Math 417 – Tenth Day

Bruce Reznick
University of Illinois at Urbana-Champaign

September 16, 2020

Notation that is standard and in the book: if H is a subgroup of G, we often write $H \leq G$ or $G \geq H$, with $H < G$ and $G > H$ meaning that H is a subgroup of G and $H \neq G$.

I'd like to return to cosets, in general. There will be examples later. Once again, recall the definition: Suppose H is a subgroup of G and $g \in G$ (not necessarily in H). The left coset gH and the right coset Hg are defined by

$$gH = \{gh \mid h \in H\}, \quad Hg = \{hg \mid h \in H\}.$$

Before we prove some important results about them, I'd like to give an example involving infinite groups that shows we've already been working with cosets.

Consider the group $(\mathbb{Z}, +)$; that is, the integers under addition. We have already seen that this is a group: 0 is the identity $-n$ is the inverse of $n \in \mathbb{Z}$ and ordinary addition is associative. Suppose $d \in \mathbb{N}$, so $d \geq 1$.

Then we saw early on

$$d\mathbb{Z} = \{dn \mid n \in \mathbb{Z}\} = \{\dots, -3d, -2d, -d, 0, d, 2d, 3d, \dots\}$$

is a group with the same identity and inverses, and as strange as it may look, $\mathbb{Z} \geq d\mathbb{Z}$.

What are the cosets of $d\mathbb{Z} \in \mathbb{Z}$? Since the operation is addition, a typical coset is

$$a + d\mathbb{Z} = \{\dots, a - 3d, a - 2d, a - d, a, a + d, a + 2d, a + 3d, \dots\}.$$

We've seen this before: $x \in a + d\mathbb{Z} \iff x \equiv a \mod d$. In other words $a + d\mathbb{Z} = [a]_d$, and these are the cosets of $d\mathbb{Z} \subset \mathbb{Z}$.

LEMMA If $G \geq H$ and H is a finite group, then for every $g \in G$, we have $|H| = |gH| = |Hg|$; that is, every left and right coset has the same number of elements as H.

PROOF Suppose $H = \{h_1, \ldots, h_m\}$. Then $gH = \{gh_1, \ldots, gh_m\}$, so the statement is true provided $h_i \neq h_j \implies gh_i \neq gh_j$.

But the contrapositive of that statement is $gh_i = gh_j \implies h_i = h_j$, which we know to be true upon multiplication of both sides by g^{-1}. The same argument works for Hg. □

The next result is sort of surprising and really important.

THEOREM If $G \geq H$ and xH and yH are two left cosets, then either $xH = yH$ as sets, or xH and yH are disjoint; that is, $xH \cap yH = \emptyset$. Furthermore, $xH = yH$ if and only if $x = yh, y = xh'$ for some $h, h' \in H$. The same thing holds for right cosets, with the last condition changed to $x = hy, y = h'x$.

PROOF. Suppose $z \in xH \cap yH$, so the intersection is not empty. By definition, this means that there exist $h_1, h_2 \in H$ so that

$$z = xh_1 = yh_2 \implies x = yh_2h_1^{-1}.$$

Since H is a subgroup, $h_2h_1^{-1} \in H$. Suppose now that $u \in xH$. Then for some $h \in H$,

$$u = xh = (yh_2h_1^{-1})h = y(h_2h_1^{-1}h)$$

and, again, H is a subgroup, so $h_2h_1^{-1}h \in H$. This implies that $u \in yH$. Thus $xH \subseteq yH$.

But also $y = xh_1h_2^{-1}$, so an almost identical argument shows that $yH \subseteq xH$, and so $xH = yH$.

We have seen that if $x = yh$ or $y = xh'$, then $xH = yH$. The converse is easier: if $xH = yH$, then $x \in xH \implies$ $x \in yH \implies x = yh, y = xh^{-1}$ for some $h \in H$.

The identical argument (up to the order in which you write elements) applies to right cosets. □

COROLLARY If $G \geq H$, then we may write G as a union of disjoint cosets of H.

PROOF Observe that $x \in G$, $e \in H$ (because it's a group) imply that $x = xe \in xH$. Thus, every $x \in G$ belongs to some coset, so

$$G = \bigcup_{x \in G} xH.$$

Delete duplicate cosets, so the remaining ones are disjoint. $\square$.

