

§10 Lagrange's Theorem

The order of any subgroup of U in Example 9.4(h) divides the order of U . The same thing is true for the group E in Example 9.4(i). Likewise, the reader verified that the order of L in §9, Ex.4 is divisible by the order of any subgroup of L . These are special instances of a general theorem named after J. L. Lagrange (1736-1813), which asserts that the order of a subgroup divides the order of a group, provided, of course, the group has finite order so that we can meaningfully speak about divisibility. It is the first important theorem of group theory that we come across.

The proof of Lagrange's theorem requires the notion of cosets, which plays an important role in group theory.

10.1 Definition: Let G be a group, $H \leq G$ and $a \in G$. We put

$$Ha := \{ha \in G : h \in H\} \subseteq G$$

and call Ha a *right coset of H in G* . We put

$$aH := \{ah \in G : h \in H\} \subseteq G$$

and call aH a *left coset of H in G* .

Right and left cosets of H are subsets of G . When the group is written additively, we write $H + a = \{h + a \in G : h \in H\}$ and $a + H = \{a + h \in G : h \in H\}$ for the right and left cosets of H . A right coset is not necessarily a left coset and a left coset is not necessarily a right coset. However, when the group is commutative, the right and left cosets coincide, as is evident from the definition. During a particular discussion, we usually fix a subgroup H of a group G and consider its various (right or left) cosets. Then we refer to Ha as the *right coset of $a \in G$* , or as the *right coset of H determined by a* . We use similar expressions for aH .

Cosets are subsets of a group, so the equality of two cosets is defined by mutual inclusion. We ask when two cosets are equal. The next lemma gives an answer.

10.2 Lemma: *Let G be a group, $H \leq G$ and $a, b \in G$.*

- (1) *The right coset $H1 =$ the subgroup $H =$ the left coset $1H$.*
- (2) *$Ha = H$ if and only if $a \in H$; $aH = H$ if and only if $a \in H$.*
- (3) *$Ha = Hb$ if and only if $a = hb$ for some $h \in H$; $aH = bH$ if and only if $a = bh$ for some $h \in H$.*
- (4) *$Ha = Hb$ if and only if $a \in Hb$; $aH = bH$ if and only if $a \in bH$.*
- (5) *$Ha = Hb$ if and only if $ab^{-1} \in H$; $aH = bH$ if and only if $a^{-1}b \in H$.*
- (6) *$Ha = Hb$ if and only if $Hab^{-1} = H$; $aH = bH$ if and only if $a^{-1}bH = H$.*

Proof: We prove only the assertions for right cosets and leave the discussion of left cosets to the reader.

- (1) From the definition of $H1$ and 1 , we get

$$H1 = \{h1 \in G: h \in H\} = \{h \in G: h \in H\} = H.$$

- (2) If $Ha = H$, then $a = 1a \in \{ha \in G: h \in H\} = Ha = H$, so $a \in H$. Conversely, if $a \in H$, then

$$\begin{array}{lll} a \in H & \text{and} & a^{-1} \in H, \\ ha \in H & \text{and} & ha^{-1} \in H \text{ for any } h \in H, \text{ since } H \\ & & \text{is closed under multiplication),} \\ ha \in H & \text{and} & h = (ha^{-1})a \in Ha \text{ for all } h \in H, \\ Ha \subseteq H & \text{and} & H \subseteq Ha, \end{array}$$

so $Ha = H$.

- (3) If $Ha = Hb$, then $a \in Ha = Hb$, so $a = hb$ for some $h \in H$. Conversely, assume $a = hb$, where $h \in H$. Then

$$\begin{array}{lll} a = hb & \text{and} & b = h^{-1}a, \\ h'a = h'hb \in Hb & \text{and} & h'b = h'h^{-1}a \in Ha \text{ for all } h' \in H, \\ Ha \subseteq Hb & \text{and} & Hb \subseteq Ha, \end{array}$$

so $Ha = Hb$.

