

10. COSETS

In the symmetric group S_n , half the elements are odd and half are even. The even permutations form a subgroup A_n . The odd ones form a subset which is not a subgroup. It is called a *coset* of A_n . The important point is that a coset is a *subset* of a group.

Definition 10.1. *Suppose that H is a subgroup of a group G and $a \in G$. Then*

$$aH := \{ah \mid h \in H\}$$

*is called a **left coset** of H in G and*

$$Ha := \{ha \mid h \in H\}$$

*is called a **right coset** of H in G .*

If the group is additive then the cosets of H in G are

$$a + H = H + a = \{a + h \mid h \in H\}$$

10.1. **examples.** I will give you three examples for now. The first example will show that the same coset can be written in different ways. The second example will show that left cosets and right cosets can be different. The third example shows that infinite cosets also have conceptual meaning.

10.1.1. $G = \mathbb{Z}_4, H = \langle 2 \rangle$. This is an additive group. So, by definition, the cosets of H in G are given by adding⁴ elements of G to H . So, naively, there appear to be four cosets: $0 + H, 1 + H, 2 + H, 3 + H$. But, remember, these are just the *names* of the cosets. Since $H = \{0, 2\}$,

$$1 + H = \{1, 3\}$$

What are the other cosets?

10.1.2. $G = S_3, H = \langle (12) \rangle$. This example will show that the left cosets are not the same sets as the right cosets. There are three left cosets of $H = \{e, (12)\}$ in S_3 :

$$H = \{e, (12)\}, \quad (13)H = \{(13), (123)\}, \quad (23)H = \{(23), (132)\}$$

There are three right cosets:

$$H = \{e, (12)\}, \quad H(13) = \{(13), (132)\}, \quad H(23) = \{(23), (123)\}$$

⁴Note that the book and I are both writing $+$ instead of $+_4$ at this point. It is not as precise but it is standard notation.

So, left and right cosets are different. This picture might help.

$H :$	$e \quad (12)$	$H :$	$e \quad (12)$	$H(23)$				
$(13)H :$	$(13) \quad (123)$	$H(13) :$	<table style="border-collapse: collapse; width: 100%;"> <tr> <td style="border-right: 1px solid black; padding: 5px; text-align: center;">(13)</td> <td style="padding: 5px; text-align: center;">(123)</td> </tr> <tr> <td style="border-right: 1px solid black; padding: 5px; text-align: center;">(132)</td> <td style="padding: 5px; text-align: center;">(23)</td> </tr> </table>	(13)	(123)	(132)	(23)	
(13)	(123)							
(132)	(23)							
$(23)H :$	$(132) \quad (23)$							

Can you explain why this happens? If we take the subgroup $A_3 = \{e, (123), (132)\}$, the left and right cosets are the same. What do you think is the difference?

10.1.3. $G = \mathbb{R}^2$, $H = \text{line}$. If G is the additive group \mathbb{R}^2 then a straight line through the origin is a subgroup. If you choose one nonzero vector v in the line then

$$H = \mathbb{R}v = \{rv \mid r \in \mathbb{R}\}$$

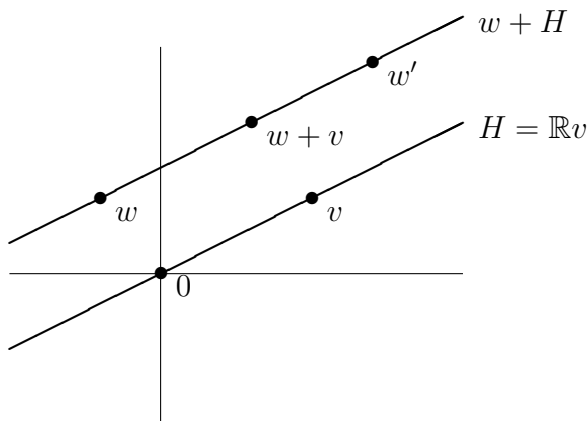
Show that this is an additive subgroup of \mathbb{R}^2 .

