respect to vector addition. If $f : V_1 \to V_2$ is a linear transformation between vector spaces, then f is also a homomorphism of groups.

- Trivial homomorphism.

Given groups G and H, we define $f : G \to H$ by $f(g) = e_H$ for all $g \in G$, where e_H is the identity element of H.

Properties of homomorphisms

Let $f : G \to H$ be a homomorphism of groups.

- The identity element e_G in G is mapped to the identity element e_H in H.

$f(e_G) = f(e_G e_G) = f(e_G)f(e_G)$. Also, $f(e_G) = f(e_G)e_H$.
By cancellation in H, we get $f(e_G) = e_H$.

- $f(g^{-1}) = (f(g))^{-1}$ for all $g \in G$.

$f(g)f(g^{-1}) = f(gg^{-1}) = f(e_G) = e_H$. Similarly,
$f(g^{-1})f(g) = e_H$. Thus $f(g^{-1}) = (f(g))^{-1}$.

- $f(g^n) = (f(g))^n$ for all $g \in G$ and $n \in \mathbb{Z}$.

- The order of $f(g)$ divides the order of g.

Indeed, $g^n = e_G \implies (f(g))^n = e_H$ for any $n \in \mathbb{N}$.

Properties of homomorphisms

Let $f : G \to H$ be a homomorphism of groups.

- If K is a subgroup of G, then $f(K)$ is a subgroup of H.
- If L is a subgroup of H, then $f^{-1}(L)$ is a subgroup of G.
- If L is a normal subgroup of H, then $f^{-1}(L)$ is a normal subgroup of G.
- $f^{-1}(e_H)$ is a normal subgroup of G called the **kernel** of f and denoted $\mathrm{Ker}(f)$.