- (4) This is just a reformulation of (3).

(5) $Ha = Hb$ if and only if $a = hb$ for some $h \in H$, and there is a unique h with $a = hb$, namely $h = ab^{-1}$ (Lemma 7.5(2)); thus $a = hb$ for some $h \in H$ if and only if $ab^{-1} \in H$.

(6) $Ha = Hb$ if and only if $ab^{-1} \in H$ by (5), and $ab^{-1} \in H$ if and only if $Hab^{-1} = H$ by (2).

10.3 Lemma: *Let $H \leq G$. Then G is the union of the right cosets of H . The right cosets of H are mutually disjoint. Analogous statements hold for left cosets.*

Proof: As $Ha \subseteq G$ for any $a \in G$, we get $\bigcup_{a \in G} Ha \subseteq G$. Also, for any $g \in G$, we have $g \in Hg$, so $g \in \bigcup_{a \in G} Ha$, thus $G \subseteq \bigcup_{a \in G} Ha$. This proves $G = \bigcup_{a \in G} Ha$.

Now we prove that the right cosets of H are mutually disjoint. Assume $Ha \cap Hb \neq \emptyset$. We are to show $Ha = Hb$. Well, we take $c \in Ha \cap Hb$ if $Ha \cap Hb \neq \emptyset$. Then $c \in Ha$ and $c \in Hb$. So $Ha = Hc$ and $Hc = Hb$ by Lemma 10.2(4). We obtain $Ha = Hb$.

The left cosets are treated similarly. □

In the terminology of Theorem 2.5, right cosets of H form a partition of G . Theorem 2.5 tells us that the right cosets are the equivalence classes of a certain equivalence relation on G . By the proof of Theorem 2.5, we see that this equivalence relation \sim is given by

$$\text{for all } a, b \in G: a \sim b \text{ if and only if } Ha = Hb,$$

which we can read as

$$\text{for all } a, b \in G: a \sim b \text{ if and only if } ab^{-1} \in H.$$

It may be worth while to obtain Lemma 10.3 from this relation \sim , instead of obtaining the relation \sim from Lemma 10.3.

10.4 Definition: Let $H \leq G$ and $a, b \in G$. We write $a \equiv_r b \pmod{H}$ and say a is right congruent to b modulo H if $ab^{-1} \in H$. Similarly, we write $a \equiv_l b \pmod{H}$ and say a is left congruent to b modulo H if $a^{-1}b \in H$.

10.5 Lemma: *Let $H \leq G$. Right congruence modulo H and left congruence modulo H are equivalence relations on G .*

Proof: We give the proof for right congruence only. We check that it is reflexive, symmetric and transitive.

(i) For all $a \in G$, $a \equiv_r a \pmod{H}$, as this means $aa^{-1} = 1 \in H$. So right congruence is reflexive. Reflexivity of right congruence follows from the fact that $1 \in H$.

(ii) If $a \equiv_r b \pmod{H}$, then $ab^{-1} \in H$, then $(ab^{-1})^{-1} \in H$, hence $ba^{-1} \in H$ and $b \equiv_r a \pmod{H}$. So right congruence is symmetric. Symmetry of right congruence follows from the fact that H is closed under the forming of inverses.

(iii) If $a \equiv_r b \pmod{H}$ and $b \equiv_r c \pmod{H}$, then $ab^{-1} \in H$ and $bc^{-1} \in H$, then $(ab^{-1})(bc^{-1}) \in H$, hence $ac^{-1} \in H$ and $a \equiv_r c \pmod{H}$. So right congruence is transitive. Transitivity of right congruence follows from the fact that H is closed under multiplication.

Hence right congruence is an equivalence relation on G . □

According to Theorem 2.5, G is the disjoint union of right congruence classes. The right congruence class of $a \in G$ is the right coset of a :

$$\begin{aligned}
 [a] &= \{x \in G: x \equiv_r a \pmod{H}\} \\
 &= \{x \in G: xa^{-1} \in H\} \\
 &= \{x \in G: xa^{-1} = h, \text{ where } h \in H\} \\
 &= \{x \in G: x = ha, \text{ where } h \in H\} \\
 &= \{ha \in G: h \in H\} \\
 &= Ha.
 \end{aligned}$$

This gives a new proof of Lemma 10.3.