The cosets of the line are

$$w + H = w + \mathbb{R}v$$

This is the straight line parallel to H which passes through the point w . If w' any other point in the same line then you get the equation

$$w + H = w' + H.$$



The key point is that parallel lines do not meet unless they are the same line. (A line is parallel to itself.)

10.2. properties of cosets. The main property is that cosets of H do not meet unless they are equal. And two cosets may be equal even though they look different.

10.2.1. *different ways to write the same coset.*

Theorem 10.2. *Two left cosets aH, bH of H in G are equal if and only if $a^{-1}b \in H$. This is also equivalent to the statement $b \in aH$.*

Proof. ($aH = bH \Rightarrow a^{-1}b \in H$) Suppose that $aH = bH$. Then $b = be \in bH$. So, b will also be an element of aH . So, $b = ah$ for some $h \in H$. But, solving for h , we get $h = a^{-1}b \in H$.

($a^{-1}b \in H \Rightarrow aH = bH$) Conversely, if $a^{-1}b \in H$ then we want to show that $aH = bH$. To show this we have to show that each set is contained in the other. So, take any $bh \in bH$. Then

$$bh = a \underbrace{(a^{-1}b)h}_{\in H} \in aH$$

So, $bH \subseteq aH$. Now take any $ah \in aH$. Then $ah = b(a^{-1}b)^{-1}h \in bH$. So, $aH \subseteq bH$ and we conclude that $aH = bH$. \square

This theorem means the following. If C is a left coset of H in G then the possible ways to write C are:

$$C = cH$$

where c is any element of C . In example 10.1.2, The left coset $C = \{(12), (123)\}$ can be written as

$$C = (12)H \quad C = (123)H$$

You take one of the two elements of C and put them next to H on the left.

10.2.2. *different cosets are disjoint.*

Theorem 10.3. *If $aH \neq bH$ then aH, bH are disjoint.*

Proof. If $c \in aH \cap bH$ then $aH = cH = bH$. \square

Another way to say this: If two left cosets overlap then they are equal. Since every element of the group $g \in G$ is contained in the left coset gH , this theorem implies:

Corollary 10.4. *G is divided up (as in the figure in Example 10.1.2) into a disjoint union of left cosets.*

10.2.3. *cosets have the same cardinality.*

Theorem 10.5. *Every left coset aH of H is in 1-1 correspondence with H . In particular, all left cosets have the same number of elements.*

Proof. The correspondence is that $h \in H$ corresponds to $ah \in aH$ and $x \in aH$ corresponds to $a^{-1}x \in H$. \square

10.3. **Lagrange theorem.** If we put this together we get:

Theorem 10.6 (Lagrange). *If H is a subgroup of a finite group G then the order of H divides the order of G and the quotient*

$$|G|/|H|$$

*is equal to the number of left cosets of H in G . This is called the **index** of H in G and denoted $|G : H|$.*

Lagrange's theorem says that the order of a subgroup divides the order of the group. Here are some immediate consequences.

Corollary 10.7. *If $g \in G$ then the order of g divides the order of G .*

Proof. The order of g is equal to the order of the cyclic subgroup $\langle g \rangle$: $|g| = |\langle g \rangle|$ which divides $|G|$ by Lagrange. \square

Corollary 10.8. *If $|G| = n$ then $g^n = e$ for all $g \in e$.*

Proof. The previous corollary said that $n = mk$ if $|g| = m$. Then

$$g^n = g^{mk} = (g^m)^k = e^k = e$$

Or, you can just use the rule that $g^n = e$ iff n is a multiple of $|g|$. \square

Corollary 10.9. *If p is a prime then*

$$x^p \equiv x \pmod{p}$$

for any integer x .

Proof. Here the group is $U(p) = \{1, 2, \dots, p-1\}$ which has order $p-1$. The previous corollary implies that

$$x^{p-1} \equiv 1 \pmod{p}$$

if x is not divisible by p . So, $x^p \equiv x$ in those cases. If $p|x$ then $x^p \equiv 0 \equiv x$. So, the formula also holds in that case. So, it holds in all cases. \square