1.6 Cosets

The choice of a subgroup leads to a surprising amount of structure on a group.

1.6.1 Definition. Let H be a subgroup of G. The ***left coset*** of H in G determined by an element $g \in G$ is the set $g\,H := \{g\,h \mid h \in H\}$. Similarly, the ***right coset*** is $H\,g := \{h\,g \mid h \in H\}$.

The concept and notation for a coset was used by Évariste Galois. However, the term *coset* was introduced by George Abram Miller (1910).

1.6.2 Example. Consider $\mathbb{R}^2$ as an additive abelian group. A line L through the origin is a subgroup. For a point $p \in \mathbb{R}^2$, the left coset $p + L$ is the line containing p parallel to L. ⋄

1.6.3 Example. Let $H := \langle (2\ \ 1) \rangle$ be a subgroup of the symmetric group $\mathfrak{S}_3$. The distinct left cosets and the distinct right cosets are

$$\begin{aligned} H = (2\ \ 1)\,H &= \{(1), (2\ \ 1)\}, & H = H\,(2\ \ 1) &= \{(1), (2\ \ 1)\}, \\ (3\ \ 1)\,H = (3\ \ 1\ \ 2)\,H &= \{(3\ \ 1), (3\ \ 1\ \ 2)\}, & H\,(3\ \ 1) = H\,(3\ \ 2\ \ 1) &= \{(3\ \ 1), (3\ \ 2\ \ 1)\}, \\ (3\ \ 2)\,H = (3\ \ 2\ \ 1)\,H &= \{(3\ \ 2), (3\ \ 2\ \ 1)\}, & H\,(3\ \ 2) = H\,(3\ \ 1\ \ 2) &= \{(3\ \ 2), (3\ \ 1\ \ 2)\}. \end{aligned}$$

Notice that they are not equal. ⋄

1.6.4 Lemma. *Let H be a subgroup of a group G.*

(i) *The left cosets of H partition the elements in G.*

(ii) *Two elements $f, g \in G$ belong to the same left coset of H if and only if the relation $g^{-1} f \in H$ holds.*

(iii) *For any element $g \in G$, the map $h \mapsto g\,h$ defines a bijection from left coset H and the left coset $g\,H$.*

Proof.

(i) It suffices to prove that left cosets are equivalence classes for the *congruence* relation: two element $f, g \in G$ are congruent, denoted by $f \equiv g$, if there exists an element $h \in H$ such that $f = g\,h$. We verify that congruence is an equivalence relation.

(transitive) Suppose that $f \equiv g$ and $g \equiv g'$. By definition, there exists elements $h, h' \in H$ such $f = g\,h$ and $g = g'\,h'$, so we obtain $f = g'\,(h'\,h)$. Since $h'\,h \in H$, it follows that $f \equiv g'$.

(symmetric) If $f \equiv g$, then there exists $h \in H$ such that $f = g\,h$, so $g = f\,h^{-1}$. Since $h^{-1} \in H$, it follows that $g \equiv f$.

(reflexive) Since identity element $e \in G$ belongs to H, we see that, for all $g \in G$, we have $g = g\,e$ and $g \equiv g$.

(ii) The relation $f \in g\,H$ is equivalent to $f \equiv g$ or $g^{-1} f \in H$.

(iii) The inverse map sends $f \in g\,H$ to the element $g^{-1} f$ which by part (ii) belongs to H. □

1.6.5 Definition. For any subgroup H of a group G, the ***index*** $[G : H]$ is the number of distinct left cosets of H in G.

The map $g\,H \mapsto H\,g^{-1}$ defines a bijection between left and right cosets of H in G, so the index is also the number of distinct right cosets.

1.6.6 Example. Example 1.6.3 shows that $[\mathfrak{S}_3 : \langle (2\ \ 1) \rangle] = 3$. ⋄

1.6.7 Example. Given a positive integer n, consider the subgroup $\langle n \rangle$ in $\mathbb{Z}$. For any $m \in \mathbb{Z}$, the left coset $m + \langle n \rangle$ consists of all integers that have the same remainder as m upon division by n. Since the possible remainders are greater than or equal to 0 and less than n, it follows that $[\mathbb{Z} : \langle n \rangle] = n$. ◇

The family of matrices

$$\left\{ \begin{bmatrix} r & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix} \,\middle|\, r \in \mathbb{R}^{\times} \right\}$$

forms a complete set of coset representatives for $\mathrm{SL}(n, \mathbb{R})$ in $\mathrm{GL}(n, \mathbb{R})$.

1.6.8 Example. Given a positive integer n, consider the subgroup $\mathrm{SL}(n, \mathbb{R})$ of $\mathrm{GL}(n, \mathbb{R})$. Two matrices $\mathbf{A}, \mathbf{B} \in \mathrm{GL}(2, \mathbb{R})$ belong to the same left coset of $\mathrm{SL}(n, \mathbb{R})$ if and only if we have $\det(\mathbf{A}^{-1}\mathbf{B}) = 1$ or $\det(\mathbf{A}) = \det(\mathbf{B})$. We deduce that $[\mathrm{GL}(n, \mathbb{R}) : \mathrm{SL}(n, \mathbb{R})] = \infty$. ◇

Joseph-Louis Lagrange (1771) gives a special case of this theorem in work that predates the definition of a group. Camille Jordan (1861) first proves the general form, but attributes the basic idea to Lagrange.

