

19. COSETS

19.1. Products of subsets in a group.

Definition. Let G be a group and A and B subsets of G . The product of A and B is the subset AB of G defined by

$$AB = \{x \in G : x = ab \text{ for some } a \in A, b \in B.\}$$

The following lemma is left as a homework exercise:

Lemma 19.1. *The multiplication of subsets in a group is associative, that is, if A, B and C are subsets of a group G , then $(AB) \cdot C = A \cdot (BC)$.*

Definition. Let G be a group and H a subgroup of G . If g is an element of G , the set $gH = \{g\}H$ (the product of subsets $\{g\}$ and H) will be called a left coset of H . In other words,

$$gH = \{x \in G : x = gh \text{ for some } h \in H\}$$

(here g is fixed and h ranges over the entire subgroup H .)

From now on a *coset* will mean a left coset.

Below we collect some basic properties of cosets.

Claim. *Let G be a group and H a subgroup of G .*

- (cos1) *Every element of G lies in one of the cosets of H . This is because $g = g \cdot e \in gH$ for every $g \in G$.*
- (cos2) *One of the cosets of H is H itself. This is because $H = eH$.*
- (cos3) *If H is finite, then $|gH| = |H|$ for every $g \in G$. Indeed, suppose that $k = |H|$ and $H = \{h_1, \dots, h_k\}$. By cancellation law, elements gh_1, \dots, gh_k are distinct, so $|gH| = |\{gh_1, \dots, gh_k\}|$.*
- (cos4) *Any two cosets of H are either the same or disjoint. In other words, for any $g, k \in G$ either $gH = kH$ or $gH \cap kH = \emptyset$.*

Property (cos4) is a special case of the following more general result:

Theorem 19.2. *Let G be a group, H a subgroup of G and $g, k \in G$.*

- (i) *If $g^{-1}k \in H$, then $gH = kH$*
- (ii) *If $g^{-1}k \notin H$, then $gH \cap kH = \emptyset$.*

Proof. (i) We are given that $g^{-1}k = h$ for some $h \in H$. Hence $k = gh$, and therefore

$$kH = (gh)H = g(hH) \subseteq gH.$$

Here the equality $(gh)H = g(hH)$ holds by Lemma 19.1, and inclusion $g(hH) \subseteq gH$ follows from $hH \subseteq H$ which, in turn, holds since H is closed under group operation.

Thus, $kH \subseteq gH$. Next note that by product inverse formula $k^{-1}g = (g^{-1}k)^{-1} = h^{-1} \in H$ (since H is closed under inversion). Thus, we can repeat the above argument with roles of g and k switched and conclude that $gH \subseteq kH$.

Thus, we showed that $kH \subseteq gH$ and $gH \subseteq kH$, and so $kH = gH$.

(ii) We will prove this by contrapositive. Suppose that $gH \cap kH \neq \emptyset$, so there exists $x \in gH \cap kH$. This means that $x = gh_1$ and $x = kh_2$ for some $h_1, h_2 \in H$. Hence $kh_2 = gh_1$. Multiplying by g^{-1} on the left and h_2^{-1} on the right, we get $g^{-1}k = h_1h_2^{-1} \in H$, as desired. \square

Corollary 19.3. *Let G be a group, H a subgroup of G and $g, k \in G$. Then $gH = kH \iff g^{-1}k \in H$.*

Proof. The backwards direction holds by Theorem 19.2(i). For the forward direction, suppose that $gH = kH$. If $g^{-1}k \notin H$, then $gH \cap kH = \emptyset$ by Theorem 19.2(ii) which contradicts $gH = kH$. Hence $g^{-1}k \in H$. \square

19.2. Proof of Lagrange Theorem.

Lagrange Theorem. *Let G be a finite group and H a subgroup of G . Then $|H|$ divides $|G|$.*

Proof. Let g_1H, \dots, g_kH be the complete list of cosets of H without repetition. Then $G = g_1H \cup \dots \cup g_kH$ by (cos1) and $g_iH \cap g_jH = \emptyset$ for $i \neq j$ by (cos3). Therefore, $|G| = \sum_{i=1}^k |g_iH|$.

Finally, $|g_iH| = |H|$ for each i by (cos3), whence $|G| = k|H|$, so $|H|$ divides $|G|$. \square

Definition. Let G be a group and H a subgroup of G . The number of distinct cosets of H is called the index of H in G and denoted by $[G : H]$.

The proof of Lagrange theorem shows that when G is a finite group, the index of a subgroup is given by the formula

$$[G : H] = \frac{|G|}{|H|}.$$

19.3. Examples of coset multiplication.

Example 1. $G = S_3 = \text{permutations of } \{1, 2, 3\}$, $H = \langle (1, 2) \rangle = \{e, (1, 2)\}$.

In this example $|G| = 6$, $|H| = 2$, so H should have $3 = \frac{6}{2} = \frac{|G|}{|H|}$ cosets. This is confirmed by an explicit computation below.

g	gH
e	$\{e, (1, 2)\}$
$(1, 2)$	$\{(1, 2), (1, 2)(1, 2)\} = \{(1, 2), e\}$
$(1, 3)$	$\{(1, 3), (1, 3)(1, 2)\} = \{(1, 3), (1, 2, 3)\}$
$(2, 3)$	$\{(2, 3), (2, 3)(1, 2)\} = \{(2, 3), (1, 3, 2)\}$
$(1, 2, 3)$	$\{(1, 2, 3), (1, 2, 3)(1, 2)\} = \{(1, 2, 3), (1, 3)\}$
$(1, 3, 2)$	$\{(1, 3, 2), (1, 3, 2)(1, 2)\} = \{(1, 3, 2), (2, 3)\}$

The distinct cosets of H are $\{e, (1, 2)\}$, $\{(1, 3), (1, 2, 3)\}$ and $\{(2, 3), (1, 3, 2)\}$.

Example 2. Let $G = (\mathbb{Z}, +)$, $H = 3\mathbb{Z} = \{3k : k \in \mathbb{Z}\}$. Here the group operation is addition, so cosets of H are subsets of the form $g + H$ with $g \in G$.

We have $0 + H = H = \{3k : k \in \mathbb{Z}\}$, $1 + H = \{1 + 3k : k \in \mathbb{Z}\}$ and $2 + H = \{2 + 3k : k \in \mathbb{Z}\}$. These 3 cosets cover the entire \mathbb{Z} , so there are 3 distinct cosets.

In general, for any $i \in \mathbb{Z}$ we have $i + H = \{x \in \mathbb{Z} : x \equiv i \pmod{3}\} = [i]_3$, the congruence class of $i \pmod{3}$.

19.4. Book references. This lectures follows [Gilbert, 4.4] pretty closely. Pinter introduces cosets in Chapter 13, although some of their basic properties are established later in Chapter 15. Note that Pinter primarily works with right cosets! (the theory of right cosets is completely analogous, but some statements like Theorem 19.2 should be suitably modified if left cosets are replaced by right cosets).