Abstract Algebra Homework 4

Joe Loser

February 21, 2016

This problem set includes problems from sections 4.4 and 5.3 as well as an extra problem from lecture: in particular, problem 9 from 4.4, 27 and 30 from section 5.3.

9) List every generator of each subgroup of order 8 in $\mathbb{Z}_{32}$.

<u>Proof</u>: Because $\mathbb{Z}_{32}$ is a finite cyclic group of order 32 generated by 1, by theorem G9, there is a *unique* subgroup, let's call it H, of order 8 which is

$$\left\langle \frac{32}{8} \right\rangle = \left\langle 4 \cdot 1 \right\rangle = \left\langle 4 \right\rangle.$$

To find the generators of this subgroup, we want to find all $1 \leq k < 8$ such that $gcd(8, k) = 1$. As you can see, k can be $1, 3, 5$, or 7 (note: this is $U(8)$.) So,

$$\langle 4^1 \rangle = \langle 4^3 \rangle = \langle 4^5 \rangle = \langle 4^7 \rangle.$$

Thus, the generators of H are

$$\{4 \cdot 1, 4 \cdot 3, 4 \cdot 5, 4 \cdot 7\} = \{4, 12, 20, 28\}$$

We can verify the order of each of these elements have order 8:

$$\begin{aligned}
|4| &= \frac{32}{gcd(4, 32)} = \frac{32}{4} = 8 \\
|12| &= \frac{32}{gcd(12, 32)} = \frac{32}{4} = 8 \\
|20| &= \frac{32}{gcd(20, 32)} = \frac{32}{4} = 8 \\
|28| &= \frac{32}{gcd(28, 32)} = \frac{32}{4} = 8
\end{aligned}$$

As we have shown, the generators of H (keeping in mind our binary operator is +) are $\{4, 12, 20, 28\}$. $\square$

27) Let G be a group and define a map $\lambda_g : G \to G$ by $\lambda_g(a) = ga$. Prove that λ_g is a permutation of G.

Proof: In order to show λ_g is a permutation of G, we need to show $\lambda_g(a)$ is well-defined under multiplication and that λ_g is one-to-one and onto.

First, $\lambda_g(a)$ is well-defined since the multiplication in the group G is well-defined by definition of being a group equipped with operator *.

Next, let $a, b \in G$ and $\lambda_g(a) = \lambda_g(b)$. Then we have that $ga = gb$. So, by left-cancellation, we arrive immediately at the fact that $a = b$. Hence, λ_g is one-to-one.

Lastly, to prove λ_g is onto, let $c \in G$. Then $g^{-1}c \in G$ since G is a group (G has inverses). So, $\lambda_g(g^{-1}c) = g(g^{-1}c) = (gg^{-1})c = c$. Hence, λ_g is onto.

Therefore, $\lambda_g : G \to G$ is a permutation since it is one-to-one and onto. $\square$

30) Let $\tau = (a_1, a_2, \ldots, a_k)$ be a cycle of length k.

a) Prove that if σ is any permutation, then

$$\sigma\tau\sigma^{-1} = (\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_k)) \tag{1}$$

is a cycle of length k.

b) Let μ be a cycle of length k. Prove that there is a permutation σ such that

$$\sigma\tau\sigma^{-1} = \mu.$$

Proof:

a) By right multiplying equation (1) by σ, we see that equation (1) is true precisely if

$$\sigma\tau = (\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_k))\sigma. \tag{2}$$

Now, we want to prove equation (2) is indeed true. Let's consider $x \notin \{a_1, a_2, \ldots, a_k\}$ and $x \in \{a_1, a_2, \ldots, a_k\}$ for some x.

If $x \notin \{a_1, a_2, \ldots, a_k\}$, then $\sigma\tau(x) = \sigma(x)$ since $\tau(x) = x$. Further, notice that

$$(\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_k))\sigma(x) = \sigma(x) \tag{3}$$

because the cycle $(\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_k))$ only acts on the elements $\sigma(a_i)$ for some $1 \leq i \leq k$. As we discussed in recitation, the cycle in (3) fixes everything else, i.e. it does not change to what it maps to. Thus, since we have $x \notin \{a_1, \ldots, a_k\}$, the cycle fixes $\sigma(x)$. Therefore, when we consider $x \notin \{a_1, a_2, \ldots, a_k\}$, we get the following:

$$\begin{aligned}\sigma\tau(x) &= \sigma(x) \\ &= (\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_k))\sigma(x).\end{aligned}$$

