Groups and Group Action, Sheet 4, HT2020

Starter

I would really appreciate feedback on ways in which these comments and solutions could be improved and made more helpful, so please let me know about typos (however trivial), mistakes, alternative solutions, or additional comments that might be useful.

Vicky Neale (vicky.neale@maths)

S1. In this question we work in $\mathbb{Z}_8$. For each $a \in \mathbb{Z}_8$, find a^7. How does this relate to Fermat's Little Theorem and to the Fermat-Euler Theorem?

a	0	1	2	3	4	5	6	7
a^7	0	1	0	3	0	5	0	7

This shows that Fermat's Little Theorem doesn't hold in $\mathbb{Z}_8$: we don't have $a^7 \equiv 1 \pmod 8$ for all a coprime to 8. Of course, the theorem only claimed that this would hold for primes, and 8 is not prime, so this is not a counterexample, but it does show that we cannot simply extend the result to non-primes.

We have $\phi(8) = 4$, so the Fermat-Euler Theorem says that $a^4 \equiv 1 \pmod 8$ for all a coprime to 8. This does not tell us about 7th powers. In fact, we find that $a^2 \equiv 1 \pmod 8$ for all a coprime to 8, so in this case there is a stronger result than Fermat-Euler.

S2. Consider the dihedral group $D_8 = \{e, r, r^2, r^3, s, rs, r^2s, r^3s\}$ with the notation from lectures. Find all the left cosets of $\langle r \rangle$ in D_8. Find all the right cosets of $\langle r \rangle$. How do these lists compare? Now repeat for the subgroup $\langle s \rangle$.

We have $\langle r \rangle = \{e, r, r^2, r^3\}$. Now we find the left cosets of $\langle r \rangle$ in D_8.

$$\begin{aligned}
e\langle r \rangle &= \{e, r, r^2, r^3\} \\
r\langle r \rangle &= \{r, r^2, r^3, e\} \\
r^2\langle r \rangle &= \{r^2, r^3, e, r\} \\
r^3\langle r \rangle &= \{r^3, e, r, r^2\} \\
s\langle r \rangle &= \{s, r^3s, r^2s, rs\} \\
rs\langle r \rangle &= \{rs, s, r^3s, r^2s\} \\
r^2s\langle r \rangle &= \{r^2s, rs, s, r^3s\} \\
r^3s\langle r \rangle &= \{r^3s, r^2s, rs, s\}
\end{aligned}$$

—so there are two left cosets of $\langle r \rangle$ in D_8, as we expect from Lagrange's theorem (since $|D_8| = 8$ and $|\langle r \rangle| = 4$.

And the right cosets:

$$\begin{aligned}
\langle r \rangle e &= \{e, r, r^2, r^3\} \\
\langle r \rangle r &= \{r, r^2, r^3, e\} \\
\langle r \rangle r^2 &= \{r^2, r^3, e, r\} \\
\langle r \rangle r^3 &= \{r^3, e, r, r^2\} \\
\langle r \rangle s &= \{s, rs, r^2 s, r^3 s\} \\
\langle r \rangle rs &= \{rs, r^2 s, r^3 s, s\} \\
\langle r \rangle r^2 s &= \{r^2 s, r^3 s, s, rs\} \\
\langle r \rangle r^3 s &= \{r^3 s, s, rs, r^2 s\}
\end{aligned}$$

There are two right cosets, and in fact the left cosets are the same as the right cosets (we have $g\langle r \rangle = \langle r \rangle g$ for all $g \in D_8$). This relates to the notion of a *normal subgroup*, which will play an important role in the second half of this course.

Now $\langle s \rangle = \{e, s\}$, and the left cosets of $\langle s \rangle$ in D_8 are

$$\begin{aligned}
e\langle s \rangle &= \{e, s\} \\
r\langle s \rangle &= \{r, rs\} \\
r^2\langle s \rangle &= \{r^2, r^2 s\} \\
r^3\langle s \rangle &= \{r^3, r^3 s\} \\
s\langle s \rangle &= \{s, e\} \\
rs\langle s \rangle &= \{rs, r\} \\
r^2 s\langle s \rangle &= \{r^2 s, r^2\} \\
r^3 s\langle s \rangle &= \{r^3 s, r^3\}
\end{aligned}$$

while the right cosets are

$$\begin{aligned}
\langle s \rangle e &= \{e, s\} \\
\langle s \rangle r &= \{r, r^3 s\} \\
\langle s \rangle r^2 &= \{r^2, r^2 s\} \\
\langle s \rangle r^3 &= \{r^3, rs\} \\
\langle s \rangle s &= \{s, e\} \\
\langle s \rangle rs &= \{rs, r^3\} \\
\langle s \rangle r^2 s &= \{r^2 s, r^2\} \\
\langle s \rangle r^3 s &= \{r^3 s, r\}
\end{aligned}$$

Lagrange's theorem tells us that we should have 4 different left cosets (and 4 different right cosets), and indeed we do.

Note that this time it is not always the case that the left and right cosets are the same, for example $r\langle s \rangle \neq \langle s \rangle r$. Again, this relates to the concept of a normal subgroup—more precisely, it shows that $\langle s \rangle$ is not a normal subgroup of D_8, whereas $\langle r \rangle$ is.

S3. For each of the following, give a proof or a counterexample.

(i) A group with order 20 cannot have a subgroup of order 10.

(ii) A group with order 22 cannot have a subgroup of order 10.

(iii) A group with order 10 cannot have a subgroup of order 22.

(iv) A group with order 10 must have a subgroup of order 10.

(v) A group with order 12 must have a subgroup of order 6.

(i) This is false. For example, consider $C_{20} = \langle g \rangle$, then the subgroup $\langle g^2 \rangle$ has order 10.

(ii) This is true, by Lagrange's Theorem, because $10 \nmid 22$.

(iii) This is true, because any subgroup of a group of order 10 contains at most 10 elements.

(iv) This is true, because if G is a group with order 10, then G is a subgroup of order 10.

(v) This is false. The alternating group A_4 has order 12, but contains no subgroup of order 6.