10.6 Lemma: *Let $H \leq G$. There are as many distinct right cosets of H in G as there are distinct left cosets of H in G . More precisely, let \mathcal{R} be the set of right cosets of H in G and let \mathcal{L} be the set of left cosets of H in G . Then \mathcal{R} and \mathcal{L} have the same cardinality: $|\mathcal{R}| = |\mathcal{L}|$.*

Proof: We must find a one-to-one correspondence between \mathcal{R} and \mathcal{L} .

We put

$$\begin{aligned}\sigma: \mathcal{R} &\rightarrow \mathcal{L} \\ Ha &\rightarrow a^{-1}H.\end{aligned}$$

We show that σ is a one-to-one, onto mapping. First we prove it is a mapping. We have to do it. Indeed, how do we find $X\sigma$ if $X \in \mathcal{R}$? Well, we write $X = Ha$, that is, we choose an $a \in X$, then we find the inverse of this a , and "map" $X = Ha$ to the left coset $a^{-1}H$ of H determined by a^{-1} . So we must show that $X\sigma$ is independent of the element a we choose from X , i.e., that σ is a well defined function. We are to prove

$$Ha = Hb \implies (Ha)\sigma = (Hb)\sigma.$$

If $Ha = Hb$, then $ab^{-1} \in H$ by Lemma 10.2(5), then $(ab^{-1})^{-1} \in H$, so $ba^{-1} \in H$, so $a^{-1}H = b^{-1}H$ by Lemma 10.2(5), and $(Ha)\sigma = (Hb)\sigma$. Hence σ is indeed a well defined function.

σ is one-to-one since $(Ha)\sigma = (Hb)\sigma \implies a^{-1}H = b^{-1}H \implies (b^{-1})^{-1}a^{-1} \in H \implies ba^{-1} \in H \implies (ba^{-1})^{-1} \in H \implies ab^{-1} \in H \implies Ha = Hb$, and σ is onto as well, since any $bH \in \mathcal{L}$ is the image of $Hb^{-1} \in \mathcal{R}$ under σ :

$$(Hb^{-1})\sigma = (b^{-1})^{-1}H = bH.$$

Hence $|\mathcal{R}| = |\mathcal{L}|$. □

10.7 Definition: Let G be a group and $H \leq G$. The (cardinal) number of distinct right cosets of H in G , which is also the (cardinal) number of distinct left cosets of H in G , is called the *index of H in G* , and is denoted by $|G:H|$.

So $|G:H|$ is a natural number or $|G:H| = \infty$. Notice that G is written before H in $|G:H|$, but when we read, " H " is pronounced before " G ": index of H in G . Lemma 10.6 states essentially that we do not have to distinguish between "right" and "left" index.

Note that $|G:H| = 1$ means $H = H1$ is the only right coset of H in G , whence $a \in Ha = H$ for all $a \in G$ and so $G \subseteq H$. Thus $|G:H| = 1$ if and only if $H = G$.

We will be mostly interested in cases where $|G:H|$ is finite. This can happen even if $|G|$ is infinite. For instance, $4\mathbb{Z}$ is a subgroup of \mathbb{Z} (under addition) by Example 9.4(c) and the left (right) cosets

$$0 + 4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z}$$

of $4\mathbb{Z}$ in \mathbb{Z} are all the left cosets of $4\mathbb{Z}$ in \mathbb{Z} . Hence $|\mathbb{Z} : 4\mathbb{Z}| = 4$. Incidentally, we see that Definition 10.4 is a natural generalization of the congruence relation on \mathbb{Z} .

We need one more lemma for the proof of Lagrange's theorem.

