

MATH 30A: CHAPTER 7

7. COSETS

Cosets are the first concept that students have a lot of trouble with. This may be because the same coset can be written in different way. The same coset has several different *names*. This is confusing but unavoidable. The important point is that a coset is a *subset* of a group.

Definition 7.1. *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

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

7.1. examples. I will give you three examples for now. The first example will show that the same coset can be written in many 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.

7.1.1. $G = \mathbb{Z}_4, H = \langle 2 \rangle$. This is an additive group. So, by definition, the cosets of H in G are given by adding 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. Cosets are subsets of G :

$$0 + H = H = \{0, 2\}$$

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

$$2 + H = \{2, 0\}$$

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

So, there are only two cosets: $H = 0 + H = 2 + H$ and $1 + H = 3 + H$. I will explain the theory after the third example.

Date: October 11, 2006.

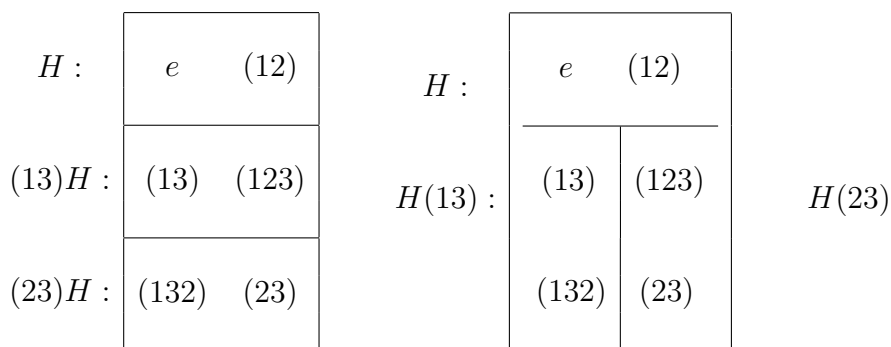
7.1.2. $G = S_3, H = \langle (12) \rangle$. This example will show that the left cosets are not the same sets as the right cosets. There are three left cosets of $H = \{e, (12)\}$ in S_3 :

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

There are three right cosets:

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

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



So, the left cosets are not the same sets as the right cosets.

7.1.3. $G = \mathbb{R}^2, H = \text{line}$. 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

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

and you can see that it is subgroup in one step: $rv - sv = (r - s)v \in H$.

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

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

7.2. properties of cosets. Let's first talk about the question I started with, namely, what are all the different ways to write the same left coset?

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

Theorem 7.2. *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. Suppose that $aH = bH$. Then $e \in H$. So, $b = be \in bH$. If $aH = bH$ then $b \in aH$. So, $b = ah$ for some $h \in H$. But, solving for h , we get $h = a^{-1}b \in H$.

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 $bh = a(a^{-1}b)h \in aH$. 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 7.1.2, 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.

7.2.2. *different cosets are disjoint.*

Theorem 7.3. *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 7.4. *G is divided up (as in the figure in Example 7.1.2) into a disjoint union of left cosets.*

7.2.3. *cosets have the same cardinality.*

Theorem 7.5. *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

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

Theorem 7.6 (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 $|G : H|$.

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

Corollary 7.7. *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 7.8. *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 7.9. *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

7.4. groups of order $2p$. One of the nice theorems of this section is:

Theorem 7.10 (classification of groups of order $2p$). *If $|G| = 2p$ where p is an odd prime then G is either cyclic or dihedral. ($G \cong \mathbb{Z}_{2p}$ or $G \cong D_p$.)*

7.4.1. difference between \mathbb{Z}_{2n} and D_n . At this point we discussed the difference between cyclic and dihedral groups of the same order $2n$. On thing is obvious. \mathbb{Z}_{2n} is abelian while D_n is not (for $n \geq 3$). Other more subtle differences are:

- (1) \mathbb{Z}_{2n} has a unique element of order 2. However, D_n has n or $n + 1$ elements of order 2. The dihedral group has n rotations and n reflections. All reflections have order 2. In addition, if n is even then we have rotation by $\pi = 180^\circ$. This has order 2.
- (2) The center of any abelian group is the whole group. So, $Z(\mathbb{Z}_{2n}) = \mathbb{Z}_{2n}$. The center of the dihedral group has either one or two elements. The identity is in the center and rotation by π is also central if it lies in the group (when n is even).