For example, if, say $d = 3$, then

$$\mathbb{Z} = (0 + 3\mathbb{Z}) \cup (1 + 3\mathbb{Z}) \cup (2 + 3\mathbb{Z}) = [0]_3 \cup [1]_3 \cup [2]_3.$$

For the rest of today, I will assume that G is a finite group. It makes sense to define $[G : H]_L$ – the number of distinct left cosets of H in G and $[G : H]_R$ – the number of distinct right cosets of H in G. Don't get too attached to the subscripts!

We've seen examples of this earlier. If $G = C_6 = \langle a \rangle, a^6 = e$, then as we have already seen, G has four subgroups: $H_1 = \{e\}$, $H_2 = \{e, a^3\}$, $H_3 = \{e, a^2, a^4\}$ and G itself, and we have seen that

$$[G : H_1]_L = [G : H_1]_R = 6, \quad [G : H_2]_L = [G : H_2]_R = 3$$
$$[G : H_3]_L = [G : H_3]_R = 2, \quad [G : G]_L = [G : G]_R = 1.$$

The pattern isn't an accident. The following was the first major theorem in the subject.

LAGRANGE'S THEOREM If G is a finite group and $G \geq H$, then

$$[G : H]_L = [G : H]_R = \frac{|G|}{|H|}.$$

In particular, $|H|$ is a divisor of $|G|$.

We have already seen this in the special case of the cyclic group.

PROOF. Suppose that $|G| = n$ and $H = \{h_1, \ldots, h_m\}$ and $[G : H]_L = r$. Write down G as a union of the distinct cosets of H: $a_1H, \ldots, a_rH$.

$$a_1H = \{a_1h_1, \ldots a_1h_m\}$$
$$a_2H = \{a_2h_1, \ldots a_2h_m\}$$
$$\ldots$$
$$a_rH = \{a_rh_1, \ldots a_rh_m\}.$$

Now count elements.

$$G = \bigcup_{k=1}^{r} a_kH = \{a_1h_1, \ldots a_1h_m, a_2h_1, \ldots a_2h_m \ldots, a_rh_1, \ldots a_rh_m\}$$

There are n elements in G and $r \cdot m = [G : H]_L \cdot |H|$ elements on the right hand side, so $|G| = [G : H]_L \cdot |H|$.
The exact same argument would work with right cosets as well, so $|G| = [G : H]_R \cdot |H|$, hence $[G : H]_L = [G : H]_R$ and we get the desired formula. □.

We now define $[G : H] = [G : H]_L = [G : H]_R$.

COROLLARY Suppose G is a finite group with $|G| = n$ and suppose $x \in G$. Then the order of x is a divisor of n.

PROOF Consider the subgroup $\langle x \rangle = \{e, x, \ldots, x^{d-1}\}$ of G, where $x^d = e$. Then the order of x is d, which is the size of the subgroup $\langle x \rangle$, and by LaGrange, $d \mid n$.

COROLLARY If G is a finite group and $|G| = p$ is prime, then G is a cyclic group of order p, and every non-identity element is a generator.

PROOF Suppose $x \in G, x \neq e$. Then $x^1 \neq e$, so d, the order of x, is ≥ 2. But $d \mid p$ and p is prime, so $d = p$. That is, x has order p, so $\{e, x, \ldots, x^{p-1}\}$ are all distinct, and they constitute all of G. □

COROLLARY If $G > H$, and $[G : H] = 2$, then the cosets of H (left or right) are H and $G \setminus H$, the elements of G which are not in H.

PROOF The coset associated with e is $eH = He = H$, so we may take one of the left (or right) cosets to be H, so

$$G = H \cup aH; \qquad G = H \cup Hb$$

for some $a, b \in G$. But these are disjoint unions, so aH (and Hb) consist of the elements in G which are not in H. □

Well this might seem very abstract, so let's look at the cosets of the subgroups of S_3. I'll cut and paste the multiplication table again.

$$\rho_0 = \begin{pmatrix} 123 \\ 123 \end{pmatrix} = (1)(2)(3), \quad \rho_1 = \begin{pmatrix} 123 \\ 231 \end{pmatrix} = (123),$$

$$\rho_2 = \begin{pmatrix} 123 \\ 312 \end{pmatrix} = (132), \quad \mu_1 = \begin{pmatrix} 123 \\ 132 \end{pmatrix} = (1)(23),$$

$$\mu_2 = \begin{pmatrix} 123 \\ 321 \end{pmatrix} = (13)(2), \quad \mu_3 = \begin{pmatrix} 123 \\ 213 \end{pmatrix} = (12)(3).$$

S_3	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

We have already seen that the subgroups of S_3 are the trivial ones ($\{\rho_0\}$, S_3), plus $\{\rho_0, \rho_1, \rho_2\}$ and $\{\rho_0, \mu_1\}$, $\{\rho_0, \mu_2\}$, $\{\rho_0, \mu_3\}$.