10.8 Lemma: *Let G be a group and $H \leq G$. Any right coset of H and any left coset of H in G have the same (cardinal) number of elements as H . In fact, $|Ha| = |aH| = |H|$ for all $a \in G$.*

Proof: We prove the lemma for right cosets only. For any $a \in G$, we must find a one-to-one correspondence between H and Ha . What is more natural than the mapping

$$\begin{aligned} \varphi: H &\rightarrow Ha \\ h &\rightarrow ha \end{aligned}$$

from H into Ha ? Now φ is indeed a mapping H into Ha . It is one-to-one, for $h\varphi = h'\varphi$ ($h, h' \in H$) implies $ha = h'a$, which gives $h = h'$ after cancelling a (Lemma 8.1(2)). Also, it is onto by the very definition of Ha . So we get $|Ha| = |H|$. \square

10.9 Theorem (Lagrange's theorem): *If $H \leq G$, then $|G| = |G:H||H|$. In particular, if G is a finite group, then $|H| \mid |G|$.*

Proof: From Lemma 10.3, we know $G = \bigcup_{a \in G} Ha$ and that the Ha are mutually disjoint. Avoiding redundancies, we write

$$G = \bigcup_{Ha \in \mathcal{R}} Ha,$$

where \mathcal{R} is the set of distinct right cosets of H in G . Since Ha are disjoint, we obtain

$$|G| = \sum_{Ha \in \mathcal{R}} |Ha|$$

when we count the elements. Since $|Ha| = |H|$ for all $Ha \in \mathcal{R}$ by Lemma 10.8, we get

$$|G| = \sum_{Ha \in \mathcal{R}} |Ha| = \sum_{Ha \in \mathcal{R}} |H| = |\mathcal{R}| |H| = |G:H| |H|$$

as $|G:H| = |\mathcal{R}|$ by Definition 10.7. \square

The basic idea of the preceding proof is simple. We have a disjoint union $G = \bigcup_{Ha \in \mathcal{R}} Ha$ and we count the elements. Then we get $|G| = \sum_{Ha \in \mathcal{R}} |Ha|$. In

the sequel, we will prove some important results by a similar reasoning. We will have a disjoint union $S = \bigcup_{i \in I} T_i$ and, counting the elements, we will get $|S| = \sum_{i \in I} |T_i|$. See §§25,26.

Here is an application of Lagrange's theorem.

10.10 Theorem: *Let p be a positive prime number and G be a group of order p . Then G has no nontrivial proper subgroup.*

Proof: We are to show that $\{1\}$ and G are the only subgroups of G . Now if $H \leq G$, then $|H| \mid |G|$ by Lagrange's theorem, so $|H| \mid p$ and $|H| = 1$ or p . If $|H| = 1$, then necessarily $H = \{1\}$. If $|H| = p$, then $|H| = |G|$ and $H \leq G$ together yield $H = G$. \square

If G is a finite group and $K \leq H \leq G$, Lagrange's theorem gives

$$|G:H| = \frac{|G|}{|H|}, |H:K| = \frac{|H|}{|K|}, \text{ so } |G:H||H:K| = \frac{|G|}{|H|} \frac{|H|}{|K|} = \frac{|G|}{|K|} = |G:K|.$$

We give another proof of this result which works also in the case of infinite groups and infinite indices.

10.11 Theorem: *If $K \leq H \leq G$, then $|G:H||H:K| = |G:K|$. In particular, if any two of $|G:H|, |G:K|, |H:K|$ is finite, then the third is finite, too.*

Proof: Let $\mathcal{R} = \{Ha_i : i \in I\}$ be the set of all distinct right cosets of H in G . We have

$$G = \bigcup_{i \in I} Ha_i, \text{ with } a_i \in G, Ha_i \neq Ha_{i_1} \text{ for } i \neq i_1, |I| = |G:H|. \quad (1)$$

