Section II.10. Cosets and the Theorem of Lagrange

Note. In this section, we prove that the order of a subgroup of a given finite group divides the order of the group. This is called Lagrange's Theorem. The proof involves partitioning the group into sets called *cosets*. Later, we will form a group using the cosets, called a *factor group* (see Section 14).

Theorem 10.1. Let H be a subgroup of group G. Let the relation $\sim_L$ be defined on G by

$$a \sim_L b \text{ iff } a^{-1}b \in H.$$

Let the relation $\sim_R$ be defined by

$$a \sim_R b \text{ iff } ab^{-1} \in H.$$

Then $\sim_L$ and $\sim_R$ are both equivalence relations on G.

Definition 10.2. Let H be a subgroup of a group G. The subset $aH = \{ah \mid h \in H\}$ of G is the *left coset* of H containing a. The subset $Ha = \{ha \mid h \in H\}$ is the *right coset* of H containing a.

Note. Suppose $x, y \in aH$. Then $x = ah_1$ and $y = ah_2$ for some $h_1, h_2 \in H$. So $h_1 = a^{-1}x$ and $h_2 = a^{-1}y$. So $a \sim_L x$ and $a \sim_L y$. Therefore, $x \sim_L y$. Now $e \in H$ since H is a group, so $a = ae \in aH$. Equivalently, $a^{-1}a = e \in H$, so $a \sim_L a$. So the coset aH is actually the $\sim_L$ equivalence class of elements of G which contains a. Similarly, Ha is the $\sim_R$ equivalence class of elements of G which contains a.

Exercise 10.4. Find the cosets of the subgroup $\langle 4 \rangle$ of $\mathbb{Z}_{12}$.

Solution. First, $\langle 4 \rangle = \{0, 4, 8\}$ and $\mathbb{Z}_{12}$ is an additive group. So we get the cosets:

$$0 + \langle 4 \rangle = \{0, 4, 8\} = \langle 4 \rangle + 0$$

$$1 + \langle 4 \rangle = \{1, 5, 9\} = \langle 4 \rangle + 1$$

$$2 + \langle 4 \rangle = \{2, 6, 10\} = \langle 4 \rangle + 2$$

$$3 + \langle 4 \rangle = \{3, 7, 11\} = \langle 4 \rangle + 3.$$

Now we get repetitions:

$$4 + \langle 4 \rangle = \langle 4 \rangle + 4 = 8 + \langle 4 \rangle = \langle 4 \rangle + 8 = \langle 4 \rangle$$

$$5 + \langle 4 \rangle = \langle 4 \rangle + 5 = 9 + \langle 4 \rangle = \langle 4 \rangle + 9 = \langle 4 \rangle + 1$$

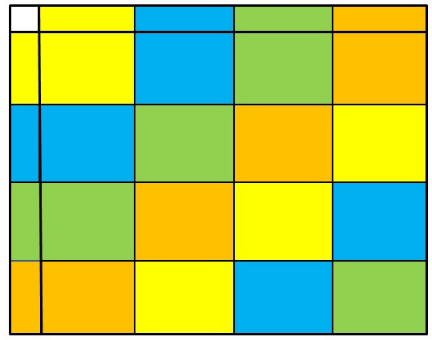
$$6 + \langle 4 \rangle = \langle 4 \rangle + 6 = 10 + \langle 4 \rangle = \langle 4 \rangle + 10 = \langle 4 \rangle + 2$$

$$7 + \langle 4 \rangle = \langle 4 \rangle + 7 = 11 + \langle 4 \rangle = \langle 4 \rangle + 11 = \langle 4 \rangle + 3.$$

So the distinct cosets are $\{0, 4, 8\}$, $\{1, 5, 9\}$, $\{2, 6, 10\}$, and $\{3, 7, 11\}$. Notice that the cosets do in fact partition $\mathbb{Z}_{12}$. Also, the respective left and right cosets are equal because $\mathbb{Z}_{12}$ is abelian. The partition can be illustrated in the Cayley table as follows:

	0	4	8	1	5	9	2	6	10	3	7	11
0	0	4	8	1	5	9	2	6	10	3	7	11
4	4	8	0	5	9	1	6	10	2	7	11	3
8	8	0	4	9	1	5	10	2	6	11	3	7
1	1	5	9	2	6	10	3	7	11	4	8	0
5	5	9	1	6	10	2	7	11	3	8	0	4
9	9	1	5	10	2	6	11	3	7	0	4	8
2	2	6	10	3	7	11	4	8	0	5	9	1
6	6	10	2	7	11	3	8	0	4	9	1	5
10	10	2	6	11	3	7	0	4	8	1	5	9
3	3	7	11	4	8	0	5	9	1	6	10	2
7	7	11	3	8	0	4	9	1	5	10	2	6
11	11	3	7	0	4	8	1	5	9	2	6	10

Notice that the colors in this table hint at a group themselves:



In fact, this is the group structure of $\mathbb{Z}_4$.