Let $H = \{\rho_0, \rho_1, \rho_2\}$. Then $|H| = 3$ and $|S_3| = 6$, so $[S_3 : H] = 2$ and the corollary applies, so the other coset has to be $S_3 \setminus H$; that is, $\{\mu_1, \mu_2, \mu_3\}$. Let's check:

$$\mu_1 H = \{\mu_1\rho_0, \mu_1\rho_1, \mu_1\rho_2\} = \{\mu_1, \mu_2, \mu_3\}$$
$$H\mu_1 = \{\rho_0\mu_1, \rho_1\mu_1, \rho_2\mu_1\} = \{\mu_1, \mu_3, \mu_2\}$$

Now let $K = \{\rho_0, \mu_1\}$; recall $\rho_0 = (1)(2)(3)$ and $\mu_1 = (1)(23)$. So one left coset is $\rho_0 K = K$. How to we find another left coset? Well $e \in H$ in general, so $x \in xH$. Find an element that isn't used yet. How about μ_2?

$$\mu_2 K = \{\mu_2\rho_0, \mu_2\mu_1\} = \{(13)(2)(1)(2)(3), (13)(2)(1)(23)\}$$
$$= \{(13)(2), (132)\} = \{\mu_2, \rho_2\}.$$

What's not here yet?: μ_3, ρ_1, and it's a good guess that this is the last left coset, but let's check:

$$\rho_1 K = \{\rho_1\rho_0, \rho_1\mu_1\} = \{(123)(1)(2)(3), (123)(1)(23)\}$$
$$= \{(123), (12)(3)\} = \{\rho_1, \mu_3\}.$$

So the left cosets of K are:

$$\{\rho_0, \mu_1\}, \{\mu_2, \rho_2\}, \{\rho_1, \mu_3\}$$

Let's do the right cosets as well. One right coset is $K\rho_0 = K$. Now, ρ_1 hasn't appeared yet, so let's look for $K\rho_1$.

Important note: there are four elements you could have picked here, and any one of them is a valid choice.

$$\begin{aligned} K\rho_1 &= \{\rho_0\rho_1, \mu_1\rho_1\} = \{(1)(2)(3)(123), (1)(23)(123)\} \\ &= \{(123), (13)(2)\} = \{\rho_1, \mu_2\}. \end{aligned}$$

The two elements not accounted for are ρ_2 and μ_3, and

$$\begin{aligned} K\rho_2 &= \{\rho_0\rho_2, \mu_1\rho_2\} = \{(1)(2)(3)(132), (1)(23)(132)\} \\ &= \{(132), (12)(3)\} = \{\rho_2, \mu_3\}. \end{aligned}$$

So the right cosets of K are

$$\{\rho_0, \mu_1\}, \{\rho_1, \mu_2\}, \{\rho_2, \mu_3\}$$

while the left cosets are

$$\{\rho_0, \mu_1\}, \{\mu_2, \rho_2\}, \{\rho_1, \mu_3\}$$

These aren't the same. Except for K, there are lots of partial overlaps.

I hope you paid attention to the logic here. One worksheet exercise on Wednesday will be to do the same thing with the group $L = \{\rho_0, \mu_2\}$.

I'd like to return to D_4, and talk briefly about subgroups, even before we have worked out all of the multiplication table. Here are the elements:

$$\rho_0 = \begin{pmatrix} 1234 \\ 1234 \end{pmatrix} = (1)(2)(3)(4), \quad \rho_1 = \begin{pmatrix} 1234 \\ 2341 \end{pmatrix} = (1234),$$

$$\rho_2 = \begin{pmatrix} 1234 \\ 3412 \end{pmatrix} = (13)(24), \quad \rho_3 = \begin{pmatrix} 1234 \\ 4123 \end{pmatrix} = (1432),$$

$$\mu_1 = \begin{pmatrix} 1234 \\ 2143 \end{pmatrix} = (12)(34), \quad \mu_2 = \begin{pmatrix} 1234 \\ 4321 \end{pmatrix} = (14)(23),$$

$$\delta_1 = \begin{pmatrix} 1234 \\ 3214 \end{pmatrix} = (13)(2)(4), \quad \delta_2 = \begin{pmatrix} 1234 \\ 1432 \end{pmatrix} = (1)(24)(3).$$

This is a group and $|D_4| = 8$, so by LaGrange's Theorem, all subgroups have order dividing 8, and the proper subgroups have order 2 or 4.

