

CONTENTS

1. Recollections: cosets form a partition.....	1
2. Example: cosets of $8\mathbb{Z}$	1
3. G/H and Lagrange's theorem.....	2

1. RECOLLECTIONS: COSETS FORM A PARTITION

Last time we introduced the notion of left and right cosets of a group. These were defined as follows: given a group G and a subgroup $H \leq G$, a left coset is a set of the form

$$gH = \{gh \mid h \in H\} \quad \text{for some fixed } g \in G \quad (1.1)$$

and a right coset is one of the form

$$Hg = \{hg \mid h \in H\} \quad \text{for some fixed } g \in G. \quad (1.2)$$

We ended last class by proving the following result:

Lemma 1.1 (Equality of cosets). *Let $H \leq G$ and $g_1, g_2 \in G$. The following are equivalent:*

- (1) $g_1H \cap g_2H \neq \emptyset$;
- (2) $g_1H = g_2H$;
- (3) $g_2^{-1}g_1 \in H$;
- (4) $g_1^{-1}g_2 \in H$.

Recall the following definition:

Definition 1.1 (Partition). A *partition* of a set X is a collection of nonempty subsets $\{X_\alpha\}_{\alpha \in I}$ such that

$$X = \bigcup_{\alpha \in I} X_\alpha, \quad X_\alpha \cap X_\beta = \emptyset \quad (\alpha \neq \beta).$$

We write $X = \bigsqcup_{\alpha \in I} X_\alpha$.

Now, we can prove the basic fact:

Proposition 1.1. *The distinct left cosets of H form a partition of G .*

Proof. Every $g \in G$ belongs to gH , since $g = ge_G$ and $e_G \in H$. Thus the cosets are nonempty and cover G . By Lemma 1.1, two cosets that intersect are equal, so distinct cosets are disjoint. $\square$

2. EXAMPLE: COSETS OF $8\mathbb{Z}$

In the additive group $G = \mathbb{Z}$, take $H = 8\mathbb{Z}$. Cosets are written additively:

$$a + 8\mathbb{Z} = \{a + 8k : k \in \mathbb{Z}\}. \quad (2.1)$$

For instance,

$$\begin{aligned} 0 + 8\mathbb{Z} &= \{\dots, -16, -8, 0, 8, 16, \dots\}, \\ 1 + 8\mathbb{Z} &= \{\dots, -15, -7, 1, 9, 17, \dots\}, \\ 7 + 8\mathbb{Z} &= \{\dots, -9, -1, 7, 15, 23, \dots\}. \end{aligned}$$

Arranging the integers by their remainders gives eight disjoint columns:

remainder	0	1	2	3	4	5	6	7
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
	16	17	18	19	20	21	22	23
	8	9	10	11	12	13	14	15
	0	1	2	3	4	5	6	7
	-8	-7	-6	-5	-4	-3	-2	-1
	-16	-15	-14	-13	-12	-11	-10	-9
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Each column is one coset. The equality criterion becomes

$$a + 8\mathbb{Z} = b + 8\mathbb{Z} \iff a - b \in 8\mathbb{Z} \iff a \equiv b \pmod{8}. \quad (2.2)$$

For example, $0 + 8\mathbb{Z} = 8 + 8\mathbb{Z}$ and $1 + 8\mathbb{Z} = 17 + 8\mathbb{Z}$. Every integer has exactly one remainder in $\{0, 1, \dots, 7\}$, so

$$\mathbb{Z} = \bigsqcup_{r=0}^7 (r + 8\mathbb{Z}), \quad \mathbb{Z}/8\mathbb{Z} = \{0 + 8\mathbb{Z}, 1 + 8\mathbb{Z}, \dots, 7 + 8\mathbb{Z}\}.$$

Writing $\bar{a} = a + 8\mathbb{Z}$, we may abbreviate this as

$$\mathbb{Z}/8\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \bar{7}\}.$$

Thus an infinite group can have a finite set of cosets.

3. G/H AND LAGRANGE'S THEOREM

For a subgroup $H \leq G$, recall that

Definition 3.1. We write G/H for the set of left cosets of G . So every element of G/H is a coset of the form gH , and we often denote this as $\bar{g}$. Note that we are only recording the *distinct* left cosets here, and it could very well be that $g_1H = g_2H$, i.e. $\bar{g}_1 = \bar{g}_2$.^a If $R \subseteq G$ contains exactly one representative of each left coset, the precise formulas are

$$G/H = \{rH : r \in R\}, \quad G = \bigsqcup_{r \in R} rH. \quad (3.1)$$

^aFrom our Lemma above, this happens whenever $g_1^{-1}g_2 \in H$ or $g_2^{-1}g_1 \in H$.