- (3) The automorphism group of \mathbb{Z}_{2p} is $U(2p)$ which has $p - 1$ elements (all the odd numbers except for p).
- (4) The group D_p has at least $2p$ automorphisms $\phi_g : D_p \rightarrow D_p$ given by conjugation by g :

$$\phi_g(x) = gxg^{-1}$$

This is called the *inner automorphism* given by g . Since D_p has trivial center, the inner automorphisms $\phi_g, g \in D_p$ are all different. (See the lemma below.)

Lemma 7.11. *Two inner automorphisms ϕ_g, ϕ_h of a group G are equal if and only if $h^{-1}g \in Z(G)$. I.e., the left cosets are equal: $gZ(G) = hZ(G)$.*

Remark 7.12. *This implies that the number of different inner automorphisms is equal to the index $|G : Z(G)|$ of the center of G .*

Proof. If $\phi_g(x) = \phi_h(x)$ for all $x \in G$ then

$$gxg^{-1} = hxh^{-1}$$

Multiply both sides on the left by h^{-1} and on the right by g to get:

$$h^{-1}gx = xh^{-1}g$$

In other words $h^{-1}g$ commutes with x for all $x \in G$, i.e., $h^{-1}g \in Z(G)$. \square

7.4.2. *elements of order 2.* We proved the following lemma in class:

Lemma 7.13. *Suppose that G is an abelian group and $a, b \in G$ are elements of order 2. Then $H = \{e, a, b, ab\}$ is a subgroup of G .*

I forgot (or ran out of time) the following lemma:

Lemma 7.14. *Any finite group of even order has an element of order 2.*

Proof. This is one of my favorite proofs. Suppose that G has even order but no elements of order 2. Then there is only one solution of the equation $g^2 = e$, namely $g = e$. But this equation is the same as $g = g^{-1}$. So, there is only one element which is its own inverse. Every other element is paired with its inverse which is different. The pairs taken together have an even number of elements. If there is only one element left over then the total is odd. This is a contradiction. \square

These lemmas together say that:

Theorem 7.15. *Suppose that G is a finite abelian group of even order but $|G|$ is not divisible by 4. Then G has a unique element of order 2.*

Proof. The last lemma says that there is at least one element of order 2. Lemma 7.13 says that if there are two elements a, b then we get a subgroup $H = \{e, a, b, ab\}$ of order 4 which is impossible by Lagrange. So, the number is exactly one. \square

7.4.3. *proof of classification of groups of order $2p$.* Suppose that G is a group of order $2p$. Take any $g \neq e$ in G . Then the possibilities for the order of g are $|g| = 1, 2, p$ or $2p$.

Case 1. g has order $2p$. In this case $G = \langle g \rangle$ is cyclic.

Case 2. All nontrivial elements of G have order 2. In this case G must be abelian and Lemma 7.13 says that G has a subgroup of order 4 which is impossible by Lagrange. So, this case cannot occur.

Case 3. There are no elements of order $2p$ and there is at least one element of order p : call it r . Let $H = \langle r \rangle$. Then H has index 2 in G so $G = H \amalg sH$ for some $s \in G - H$. But I claim that $s^2 = e$. Otherwise, $s^2 = r^k$ generates H and $\langle s \rangle$ contains H and s making $p + 1$ elements. So, $\langle s \rangle = G$ in that case. This is true for every $s \in G - H$.

Now look at srs . This has order p since it is a conjugate of r . So $srs = r^k$ for some k . Then

$$r = ssr = sr^k = (sr^k)s = (sr^k)^2 = r^{k^2}$$

This means $k^2 \equiv 1 \pmod{p}$. This means that p divides $k^2 - 1 = (k - 1)(k + 1)$. But p is prime. So it must divide one of the two factors. So, either $k \equiv 1$ or $k \equiv -1$. In the first case $srs = r$ which means that s, r commute which implies that sr has order $2p$ which is a contradiction. In the second case we have $srs = r^{-1}$ and this holds for every power of r and every element s of $G - H$. So, G is the dihedral group.