Math 417 – Tenth Day – Class

Bruce Reznick
University of Illinois at Urbana-Champaign

September 16, 2020
I have gotten several useful emails suggesting that I review some of the ideas of the last lecture. Suppose, for the moment, that $G$ is a finite group. (Most of what I say still applies when it’s infinite, but this will allow us to count.)

Suppose $G > H$ so $H$ is a subgroup of $G$. We can look at the cosets, which come in two flavors, the left cosets $gH$ and the right cosets $Hg$. Basically everything we can prove about left cosets can also be proved about right cosets. Some facts:

(i) $G$ can be written as a union of left cosets which are disjoint. The number of cosets, $r = [G : H]$, is equal to $|G|/|H|$.

$$G = a_1H \cup \cdots \cup a_rH; \quad i \neq j \implies a_iH \cap a_jH = \emptyset.$$  

(You can do the same thing with right cosets.) Two left cosets are disjoint, because $z \in xH \cap yH \implies xH = yH$. 
(ii) Are cosets subgroups? Well, $eH = H$ is a subgroup, and it contains $e$. The other cosets can’t contain the identity, and so they can’t be subgroups.

(iii) When $G$ is not abelian, it is possible for the left cosets and the right cosets to have different arrangements of the elements of $G$.

If $H$ is a special kind of subgroup, then $gH = Hg$ as sets, for every $g \in G$. Ironically, this special kind of subgroup is called a normal subgroup. Every subgroup of an abelian group is normal. If $[G : H] = 2$, then $H$ turns out to be normal. We’ll see, soon but not today, that $\{\rho_0, \rho_2\}$ is a normal subgroup of $D_4$.

(iv) How do we find all the cosets? One way is to take $gH$ for every element $g \in G$, and eventually you get them all. As a shortcut, once we start with $eH = H$, we pick any $x \in G \setminus H$. We know that $x$ has to be in a coset and it’s in $xH$, so construct $xH$. If we’re done, we’re done. If not, look at $G \setminus (H \cup xH)$ to find elements we are still missing, etc.
(v) Here’s an example. Look at $C_8 = \{ e, a, a^2, a^3, a^4, a^5, a^6, a^7 \}$, with $H = \{ e, a^4 \}$.

The theorem tells us that $C_8$ can be written as a union of disjoint cosets. Let’s say my favorite element is $a^5$. I don’t see it in a coset yet, so look at $a^5H = \{ a^5 * e, a^5 * a^4 \} = \{ a^5, a^9 \} = \{ a^5, a \}$.

Now I have $H \cup a^5H = \{ e, a^4 \} \cup \{ a^5, a \}$. What’s missing? Well, there are four choices: $a^2, a^3, a^6, a^7$. Pick one, say $a^7$, and look at its coset: $a^7H = \{ a^7 * e, a^7 * a^4 \} = \{ a^7, a^{11} \} = \{ a^7, a^3 \}$.

And $H \cup a^5H \cup a^7H = \{ e, a^4 \} \cup \{ a^5, a \} \cup \{ a^7, a^3 \}$. What’s missing? Only $a^2, a^6$, and $a^2H = \{ a^2 * e, a^2 * a^4 \} = \{ a^2, a^6 \}$. We’re done.

$C_8 = H \cup a^5H \cup a^7H \cup a^2H = \{ e, a^4 \} \cup \{ a^5, a \} \cup \{ a^7, a^3 \} \cup \{ a^2, a^6 \}$.

The order of the cosets and the order of elements in the coset don’t matter: as sets $\{ a^5, a \} = \{ a, a^5 \}$, etc.
(vi) If we are looking for subgroups of $G$, the first step is to look at $\langle g \rangle$ for every $g \in G$. When $G$ is a cyclic group, these are all the subgroups we find. This was also true for $S_3$, but not $D_4$. We can use Lagrange’s Theorem to look at the size of the potential group.

I want to use Lagrange’s Theorem to finish the description of groups of order 6.

What we did the other day was this: Suppose $G$ is a group of order 6 with an element $a$ so that $\{e, a, a^2\}$ are distinct and $a^3 = e$. Suppose $b$ is another element of $G$ and $b^2 = e$. We saw that either $ba = a^2b$ (and $G$ is isomorphic to $S_3$) or $ba = ab$, (and $G$ is isomorphic to $C_6$).

Today I’ll make no hypotheses on $G$, except that $|G| = 6$, and show that these are the only possible groups.
Suppose $x \in G$, then the order of $x$ is 1, 2, 3, 6. First suppose there exists $x \in G$ so that $x$ has order 6. Then $\{e, x, x^2, x^3, x^4, x^5\}$ are distinct, $x^6 = e$, so $G$ is a cyclic group of order 6. Henceforth, we can otherwise assume that there is no element in $G$ of order 6.

We first need a simple result often assigned for homework, even though the proof is not conceptual, and a bizarre computation.