We can first list the cyclic groups generated by the elements (I'll ignore the identity ρ_0.) We have a cyclic subgroup of order 4, since $\rho_k = \rho_1^k$, and a bunch a cyclic subgroups of order 2.

$$\langle \rho_1 \rangle = \langle \rho_3 \rangle = \{\rho_0, \rho_1, \rho_2, \rho_3\},$$
$$\langle \rho_2 \rangle = \{\rho_0, \rho_2\},$$
$$\langle \mu_1 \rangle = \{\rho_0, \mu_1\}, \qquad \langle \mu_2 \rangle = \{\rho_0, \mu_2\},$$
$$\langle \delta_1 \rangle = \{\rho_0, \delta_1\}, \qquad \langle \delta_2 \rangle = \{\rho_0, \delta_2\}.$$

If H is a subgroup and $\rho_1 \in H$, then $\langle \rho_1 \rangle \subset H$, and that's already four elements, so if H has any more elements, then $|H| \geq 5$. Thus $H = D_4$. In other words, no other proper subgroup can contain ρ_1, and the same for ρ_3.

If a subgroup is not $\langle a \rangle$, then it has to have more than two elements, and so it has exactly four, the identity ρ_0 and three chosen from $\{\rho_2, \mu_1, \mu_2, \delta_1, \delta_2\}$.

We saw in Monday's worksheet that $\{\rho_0, \rho_2, \mu_1, \mu_2\}$ is a subgroup. It will turn out that $\{\rho_0, \rho_2, \delta_1, \delta_2\}$ is also a subgroup, but that's the only other one. Its table looks remarkably similar.

As a reminder,

$$\rho_0 = \begin{pmatrix} 1234 \\ 1234 \end{pmatrix} = (1)(2)(3)(4) \quad \rho_2 = \begin{pmatrix} 1234 \\ 3412 \end{pmatrix} = (13)(24)$$

$$\delta_1 = \begin{pmatrix} 1234 \\ 3214 \end{pmatrix} = (13)(2)(4), \quad \delta_2 = \begin{pmatrix} 1234 \\ 1432 \end{pmatrix} = (1)(24)(3).$$

It is very easy to check that $\rho_2\delta_1 = \delta_1\rho_2 = \delta_2$, etc, and we get another copy of the Klein 4 group.

H	ρ_0	ρ_2	δ_1	δ_2
ρ_0	ρ_0	ρ_2	δ_1	δ_2
ρ_2	ρ_2	ρ_0	δ_2	δ_1
δ_1	δ_1	δ_2	ρ_0	ρ_2
δ_2	δ_2	δ_1	ρ_2	ρ_0

Finally, suppose H is a subgroup of D_4 and H has both a μ and a δ:

$$\mu_1 = \begin{pmatrix}1234\\2143\end{pmatrix} = (12)(34), \quad \mu_2 = \begin{pmatrix}1234\\4321\end{pmatrix} = (14)(23),$$

$$\delta_1 = \begin{pmatrix}1234\\3214\end{pmatrix} = (13)(2)(4), \quad \delta_2 = \begin{pmatrix}1234\\1432\end{pmatrix} = (1)(24)(3).$$

It's not hard to see that

$$\mu_1\delta_1 = \begin{pmatrix}1234\\4123\end{pmatrix} = \rho_3 \qquad \mu_1\delta_2 = \begin{pmatrix}1234\\2341\end{pmatrix} = \rho_1$$

$$\mu_2\delta_1 = \begin{pmatrix}1234\\2341\end{pmatrix} = \rho_1 \qquad \mu_2\delta_2 = \begin{pmatrix}1234\\4123\end{pmatrix} = \rho_3.$$

Thus, any subgroup that contains μ_i and δ_j is forced to contain ρ_1 or ρ_3, and so is all of D_4.

Thus, the list given is all the subgroups of D_4. You can also find this as Figure 8.13 in the book.