Abstract Algebra Homework 5

Joe Loser

February 28, 2016

This problem set includes problems from sections 5.3 and 6.4 as well as an extra problem from lecture: in particular, problem 31 and 34 from 5.3, $5h$ and 8 from section 6.4.

31) For α and β in S_n, define $a \sim b$ if there exists an $\sigma \in S_n$ such that $\sigma\alpha\sigma^{-1} = \beta$. Show that $\sim$ is an equivalence relation on S_n.

Proof: To show $\sim$ is an equivalence relation, we need to show it is reflexive, symmetric, and transitive.

(i) Let $\alpha \in S_n$. Then there exist $\sigma \in S_n$ such that $\sigma\alpha\sigma^{-1} = \alpha$, i.e. $\sigma = 1_S$. This can be seen by first left multiplying by σ^{-1}. So we have the following:

$$\begin{aligned}
\sigma^{-1}\sigma\alpha\sigma^{-1} &= \sigma^{-1}\alpha \\
\alpha\sigma^{-1} &= \sigma^{-1}\alpha \\
\alpha &= \sigma^{-1}\alpha\sigma \\
\alpha &= \sigma^{-1}\alpha(\sigma^{-1})^{-1}
\end{aligned}$$

Hence, $\sigma = \sigma^{-1}$ and the identity works for such σ. Therefore, $a \sim a$ and we have that $\sim$ is reflexive.

(ii) Let $\alpha, \beta \in S_n$. If $\alpha \sim \beta$ then there exist $\sigma \in S_n$ such that $\sigma\alpha\sigma^{-1} = \beta$. We want to show this implies that $b \sim a$ – that is, $\sigma\beta\sigma^{-1} = \alpha$. By left multiplying by σ^{-1}, we have the following:

$$\begin{aligned}
\sigma^{-1}\sigma\alpha\sigma^{-1} &= \sigma^{-1}\beta \\
\alpha\sigma^{-1} &= \sigma^{-1}\beta \\
\alpha\sigma^{-1}\sigma &= \sigma^{-1}\beta\sigma \\
\alpha &= \sigma^{-1}\beta\sigma
\end{aligned}$$

Now, we rewrite σ as $(\sigma^{-1})^{-1}$ which yields

$$\alpha = \sigma^{-1}\beta(\sigma^{-1})^{-1}.$$

Therefore $\beta \sim \alpha$ and hence $\sim$ is symmetric.

(iii) Suppose $\alpha \sim \beta$ and $\beta \sim \gamma$. Then there exist σ_1 and $\sigma_2 \in S_n$ such that

$$\sigma_1 \alpha \sigma_1^{-1} = \beta \tag{1}$$
$$\sigma_2 \beta \sigma_2^{-1} = \gamma \tag{2}$$

We want to show $\alpha \sim \gamma$, i.e. $\sigma_1 \alpha \sigma_1^{-1} = \gamma$. Multiplying equations (1) and (2) yields:

$$\sigma_2 \sigma_1 \beta \alpha \sigma_1^{-1} \sigma_2^{-1} = \gamma \beta$$

and by canceling the β term yields:

$$\sigma_2 \sigma_1 \alpha \sigma_1^{-1} \sigma_2^{-1} = \gamma$$

which can be written as

$$(\sigma_2 \sigma_1) \alpha (\sigma_2 \sigma_1)^{-1} = \gamma.$$

Thus we have shown that $\sim$ is transitive.

Therefore, $\sim$ is reflexive, symmetric, and transitive. Hence, it is an equivalence relation on S_n. $\square$

34) If α is even, prove that α^{-1} is also even. Does a corresponding result hold if α is odd?

Proof: Let α be an even permutation. Then α can be written as a product of an even number of transpositions:

$$\alpha = \tau_1 \tau_2 \ldots \tau_m.$$

So α is even if and only if m is even. Then

$$\begin{aligned} \alpha^{-1} &= (\tau_1 \tau_2 \ldots \tau_m)^{-1} \\ &= \tau_m^{-1} \tau_{m-1}^{-1} \ldots \tau_2^{-1} \tau_1^{-1} \end{aligned}$$

Note that for any transposition (2-cycle) τ, we have that $\tau^{-1} = \tau$. Thus,

$$\alpha^{-1} = \tau_m \ldots \tau_2 \tau_1. \tag{3}$$

In equation (3), if m is even, then α^{-1} is even. A similar argument (by symmetry) can be shown for m odd. If m is odd, then this shows that α^{-1} is also odd. $\square$

Alternative Proof: Note that (1) is even and hence $\alpha\alpha^{-1}$ is also even where $\alpha\alpha^{-1}$ is the product of the transpositions of α and α^{-1}. Then this shows that

even number = number transpositions for α + number transpositions for α^{-1}

since (1) is an even number. Thus, α is even/odd if and only if α^{-1} is even/odd. $\square$

5h) List the left and right cosets for $H = \{(1), (123), (132)\}$ in S_4.

Solution: Let $G = S_4$ and H as above. Then, by Lagrange's Theorem – for a finite group G with $H < G$, the number of *distinct* left cosets (and right cosets – same number) is equal to

$$\begin{aligned}[G : H] &= \frac{|G|}{|H|} \\ &= \frac{4!}{3} \\ &= \frac{24}{3} \\ &= 8.\end{aligned}$$

We begin by noting that S_4 is a set whose order is 24 and contains the following elements:
$\{(1), (12), (13), (14), (23), (24), (34),$
$(142), (143), (134), (132), (124), (123), (243), (234)$
$(12)(34), (14)(23), (13)(24),$
$(1423), (1432), (1324), (1342), (1243), (1234)\}.$

Let $G = S_4$. To find the left cosets of H under G, we want to keep picking $g \in G$, multiply it by H and examine the sets that arise. Recall that $gH = \{gh \mid h \in H\}$ is the left coset of H in G with respect to g. Similarly, $Hg = \{hg \mid h \in H\}$ is the right coset of H in G with respect to g.

