11 Lagrange's theorem and consequences (10/13)

Definition 11.1 (Cosets)**.** Let G be a group and $H \subseteq G$ a subgroup. Given $g \in G$, define

$$gH = \{gh : h \in H\} \quad \text{and} \quad Hg = \{hg : h \in H\},$$

the left and right **cosets** of H containing g. (Note that $g \in gH$ and $g \in Hg$.) These are subsets of G.

Remark 11.2. When G is written additively, the cosets are often written $g + H$.

Example 11.3. Suppose we consider the subgroup $H = \{0, 2, 4\}$ of $\mathbf{Z}/6 = \{0, 1, 2, 3, 4, 5\}$. The right cosets are

$$\begin{aligned} H + 0 &= \{0, 2, 4\}, \\ H + 1 &= \{1, 3, 5\}, \\ H + 2 &= \{0, 2, 4\}, \\ H + 3 &= \{1, 3, 5\}, \\ H + 4 &= \{0, 2, 4\}, \\ H + 5 &= \{1, 3, 5\}. \end{aligned}$$

This scintillating pattern is explained in Lemma 11.5.

Example 11.4. Suppose we consider the subgroup $H = \{e, (1\,2)\}$ of S_3. The right cosets are

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

Lemma 11.5. *Let G be a group and $H \subseteq G$ a subgroup. If $g_0, g_1 \in G$, then the following are equivalent:*

(i) $g_0H \cap g_1H \neq \emptyset$,

(ii) $g_0^{-1}g_1 \in H$,

(iii) $g_0H = g_1H$.

Proof. Suppose that $g_0H \cap g_1H \neq \emptyset$. Then, there exist $h_0, h_1 \in H$ such that $g_0h_0 = g_1h_1$, which implies $h_0h_1^{-1} = g_0^{-1}g_1$ (multiplying on the left by g_0^{-1} and on the right by h_1^{-1}). So, (i) implies (ii) since $h_0h_1^{-1}$ is in H as H is a subgroup of G. Assume $g_0^{-1}g_1 \in H$, in which case the inverse $g_1^{-1}g_0$ is also in H. Then, for $h \in H$, we have $g_1h \in g_1H$. But, $g_1g_1^{-1}g_0h = g_0h$ is also in g_1H, so $g_0H \subseteq g_1H$. Similarly, $g_1H \subseteq g_0H$, so (ii) implies (iii). Finally, (iii) implies (i) using that cosets are always nonempty. ☐

Remark 11.6. Lemma 11.5 holds with right cosets instead of left cosets where condition (ii) is replaced by

(ii) $g_1g_0^{-1} \in H$.

Remark 11.7. Say that $g_0 \sim g_1$ if the equivalent conditions of Remark 11.6 hold. This defines an equivalence relation on G with equivalence classes given by the varying Hg. The set of equivalence classes (right cosets) is written as G/H. (Note that left and right cosets do not generally agree. There is an example in S_3.)

Remark 11.8. If H is a subgroup of G we can view it as acting on G via $h \cdot g = hg$. The orbit of H containing g, written $H \cdot g$ in Lecture 10, is the right coset Hg.

Lemma 11.9. *Let G be a group, $H \subseteq G$ a subgroup, and $g_0, g_1 \in G$. Multiplication on the right by $g_0^{-1}g_1$ gives a bijection $Hg_0 \to Hg_1$.*

Proof. Given hg_0, we have $(hg_0)(g_0^{-1}g_1) = hg_1$, so this operation defines a function $Hg_0 \to Hg_1$. It has an inverse given by right multiplication by $g_1^{-1}g_0$, so it is a bijection. □

Corollary 11.10. *If G is a group and $H \subseteq G$ is a finite group, then any two right cosets Hg_0 and Hg_1 have the same number of elements (equal to the number of elements of H).*

Proof. Bijective finite sets have the same number of elements and $He = H$, so the corollary follows from Lemma 11.9. □

Theorem 11.11 (Lagrange)**.** *Suppose that G is a finite group and $H \subseteq G$ is a subgroup, then the order of H divides the order of G.*

Proof. Since the relation $\sim$ introduced in Remark 11.7 is an equivalence relation, G is the disjoint union of some equivalence classes $Hg_1, Hg_2, \ldots, Hg_k$. Thus,

$$|G| = \sum_{i=1}^{k} |Hg_i|.$$

As each $|Hg_i| = |H|$ by Corollary 11.10, it follows that the sum is equal to $k|H|$. So, $|G| = k|H|$, as desired. □

Motto 11.12 ($|G| = |H||G/H|$)**.** If $H \subseteq G$ is a subgroup of a finite group, then the number of (right) cosets times the order of H is equal to the order of G. Indeed, in the proof of Theorem 11.11 the number of right cosets is k.

Corollary 11.13 (Lagrange's theorem for elements)**.** *Let G be a finite group and $g \in G$ an element, then $|g|$ divides $|G|$.*

Proof. Let $N = |g|$. Then, the set $\{1, g, g^2, \ldots, g^{N-1}\}$ forms a subgroup of G of order N. By Theorem 11.11, $N = |g|$ divides $|G|$. □

Remark 11.14. The converse does not hold: if G is a finite group and if $N > 1$ divides $|G|$, there need not be an element of G of order N. See Exercise 11.1.

Corollary 11.15. *If G is a finite group and $g \in G$, then $g^{|G|} = e$.*

Proof. Write $|G| = |g|k$. Then, $g^{|G|} = (g^{|g|})^k = e^k = e$. □

11.1 Exercises

Exercise 11.1. The largest order of an element of S_3 is 3. The largest order of an element of S_4 is 4. The largest order of an element of S_5 is **6**! The largest order of an element of S_6 is 6. The largest order of an element of S_7 is **12**! What are the largest orders of elements in S_8, S_9, and S_{10}? (Recall our previous work on the order of elements of symmetric groups in terms of their cycle decompositions.)

Exercise 11.2. Prove that if G is a finite group of order p, where p is a prime, then $G \cong \mathbf{Z}/p$.

Exercise 11.3. Prove that if $N \geqslant 1$ and $a \in (\mathbf{Z}/N)^\times$, then $a^{\phi(N)} \equiv 1 \mod N$, where ϕ is Euler's totient function.

Exercise 11.4 (Fermat's little theorem)**.** Prove that if p is a prime, then $a^p \equiv a \mod p$ for any $a \in \mathbf{Z}$.