1.6.9 Theorem (Lagrange). *For any subgroup H of a group G, we have $|G| = |H| \cdot [G : H]$. In particular, if G is a finite group, then the order and index of any subgroup are divisors of the order of G.*

Proof. By Lemma 1.6.4, the cosets of H partition the group G into $[G : H]$ sets and each of these cosets has $|H|$ elements. It follows that $|G| = |H| \cdot [G : H]$. □

1.6.10 Corollary. *Let G be a finite group.*

(i) *For all $g \in G$, the order of the element g is a divisor of $|G|$.*

(ii) *For all $g \in G$, we have $g^{|G|} = e$.*

Proof. Since the order of an element is the order of the subgroup it generates, Theorem 1.6.9 shows that the order of g is a divisor of $|G|$. Combining part (i) with Lemma 1.2.10 (ii) proves the second part. □

1.6.11 Corollary. *Every group of prime order is cyclic.*

Proof. Let G be a finite group of prime order. Choose $e \neq g \in G$ and consider the subgroup $H := \langle g \rangle$. Since $\{e, g\} \subseteq H$, we see $|H| > 1$. Since p is prime and Theorem 1.6.9 shows that $|H|$ is a divisor of $|G| = p$, we deduce that $|H| = p$ which means $H = G$. □

1.6.12 Example (Classifying groups of order at most 5). Let G be a finite group with $|G| \leqslant 5$. If $|G| \in \{1, 2, 3, 5\}$, then Corollary 1.6.11 shows that G is cyclic. When $|G| = 4$, Corollary 1.6.10 implies that every non-identity element has order 2 or 4. There are two cases.

(cyclic) When G has an element of order 4, the group G is cyclic.

(non-cyclic) Suppose that G does not have an element of order 4. It follows that $G = \{e, f, g, h\}$ and $f^2 = g^2 = h^2 = e$. If $fg = e$ then we would $fg = f^2$ and $g = f$ which cannot be. Similarly, the product fg cannot equal f or g, so we must have $fg = h$. Analogous arguments demonstrate that $gf = h$, $hf = g = fh$, and $gh = f = hg$. Thus, G is the Klein 4-group; see Figure 1.1. ◇

1.7 Normal Subgroups

Being the kernel of a group homomorphism distinguishes an indispensable class of subgroups.

1.7.1 Definition. A subgroup K of G is ***normal*** if, for all $k \in K$ and all $g \in G$, the product $g\,k\,g^{-1}$ belongs to K.

When K is a normal subgroup of a group G, one typically writes $K \trianglelefteq G$.

1.7.2 Example. Every subgroup of an abelian group is normal. $\diamond$

1.7.3 Example. The subgroup $\langle(2\ 1)\rangle$ in $\mathfrak{S}_3$ is not normal because $(3\ 1\ 2)(2\ 1)(3\ 1\ 2)^{-1} = (3\ 1\ 2)(2\ 1)(3\ 2\ 1) = (3\ 2) \notin \langle(2\ 1)\rangle$. $\diamond$

1.7.4 Remark. Given an element k in a group G, a ***conjugate*** of k is any element in G of the form $g\,k\,g^{-1}$ for some $g \in G$. With this terminology, we see that a subgroup K in a group G is normal if and only if the subset K contains all the conjugates of its elements.

Two matrices $\mathbf{A}, \mathbf{B}$ are ***similar*** if and only if they are conjugate: there exists a nonsingular matrix $\mathbf{P} \in \mathrm{GL}(n, \mathbb{R})$ such that $\mathbf{B} = \mathbf{P}\,\mathbf{A}\,\mathbf{P}^{-1}$.

1.7.5 Example. Every upper triangular matrix is similar to a lower triangular matrix, so the subgroup of upper triangular matrices in not a normal subgroup of $\mathrm{GL}(n, \mathbb{R})$. $\diamond$

1.7.6 Example. The center $Z(G) := \{g \in G : hg = gh \text{ for all } h \in G\}$ is normal because it contains all the conjugates of its elements. $\diamond$

1.7.7 Lemma. *The kernel of a group homomorphism is normal.*

Proof. Let $\varphi : G \to H$ be a group homomorphism. Given elements $k \in \mathrm{Ker}(\varphi)$ and $g \in G$, we have

$$\varphi(g\,k\,g^{-1}) = \varphi(g)\,\varphi(k)\,\varphi(g^{-1}) = \varphi(g)\,e_H\,\varphi(g)^{-1} = e_H\,,$$

Therefore, we conclude that $g\,k\,g^{-1} \in \mathrm{Ker}(\varphi)$. $\square$

1.7.8 Example. Since the subgroup $\mathrm{SL}(n, \mathbb{R})$ in $\mathrm{GL}(n, \mathbb{R})$ is the kernel of the map $\det : \mathrm{GL}(n, \mathbb{R}) \to \mathbb{R}^{\times}$, it is a normal subgroup. $\diamond$