Let $\mathcal{R}' = \{Kb_j : j \in J\}$ be the set of all distinct right cosets of K in H . Then

$$H = \bigcup_{j \in J} Kb_j, \text{ with } b_j \in H, Kb_j \neq Kb_{j_1} \text{ for } j \neq j_1, |J| = |H:K|. \quad (2)$$

We must prove $|G:K| = |I||J|$. Since $|I \times J| = |I||J|$, this will be accomplished if we can find a one-to-one correspondence between $I \times J$ and the set of right cosets of K in G . How we find this correspondence will be clear when we observe

$$\begin{aligned} Ha_i &= \{ha_i \in G: h \in H\} = \{ha_i \in G: h \in \bigcup_{j \in J} Kb_j\} \\ &= \{ha_i \in G: \text{there are } j \in J \text{ and } k \in K \text{ with } h = kb_j\} \\ &= \{kb_j a_i \in G: j \in J, k \in K\} \\ &= \bigcup_{j \in J} \{kb_j a_i \in G: k \in K\} = \bigcup_{j \in J} Kb_j a_i, \end{aligned}$$

so that $G = \bigcup_{i \in I} Ha_i = \bigcup_{i \in I} \bigcup_{j \in J} Kb_j a_i = \bigcup_{(i,j) \in I \times J} Kb_j a_i$. This suggests

$$(i,j) \rightarrow Kb_j a_i$$

as a mapping from $I \times J$ into the set of right cosets of K in G . Let us check if it works.

For each $(i,j) \in I \times J$, $b_j a_i$ is an element of G , hence $Kb_j a_i$ is a right coset of K in G . Thus the above correspondence is indeed a mapping from $I \times J$ into the set of right cosets of K in G .

It is onto, for if Kg ($g \in G$) is any right coset of K in G , then

$g \in \bigcup_{(i,j) \in I \times J} Kb_j a_i$ by our observation, so, by the definition of union, there is $(i_0 j_0) \in I \times J$ with $g \in Kb_{j_0} a_{i_0}$. Then $Kg = Kb_{j_0} a_{i_0}$ and Kg is the image of $(i_0 j_0) \in I \times J$.

It is one-to-one: if $Kb_j a_i = Kb_{j_1} a_{i_1}$, then $b_j a_i = kb_{j_1} a_{i_1}$ for some $k \in K \subseteq H$ by Lemma 10.2(3), then $a_i = b_j^{-1} kb_{j_1} a_{i_1}$ with $b_j^{-1} kb_{j_1} \in H$, so $Ha_i = Ha_{i_1}$ by Lemma 10.2(3), so $i = i_1$ by (1). Thus $a_i = a_{i_1}$ and we get $Kb_j = Kb_{j_1} a_{i_1} a_i^{-1} = Kb_{j_1} a_{i_1} a_i^{-1} = Kb_{j_1} a_i a_i^{-1} = Kb_{j_1}$ by Lemma 10.2(6), which yields $j = j_1$ by (2). Hence $Kb_j a_i = Kb_{j_1} a_{i_1}$ implies $(i,j) = (i_1 j_1)$. The mapping is one-to-one.

Thus $|G:K| = |I \times J| = |I| |J| = |G:H| |H:K|$. □

Exercises

1. Find the right cosets of all subgroups of U (Example 9.4(h)), of E (Example 9.4(i)) and of L (§9, Ex.4).
2. Let T be the subgroup of $S_{[0,1]}$ that we discussed in Example 9.4(g). Show that $\{\sigma \in S_{[0,1]} : 0\sigma = 1\}$ is a right coset of T in $S_{[0,1]}$. Is it a left coset of T ? Would your answer be different if we wrote the functions on the left? What is $|S_{[0,1]}:T|$?
3. Find all cosets of $n\mathbb{Z}$ in \mathbb{Z} . What is $|\mathbb{Z} : n\mathbb{Z}|$?
4. Why do we not use the "mapping" $\mathcal{R} \rightarrow \mathcal{L}$ in the proof of Lemma 10.6?

$$Ha \rightarrow aH$$