Example 10.7. We now find left and right cosets for a nonabelian group. Consider the group S_3 and subgroup $H = \{\rho_0, \mu_1\}$. Find the left and right cosets of H and give a color coded Cayley table as above.

Solution. The Cayley table for S_3 is

	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

The left cosets are:

$$\rho_0 H = \mu_1 H = \{\rho_0, \mu_1\}$$

$$\rho_1 H = \mu_3 H = \{\rho_1, \mu_3\}$$

$$\rho_2 H = \mu_2 H = \{\rho_2, \mu_2\}.$$

The right cosets are:

$$H\rho_0 = H\mu_1 = \{\rho_0, \mu_1\}$$

$$H\rho_1 = H\mu_2 = \{\rho_1, \mu_2\}$$

$$H\rho_2 = H\mu_3 = \{\rho_2, \mu_3\}.$$

Notice that the left cosets and right cosets yield different partitions of S_3. We get the Cayley table with the left cosets as:

	ρ_0	μ_1	ρ_1	μ_3	ρ_2	μ_2
ρ_0	ρ_0	μ_1	ρ_1	μ_3	ρ_2	μ_2
μ_1	μ_1	ρ_0	μ_2	ρ_2	μ_3	ρ_1
ρ_1	ρ_1	μ_3	ρ_2	μ_2	ρ_0	μ_1
μ_3	μ_3	ρ_1	μ_1	ρ_0	μ_2	ρ_2
ρ_2	ρ_2	μ_2	ρ_0	μ_1	ρ_1	μ_3
μ_2	μ_2	ρ_2	μ_3	ρ_1	μ_1	ρ_0

For the right cosets, the Cayley table is:

	ρ_0	μ_1	ρ_1	μ_2	ρ_2	μ_3
ρ_0	ρ_0	μ_1	ρ_1	μ_2	ρ_2	μ_3
μ_1	μ_1	ρ_0	μ_2	ρ_1	μ_3	ρ_2
ρ_1	ρ_1	μ_3	ρ_2	μ_1	ρ_0	μ_2
μ_2	μ_2	ρ_2	μ_3	ρ_0	μ_1	ρ_1
ρ_2	ρ_2	μ_2	ρ_0	μ_3	ρ_1	μ_1
μ_3	μ_3	ρ_1	μ_1	ρ_2	μ_2	ρ_0

Notice that in neither of the above two Cayley tables do we have the same type of group structure as we did in the case of $\mathbb{Z}_{12}$. Details will follow in Section 14 (where we will see that a group can be made from the cosets when the left coset partition and the right coset partition are the same).

Lemma. Consider group G with subgroup H. Then every left coset of H and every right coset of H have the same cardinality, namely $|H|$. That is, for any coset g_1H or Hg_2, there are one-to-one and onto mappings ϕ_1 and ϕ_2 such that $\phi_1 : H \to g_1H$ and $\phi_2 : H \to Hg_2$.

Theorem 10.10. Theorem of Lagrange ("Lagrange's Theorem").
Let H be a subgroup of a finite group G. Then the order of H is a divisor of the order of G.

Note. The text comments "*Never underestimate results that count something!*" (their emphasis). We'll use the Theorem of Lagrange to look for subgroups of given groups—it tells us the possible orders of subgroups.

Note. Lagrange's Theorem guarantees that the order of a subgroup divides the order of a a group. However, the converse does not hold. That is, if $|G| = n$ and $m \mid n$, then there is not necessarily a subgroup of G of order m. For example, the alternating group A_4 (of order $4!/2 = 12$) does not have a subgroup of order 6—this will be shown in Example 15.6 on page 146.

Corollary 10.11. Every group of prime order is cyclic.

Note. In the proof of Corollary 10.11, a could be *any* element of G other than the identity. So a group of prime order is cyclic and any non-identity element of the group is a generator.

Note. By Theorem 6.10, we know that any cyclic group of order n is isomorphic to $\mathbb{Z}_n$. So we can use Corollary 10.11 to say: "If p is a prime, then there is, up to isomorphism, only one group of order p, namely $\mathbb{Z}_p$."

Theorem 10.12. The order of an element of a finite group divides the order of the group.

Definition 10.13. Let H be a subgroup of group G. The number of left cosets of H in G (technically, the cardinality of the set of left cosets) is the *index* of H in G, denoted $(G : H)$.

Note. For finite group G, $(G : H) = |G|/|H|$.

Note. Since the cardinality of a left coset of H is the same as the cardinality of a right coset of H, then $(G : H)$ can also be defined as the "number" of right cosets of H in G. Exercise 10.35 has you give the details for this claim. The proof of the next theorem is to be given in Exercise 10.38.

Theorem 10.14. Suppose H and K are subgroups of group G where $K \leq H \leq G$. Suppose $(H : K)$ and $(G : H)$ are finite. Then $(G : K)$ is finite and

$$(G : K) = (G : H)(H : K).$$

Revised: 7/6/2023