1.7.9 Lemma. *A subgroup K of G is normal if and only if, for any element $g \in G$, we have $g\,K = K\,g$.*

Proof.
- ($\Rightarrow$) Let $g\,k \in g\,K$. Since K is normal, we have $g\,k\,g^{-1} \in K$, so we deduce that $g\,k = (g\,k\,g^{-1})g \in K\,g$ and $g\,K \subseteq K\,g$. Conversely, let $k\,g \in K\,g$. Normality gives $(g^{-1})k(g^{-1})^{-1} = g^{-1}\,k\,g \in K$, so we deduce that $k\,g = g(g^{-1}kg) \in g\,K$ and $K\,g \subseteq g\,K$.
- ($\Leftarrow$) Suppose that $g\,K = K\,g$ for all $g \in G$. Given an element $k \in K$, there exists $k' \in K$ such that $g\,k = k'\,g$. It follows that, for all $g \in G$, we have $g\,k\,g^{-1} \in K$. $\square$

1.7.10 Definition. Let $\mathcal{P}^*(G)$ be the set of all nonempty subsets of a group G. We define a binary operation on $\mathcal{P}^*(G)$ as follows: given $X, Y \in \mathcal{P}^*(G)$, set $X\,Y := \{x\,y \in G \mid x \in X, y \in Y\}$.

The associativity of the product in G implies that this binary operation is also associative.

1.7.11 Example. The singleton $\{e\}$ is the identity for this product on $\mathcal{P}^*(G)$. The product of any singleton $\{g\}$ with a subgroup H is the left coset $g\,H$ or the right coset $H\,g$. For any subgroup H, we also have $H\,H = H$. ◇

We can also view the elements of G/K as equivalence classes, with the multiplication $(g\,K)(h\,K) = gh\,K$ being independent of the choice of representatives.

1.7.12 Theorem. *Let G/K denote the family of all left cosets of a subgroup K of G. When K is normal, we have $(g\,K)(h\,K) = gh\,K$ for all $g, h \in G$ and G/K is a group under this operation.*

Proof. We view $(g\,K)(h\,K)$ as the product of 4 elements in $\mathcal{P}^*(G)$. The associativity of the product in $\mathcal{P}^*(G)$ and the normality of K imply that $(g\,K)(h\,K) = g(K\,h)K = g(h\,K)K = gh\,K$. Hence, the product on $\mathcal{P}^*(G)$ induces a binary operation on G/K. Since the product on $\mathcal{P}^*(G)$ is associativity, this operation on G/K also is. The left coset $K = e\,K$ is the identity because

When K is a normal subgroup, we call G/K the ***quotient*** group. When $|G| < \infty$, Theorem 1.6.9 establishes that $|G/K| = [G : K] = |G| / |K|$.

$$(e\,K)(g\,K) = eg\,K = g\,K = ge\,K = (g\,K)(e\,K)\,.$$

The inverse of the left coset $g\,K$ is $g^{-1}\,K$ because

$$(g^{-1}\,K)(g\,K) = g^{-1}g\,K = e\,K = gg^{-1}\,K = (g\,K)(g^{-1}\,K)\,.$$ □

1.7.13 Corollary. *Every normal subgroup K in a group G is the kernel of the canonical map $\pi : G \to G/K$ defined by $\pi(g) := g\,K$.*

Proof. Since $(g\,K)(h\,K) = gh\,K$ is equivalent to $\pi(g)\,\pi(h) = \pi(gh)$, the map π is a surjective group homomorphism. Since the left coset K is the identity element in the quotient group G/K, it follows that $\operatorname{Ker}(\pi) = \{g \in G \mid \pi(g) = K\} = \{g \in G \mid g\,K = K\} = K$. □

1.7.14 Corollary. *Let $\varphi : G \to G'$ be a group homomorphism. Assume that K is a normal subgroup of G and K' is a normal subgroup of G' such that $\varphi(K) \subseteq K'$. The induced map $\overline{\varphi} : G/K \to G'/K'$, defined by $\overline{\varphi}(g\,K) := \varphi(g)\,K'$, is a group homomorphism.*

Proof. Given $g\,K = h\,K$, it follows that $g^{-1}h \in K$ and

$$\varphi(g)^{-1}\,\varphi(h) = \varphi(g^{-1}\,h) \in \varphi(K) \subseteq K'\,.$$

Hence, we have $\varphi(g)\,K' = \varphi(h)\,K'$, so $\overline{\varphi}$ is well-defined. Since φ is a group homomorphism and both K and K' are normal subgroups, we see that

$$\begin{aligned}\overline{\varphi}\big((g\,K)(h\,K)\big) &= \overline{\varphi}(gh\,K) = \varphi(gh)\,K' = \varphi(g)\,\varphi(h)\,K' \\ &= \big(\varphi(g)\,K'\big)\big(\varphi(h)\,K'\big) = \overline{\varphi}(g\,K)\,\overline{\varphi}(h\,K)\,.\end{aligned}$$

Hence, the map $\overline{\varphi}$ is a group homomorphism. □