One of the first questions we can ask is: how big is G/H ? The answer is recorded in a quantity called the index of H in G .

Definition 3.2 (Index). The *index* of a subgroup H in G , denoted $[G : H]$, is the number of distinct left cosets:

$$[G : H] = |G/H|.$$

The index may be infinite.

Example 3.1 (Indices in S_3 and $\mathbb{Z}$).

(a) *Subgroups of S_3 .* As in Lecture 10, write $S_3 = \{1, x, x^2, y, xy, x^2y\}$ with $x^3 = 1$, $y^2 = 1$, $yx = x^2y$.

- For $N = \{1, x, x^2\}$ we found $S_3/N = \{N, yN\}$, so $[S_3 : N] = 2$.
- For $H = \{1, y\}$ we found $S_3/H = \{H, xH, x^2H\}$, so $[S_3 : H] = 3$.
- For the trivial subgroup $I = \{1\}$, each coset $gI = \{g\}$ is a single element, and distinct elements give distinct cosets. Thus $S_3/I = \{\{g\} : g \in S_3\}$ and $[S_3 : I] = 6$.
- At the other extreme, $gS_3 = S_3$ for every g , so $[S_3 : S_3] = 1$.

In each case $|S_3| = 6$ equals $[S_3 : K] \cdot |K|$:

$$6 = 2 \cdot 3 = 3 \cdot 2 = 6 \cdot 1 = 1 \cdot 6.$$

(b) *The subgroups $n\mathbb{Z} \leq \mathbb{Z}$.* Let $n \geq 1$. By the division algorithm, every $a \in \mathbb{Z}$ can be written $a = qn + r$ with $0 \leq r < n$, so $a - r \in n\mathbb{Z}$ and $a + n\mathbb{Z} = r + n\mathbb{Z}$. Hence every coset is one of

$$0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \dots, (n-1) + n\mathbb{Z}.$$

These are distinct: if $0 \leq r < s < n$, then $0 < s - r < n$, so $s - r \notin n\mathbb{Z}$ and $r + n\mathbb{Z} \neq s + n\mathbb{Z}$. Therefore

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}, \quad [\mathbb{Z} : n\mathbb{Z}] = n.$$

The case $n = 8$ is the table in Section 2. Although $\mathbb{Z}$ and $n\mathbb{Z}$ are both infinite, the index is finite.

For $n = 0$, the subgroup is $0\mathbb{Z} = \{0\}$, each coset $a + 0\mathbb{Z} = \{a\}$ is a single integer, and $[\mathbb{Z} : 0\mathbb{Z}]$ is infinite.

Theorem 3.1 (Lagrange). *If G is finite and $H \leq G$, then*

$$|G| = [G : H] |H|. \quad (3.2)$$

In particular, $|H|$ divides $|G|$.

Proof. Choose one representative of each left coset, say $g_1, \dots, g_m$, where $m = [G : H]$. The cosets partition G and each has $|H|$ elements. Indeed, as we observed earlier, for every subgroup $H \leq G$ and every $g \in G$, the map

$$H \longrightarrow gH, \quad h \longmapsto gh,$$

is a bijection. Why? It is surjective by the definition of gH . If $gh_1 = gh_2$, cancellation gives $h_1 = h_2$, so it is injective. Its inverse sends $z \in gH$ to $g^{-1}z \in H$. From this, we then conclude:

$$G = \bigsqcup_{i=1}^m g_i H, \quad |G| = \sum_{i=1}^m |g_i H| = m|H|.$$

□

Corollary 3.1. *If G is finite and $a \in G$, then the order of a divides $|G|$.*

Proof. Apply Lagrange's theorem to the cyclic subgroup $\langle a \rangle$, whose cardinality is the order of a . □

Corollary 3.2. *Every group of prime order p is cyclic, hence isomorphic to the cyclic group C_p of order p .*

Proof. Choose $a \neq e_G$. Its order divides p , so it is either 1 or p . It cannot be 1, and hence $|\langle a \rangle| = p = |G|$. Therefore $G = \langle a \rangle$. □