LEMMA If $g \in G \implies g^2 = e$ in a group $G$, then $G$ is abelian.

PROOF We need to show that $a, b \in G \implies ab = ba$. There's a trick. Since $ab \in G$, $(ab)^2 = e$. Write $(ab)^2 = abab = a(ba)b$. We also know that $a^2 = e$ and $b^2 = e$, so there is a chain of identities, multiplying by $a$ on the left and $b$ on the right:

$(ab)^2 = a(ba)b = e \implies$

$a^2(ba)b = ae \implies bab = a \implies$

$bab^2 = ab \implies ba = ab$. □
Suppose now that $G$ is a group of order 6 and $G$ has no element of order 3 or order 6. I’ll show that this is impossible.

If $x \in G$ and $x \neq e$, then $x$ must have order 2. Pick such an $x$. $G$ has 6 elements and $\{e, x\}$ only gives 2, so there has to be another element in $G$, call it $y$, so $e, x, y$ are all different.

What about $xy$? If $xy = e$, then $xy = x^2 \implies y = x$. If $xy = x = xe$, then $y = e$. If $xy = y = ey$, then $x = e$. These impossibilities say that $H = \{e, x, y, xy\}$ are all distinct. Look at the multiplication table for $H$. We know that $x^2 = y^2 = (xy)^2 = e$ and, say $y(xy) = (yx)y = (xy)y = xy^2 = x$. We can fill out the table completely.

\[
\begin{array}{c|cccc}
H & e & x & y & xy \\
\hline
e & e & x & y & xy \\
x & x & e & xy & y \\
y & y & xy & e & x \\
xy & xy & y & x & e \\
\end{array}
\]
Another copy of the Klein 4 group!

What could be wrong with that? Well, $H$ is a subset of $G$ and $H$ is a group, so it’s a subgroup of $G$, and $|H| = 4$, $|G| = 6$ and 4 doesn’t divide 6.

What does this mean? It means that our assumption that there were no elements of order three leads to a contradiction, so suppose $a \in G$ and $a$ has order 3, $\{e, a, a^2\}$ are in $G$, and let $b$ be another element of $G$. Then $ab, a^2b$ have to be in $G$, because it’s closed under multiplication, and we’ve already shown that $\{e, a, a^2, b, ab, a^2b\}$ are all different.

But now we know something more: we know that $b^2 = e$ or $b^3 = e$. We did the work a few days ago to handle the case $b^2 = e$. Now suppose $b^3 = e$. I won’t need to worry about $ba$. 
Here is the multiplication table

<table>
<thead>
<tr>
<th></th>
<th>$e$</th>
<th>$a$</th>
<th>$a^2$</th>
<th>$b$</th>
<th>$ab$</th>
<th>$a^2b$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$e$</td>
<td>$e$</td>
<td>$a$</td>
<td>$a^2$</td>
<td>$b$</td>
<td>$ab$</td>
<td>$a^2b$</td>
</tr>
<tr>
<td>$a$</td>
<td>$a$</td>
<td>$a^2$</td>
<td>$e$</td>
<td>$ab$</td>
<td>$a^2b$</td>
<td>$b$</td>
</tr>
<tr>
<td>$a^2$</td>
<td>$a^2$</td>
<td>$e$</td>
<td>$a$</td>
<td>$a^2b$</td>
<td>$b$</td>
<td>$ab$</td>
</tr>
<tr>
<td>$b$</td>
<td>$b$</td>
<td>$?$</td>
<td>$?$</td>
<td>$?$</td>
<td>$?$</td>
<td>$?$</td>
</tr>
<tr>
<td>$ab$</td>
<td>$ab$</td>
<td>$?$</td>
<td>$?$</td>
<td>$?$</td>
<td>$?$</td>
<td>$?$</td>
</tr>
<tr>
<td>$a^2b$</td>
<td>$a^2b$</td>
<td>$?$</td>
<td>$?$</td>
<td>$?$</td>
<td>$?$</td>
<td>$?$</td>
</tr>
</tbody>
</table>

It’s not clear what $b^2$ is: from looking at the column, it might be $e$, $a$, $a^2$. We’ve already talked about $b^2 = e$, so consider $b^2 = a$ or $b^2 = a^2$. Now, multiplying on the right by $b$, these imply $b^3 = ab$ or $b^3 = a^2b$. Neither of these is $e$, so this case is a dead end too, and we’ve run out of cases.
THEOREM If $G$ is a group and $|G| = 6$, then $G$ is either isomorphic to $C_6$ or isomorphic to $S_3$.

Since 2,3,5,7 are prime, any group with those orders must be cyclic. We’ve also completely analyzed groups of order 4 and order 6. It turns out that there are five different groups of order 8: we’ve already seen three of them: $C_8$, $D_4$, and $(\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/4\mathbb{Z})$. We’ll see the other two eventually.