For the left cosets, we have the following:

1. $(1)H = \{(1)(1), (1)(123), (1)(132)\} = \{(1), (123), (132)\}$
2. $(14)H = \{(14)(1), (14)(123), (14)(132)\} = \{(14), (1234), (1324)\}$
3. $(23)H = \{(23)(1), (23)(123), (23)(132)\} = \{(23), (13), (12)\}$
4. $(24)H = \{(24)(1), (24)(123), (24)(132)\} = \{(24), (1423), (1342)\}$
5. $(34)H = \{(34)(1), (34)(123), (34)(132)\} = \{(34), (1243), (1432)\}$
6. $(124)H = \{(123)(1), (124)(123), (124)(132)\} = \{(124), (14)(23), (134)\}$
7. $(142)H = \{(142)(1), (142)(123), (142)(132)\} = \{(142), (234), (13)(24)\}$
8. $(143)H = \{(143)(1), (143)(123), (143)(132)\} = \{(143), (12)(34), (243)\}$

Note that there are 8 left cosets, each of order 3. Each of them is disjoint as well and make up the original group G which has 24 elements. Further computations can show for example, that $(132)H = (1)H, (12)H = (23)H$, and more. But, we know we are done as we have found 8 distinct left cosets which is all Lagrange's Theorem guarantees us. Now let's work on the right cosets.

For the right cosets, we have the following:

1. $H(1) = \{(1)(1), (123)(1), (132)(1)\} = \{(1), (123), (132)\}$
2. $H(14) = \{(1)(14), (123)(14), (132)(14)\} = \{(14), (1423), (1432)\}$
3. $H(23) = \{(1)(23), (123)(23), (132)(23)\} = \{(23), (12), (13)\}$
4. $H(24) = \{(1)(24), (123)(24), (132)(24)\} = \{(24), (1243), (1324)\}$
5. $H(34) = \{(1)(34), (123)(34), (132)(34)\} = \{(34), (1234), (1342)\}$
6. $H(124) = \{(1)(124), (123)(124), (132)(124)\} = \{(124), (13)(24), (243)\}$
7. $H(142) = \{(1)(142), (123)(142), (132)(142)\} = \{(142), (143), (14)(23)\}$
8. $H(234) = \{(1)(234), (123)(234), (132)(234)\} = \{(234), (12)(34), (134)\}$

Note, again, that there are 8 right cosets and that these are not the same as the left cosets. They do still partition the group G into 8 cosets, each of 3 elements. $\square$

8) Use Fermat's Little Theorem to show that if $p = 4n+3$ is prime, there is no solution to the equation $x^2 \equiv -1 \pmod p$.

<u>Proof</u>: Recall that Fermat's Little Theorem states that if p is prime and $p \nmid a$ then $a^{p-1} \equiv 1 \pmod p$.

Suppose that $x^2 \equiv -1 \pmod p$. Then $x \neq 0 \pmod p$. So, by Fermat's Little Theorem, we have that $x^{p-1} \equiv 1 \pmod p$. Therefore,

$$\begin{aligned} x^{p-1} &\equiv x^{4n+3-1} \\ &\equiv x^{4n+2} \\ &\equiv x^{2\cdot(2n+1)} \\ &\equiv (x^2)^{2n+1} \\ &\equiv -1 \pmod p \end{aligned}$$

Since $x^{p-1} \equiv 1 \pmod p$ and $x^{p-1} \equiv -1 \pmod p$, we have that $1 \equiv -1 \pmod p$. So $2 \equiv 0 \pmod p$. This implies $p = 2$. However, since $p = 4n+3$, we have that

$$2 = 4n + 3 \implies -1 = 4n \implies n = -\frac{1}{4}.$$

We have reached a contradiction now though since while there are infinitely many primes of the form $4n+3$, typically the notion is that $n \in \mathbb{N}$ and hence cannot be less than 0. Thus, $p \neq 2$ and there are no solutions to the equation $x^2 \equiv -1 \pmod p$. $\square$

E1) Show 63 is not prime using Fermat's Little Theorem.

<u>Solution</u>: To begin, we want to find the first power, say x, such that $2^x > 63$. Clearly $x = 6$ since $2^6 = 64 > 63$. In fact, note that $2^6 \equiv 1 \pmod{63}$. Now we want to write

62 using the Division Algorithm: namely, $62 = 10 \cdot 6 + 2$. Then in $\pmod{63}$,

$$\begin{aligned} 2^{62} &= (2^6)^{10} \cdot 2^2 \\ &= (1)^{10} \cdot 4 \\ &= 4 \end{aligned}$$

by using the fact that $2^6 \equiv 1 \pmod{63}$. So $2^{62} \equiv 4 \pmod{63} \not\equiv 1 \pmod{63}$. Thus, 63 is not prime by Theorem 6.19 (Fermat's Little Theorem) which states that for any p prime, integer a such that $p \nmid a$

$$a^{p-1} \equiv 1 \pmod{p}.$$

As we have shown, for $a = 2$ arbitrarily, we reached that $2^{62} \equiv 4 \pmod{63}$. Hence 63 is not prime. $\square$