Overview / review of cosets, factor groups, and homomorphisms
for MATH 421, from **Abstract Algebra**, *3rd Ed.*, Sections 3.7 – 3.8

Cosets and normal subgroups

Definition 3.8.3. Let H be a subgroup of the group G, and let $a \in G$. The set

$$aH = \{x \in G \mid x = ah \ \text{ for some } \ h \in H\}$$

is called the *left coset* of H in G determined by a. Similarly, the *right coset* of H in G determined by a is the set $Ha = \{x \in G \mid x = ha \ \text{ for some } \ h \in H\}$.

The number of left cosets of H in G is called the *index* of H in G, and is denoted by $[G : H]$.

Proposition 3.8.1. Let H be a subgroup of the group G, and let $a, b \in G$. Then the following conditions are equivalent: (1) $bH = aH$; (2) $bH \subseteq aH$; (3) $b \in aH$; (4) $a^{-1}b \in H$.

A result similar to Proposition 3.8.1 holds for right cosets. Let H be a subgroup of the group G, and let $a, b \in G$. Then the following conditions are equivalent: (1) $Ha = Hb$; (2) $Ha \subseteq Hb$; (3) $a \in Hb$; (4) $ab^{-1} \in H$; (5) $ba^{-1} \in H$; (6) $b \in Ha$; (7) $Hb \subseteq Ha$. The index of H in G could also be defined as the number of right cosets of H in G, since there is a one-to-one correspondence between left cosets and right cosets.

Definition 3.7.5. A subgroup H of the group G is called a *normal* subgroup if $ghg^{-1} \in H$ for all $h \in H$ and $g \in G$.

Proposition 3.8.8. Let H be a subgroup of the group G. The following conditions are equivalent:
(1) H is a normal subgroup of G;
(2) $aH = Ha$ for all $a \in G$;
(3) for all $a, b \in G$, abH is the set theoretic product $(aH)(bH)$;
(4) for all $a, b \in G$, $ab^{-1} \in H$ if and only if $a^{-1}b \in H$.

Example 3.8.8. Any subgroup of index 2 is normal.

Factor groups

Proposition 3.8.4. Let N be a normal subgroup of G, and let $a, b, c, d \in G$. If $aN = cN$ and $bN = dN$, then $abN = cdN$.

Theorem 3.8.5. If N is a normal subgroup of G, then the set of left cosets of N forms a group under the coset multiplication given by $\qquad aNbN = abN \qquad$ for all $a, b \in G$.

Definition 3.8.5. If N is a normal subgroup of G, then the group of left cosets of N in G is called the *factor group* of G determined by N. It will be denoted by G/N.

Example 3.8.5. Let N be a normal subgroup of G. If $a \in G$, then the order of aN is the smallest positive integer n such that $a^n \in N$.

Group homomorphisms

Definition 3.7.1. Let G_1 and G_2 be groups, and let $\phi : G_1 \to G_2$ be a function. Then ϕ is said to be a *group homomorphism* if $\qquad \phi(ab) = \phi(a)\phi(b) \qquad$ for all $a, b \in G_1$.

Example 3.7.3. (Exponential functions for groups) Let G be a group, and let a be any element of G. Define $\phi : \mathbf{Z} \to G$ by $\phi(n) = a^n$, for all $n \in \mathbf{Z}$. This is a group homomorphism from $\mathbf{Z}$ to G.

If G is abelian, with its operation denoted additively, then we define $\phi : \mathbf{Z} \to G$ by $\phi(n) = na$.

Example 3.7.4. (Linear transformations) Let V and W be vector spaces. Since any vector space is an abelian group under vector addition, any linear transformation between vector spaces is a group homomorphism.

Proposition 3.7.2. If $\phi : G_1 \to G_2$ is a group homomorphism, then
(a) $\phi(e) = e$;
(b) $(\phi(a))^{-1} = \phi(a^{-1})$ for all $a \in G_1$;
(c) for any integer n and any $a \in G_1$, $\phi(a^n) = (\phi(a))^n$;
(d) if $a \in G_1$ and a has order n, then the order of $\phi(a)$ in G_2 is a divisor of n.

Example 3.7.6. (Homomorphisms defined on cyclic groups) Let C be a cyclic group, denoted multiplicatively, with generator a. If $\phi : C \to G$ is any group homomorphism, and $\phi(a) = g$, then the formula $\phi(a^m) = g^m$ must hold. Since every element of C is of the form a^m for some $m \in \mathbf{Z}$, this means that ϕ is completely determined by its value on a.

If C is infinite, then for an element g of any group G, the formula $\phi(a^m) = g^m$ defines a homomorphism.

If $|C| = n$ and g is any element of G whose order is a divisor of n, then the formula $\phi(a^m) = g^m$ defines a homomorphism.

Example 3.7.7. (Homomorphisms from $\mathbf{Z}_n$ to $\mathbf{Z}_k$) Any homomorphism $\phi : \mathbf{Z}_n \to \mathbf{Z}_k$ is completely determined by $\phi([1]_n)$, and this must be an element $[m]_k$ of $\mathbf{Z}_k$ whose order is a divisor of n. Then the formula $\phi([x]_n) = [mx]_k$, for all $[x]_n \in \mathbf{Z}_n$, defines a homomorphism. Furthermore, every homomorphism from $\mathbf{Z}_n$ into $\mathbf{Z}_k$ must be of this form. The image $\phi(\mathbf{Z}_n)$ is the cyclic subgroup generated by $[m]_k$.

Definition 3.7.3 Let $\phi : G_1 \to G_2$ be a group homomorphism. Then $\{x \in G_1 \mid \phi(x) = e\}$ is called the *kernel* of ϕ, and is denoted by $\ker(\phi)$.

Proposition 3.7.4 Let $\phi : G_1 \to G_2$ be a group homomorphism, with $K = \ker(\phi)$.
(a) K is a subgroup of G_1 such that $gkg^{-1} \in K$ for all $k \in K$ and $g \in G_1$.
(b) The homomorphism ϕ is one-to-one if and only if $K = \{e\}$.

Proposition 3.7.6 Let $\phi : G_1 \to G_2$ be a group homomorphism.

(a) If H_1 is a subgroup of G_1, then $\phi(H_1)$ is a subgroup of G_2. If ϕ is onto and H_1 is normal in G_1, then $\phi(H_1)$ is normal in G_2.

(b) If H_2 is a subgroup of G_2, then $\phi^{-1}(H_2) = \{x \in G_1 \mid \phi(x) \in H_2\}$ is a subgroup of G_1. If H_2 is a normal in G_2, then $\phi^{-1}(H_2)$ is normal in G_1.

Proposition 3.8.7. Let N be a normal subgroup of G.

(a) The natural projection mapping $\pi : G \to G/N$ defined by $\pi(x) = xN$, for all $x \in G$, is a homomorphism, and $\ker(\pi) = N$.

(b) There is a one-to-one correspondence between subgroups of G/N and subgroups H of G with $H \supseteq N$. Under this correspondence, normal subgroups correspond to normal subgroups.

Example 3.8.10. $\mathbf{Z}_n/m\mathbf{Z}_n \cong \mathbf{Z}_m$ if $m|n$.

Theorem 3.8.9. [Fundamental Homomorphism Theorem] Let G_1, G_2 be groups. If $\phi : G_1 \to G_2$ is a homomorphism with $K = \ker(\phi)$, then $G_1/K \cong \phi(G_1)$.

Definition 3.8.10. The group G is called a *simple* group if it has no proper nontrivial normal subgroups.