The number of non-isomorphic groups of a given order can get very large, especially when the order is a power of a prime.

There are 14 non-isomorphic groups of order $16 = 2^4$, 267 non-isomorphic groups of order $64 = 2^6$, 56092 non-isomorphic groups of order $256 = 2^8$ and $4948736522$ non-isomorphic groups of order $1024 = 2^{10}$.

In fact 99.15% of all the groups of order < 2000 have order 1024.
WORKSHEET PROBLEM 1. (As promised.) Find the left cosets and the right cosets for the subgroup $L = \{\rho_0, \mu_2\}$.

$$
\begin{align*}
\rho_0 &= \begin{pmatrix} 123 \\ 123 \end{pmatrix} = (1)(2)(3), & \rho_1 &= \begin{pmatrix} 123 \\ 231 \end{pmatrix} = (123), \\
\rho_2 &= \begin{pmatrix} 123 \\ 312 \end{pmatrix} = (132), & \mu_1 &= \begin{pmatrix} 123 \\ 132 \end{pmatrix} = (1)(23), \\
\mu_2 &= \begin{pmatrix} 123 \\ 321 \end{pmatrix} = (13)(2), & \mu_3 &= \begin{pmatrix} 123 \\ 213 \end{pmatrix} = (12)(3).
\end{align*}
$$

<table>
<thead>
<tr>
<th>$S_3$</th>
<th>$\rho_0$</th>
<th>$\rho_1$</th>
<th>$\rho_2$</th>
<th>$\mu_1$</th>
<th>$\mu_2$</th>
<th>$\mu_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\rho_0$</td>
<td>$\rho_0$</td>
<td>$\rho_1$</td>
<td>$\rho_2$</td>
<td>$\mu_1$</td>
<td>$\mu_2$</td>
<td>$\mu_3$</td>
</tr>
<tr>
<td>$\rho_1$</td>
<td>$\rho_1$</td>
<td>$\rho_2$</td>
<td>$\rho_0$</td>
<td>$\mu_3$</td>
<td>$\mu_1$</td>
<td>$\mu_2$</td>
</tr>
<tr>
<td>$\rho_2$</td>
<td>$\rho_2$</td>
<td>$\rho_0$</td>
<td>$\rho_1$</td>
<td>$\mu_2$</td>
<td>$\mu_3$</td>
<td>$\mu_1$</td>
</tr>
<tr>
<td>$\mu_1$</td>
<td>$\mu_1$</td>
<td>$\mu_2$</td>
<td>$\mu_3$</td>
<td>$\rho_0$</td>
<td>$\rho_1$</td>
<td>$\rho_2$</td>
</tr>
<tr>
<td>$\mu_2$</td>
<td>$\mu_2$</td>
<td>$\mu_3$</td>
<td>$\mu_1$</td>
<td>$\rho_2$</td>
<td>$\rho_0$</td>
<td>$\rho_1$</td>
</tr>
<tr>
<td>$\mu_3$</td>
<td>$\mu_3$</td>
<td>$\mu_1$</td>
<td>$\mu_2$</td>
<td>$\rho_1$</td>
<td>$\rho_2$</td>
<td>$\rho_0$</td>
</tr>
</tbody>
</table>
WORKSHEET SOLUTION

First the left cosets. As always, \( L = L\rho_0 = \{\rho_0, \mu_2\} \) is one of the cosets. I don’t see \( \rho_1 \) so I’ll look at

\[
\rho_1 L = \{\rho_1\rho_0, \rho_1\mu_2\} = \{\rho_1, \mu_1\}.
\]

I don’t see \( \rho_2 \), so I’ll take that:

\[
\rho_2 L = \{\rho_2\rho_0, \rho_2\mu_2\} = \{\rho_2, \mu_3\}.
\]

So the left cosets are

\[
\{\rho_0, \mu_2\}, \quad \{\rho_1, \mu_1\}, \quad \{\rho_2, \mu_3\}.
\]

You could have taken other missing elements, but you should wind up with the same cosets.
Now the right cosets. As always, \( L = L\rho_0 = \{\rho_0, \mu_2\} \) is one of the cosets. I don’t see \( \rho_1 \) so I’ll look at

\[
L\rho_1 = \{\rho_0\rho_1, \mu_2\rho_1\} = \{\rho_1, \mu_3\}.
\]

I don’t see \( \rho_2 \), so I’ll take that:

\[
L\rho_2 = \{\rho_0\rho_2, \mu_2\rho_2\} = \{\rho_2, \mu_1\}.
\]

So the right cosets are

\[
\{\rho_0, \mu_2\}, \quad \{\rho_1, \mu_3\}, \quad \{\rho_2, \mu_1\}.
\]

Recall, the left cosets were

\[
\{\rho_0, \mu_2\}, \quad \{\rho_1, \mu_1\}, \quad \{\rho_2, \mu_3\}.
\]

Again, a partial overlap.