Now, let's consider if $x \in \{a_1, a_2, \ldots, a_k\}$. In this case, we have that $x = a_i$ for $1 \le i \le k$ as earlier. If $i \neq k$, then $\tau(a_i) = a_{i+1}$. Then, we get that

$$\begin{aligned}\sigma\tau(x) &= \sigma\tau(a_i)\\ &= \sigma(a_{i+1})\end{aligned}$$

So, we effectively get the next element as seen below:

$$(\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_k))\sigma(a_i) = \sigma(a_{i+1}).$$

If $i = k$, then $\tau(a_k) = a_1$. Hence, $\sigma\tau(a_k) = \sigma(a_1)$, i.e. it forms a k-cycle since it points back to a_1 and

$$(\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_k))\sigma(a_k) = \sigma(a_1).$$

Therefore $\sigma\tau(x) = (\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_k))\sigma(x)$ for all x and hence equations (1) and (2) are equivalently true. □

b) Let $\mu := (b_1, b_2, \ldots, b_k)$. Now we just need to have some permutation, σ, in which $\sigma(a_i) = b_i$ and fixes x otherwise, i.e. $\sigma(x) = x$. Then by part a) of this question, we have the following:

$$\begin{aligned}\sigma\tau\sigma^{-1} &= (\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_k))\\ &= (b_1, b_2, \ldots, b_k)\\ &= \mu\end{aligned}$$

as desired. □

E1) Use Theorem $G9$ to dissect the group $\mathbb{Z}_{45}$. We want to find all subgroups, list all elements of each subgroup, and find all of the generators of each subgroup. In addition, draw a subgroup diagram and show that our work implies that

$$\sum_{\substack{k \geq 1 \\ k \mid 45}} \phi(k) = 45.$$

<u>Solution</u>: *All* of the generators of $\mathbb{Z}_{45}$ are the numbers a that are relatively prime to 45. So,

$$1, 2, 4, 7, 8, 11, 13, 14, 16, 17, 19, 22, 23, 26, 28, 29, 31, 32, 34, 37, 38, 41, 43, 44$$

are all of the generators. Note in particular that there are 24 generators = $\phi(45)$.

To find all of the subgroups of $\mathbb{Z}_{45}$, we can just look at the positive divisors of 45 per Theorem G9. These are $1, 3, 5, 9, 15, 45$. Below we list the elements of each of these subgroups formed. Note that the operator in our group is addition, so the subgroups generated by a, $\langle a \rangle$, are $\{na \mid n \in \mathbb{Z}\}$.

$$
\begin{aligned}
\langle 1\rangle &= \{1, a, 2a, 3a, \ldots, 44a\} \\
\langle 3\rangle &= \{1, 3a, 6a, 9a, \ldots, 42a\} \\
\langle 5\rangle &= \{1, 5a, 10a, 15a, 20a, 25a, 30a, 35a, 40a\} \\
\langle 9\rangle &= \{1, 9a, 18a, 27a, 36a\} \\
\langle 15\rangle &= \{1, 15a, 30a\} \\
\langle 45\rangle &= \{1\}
\end{aligned}
$$

The order of each of these subgroups is:

$$
\begin{aligned}
|\langle 1\rangle| &= \frac{45}{1} = 45 \\
|\langle 3\rangle| &= \frac{45}{3} = 15 \\
|\langle 5\rangle| &= \frac{45}{5} = 9 \\
|\langle 9\rangle| &= \frac{45}{9} = 5 \\
|\langle 15\rangle| &= \frac{45}{15} = 3 \\
|\langle 45\rangle| &= \frac{45}{45} = 1
\end{aligned}
$$

Note: I did not feel up for learning the Tikz package for drawing the subgroup diagrams, so it is hand-drawn and attached.

To show our implies that

$$\sum_{\substack{k\geq 1 \\ k|45}} \phi(k) = 45$$

we can use brute force or think in terms of generators. The former can be seen by simply noting

$$
\begin{aligned}
\sum_{\substack{k\geq 1 \\ k|45}} \phi(k) &= \phi(1) + \phi(3) + \phi(5) + \phi(9) + \phi(15) + \phi(45) \\
&= 1 + 2 + 4 + 6 + 8 + 24 \\
&= 45
\end{aligned}
$$

Thinking along the line of generators, notice that if G is finite cyclic group with order n then G is isomorphic to $\mathbb{Z}/n\mathbb{Z}$. If we have a generator $a \in G$ – for example, the image of 1 under an isomorphism of $\mathbb{Z}/n\mathbb{Z} \to G$, then $a^k \in G$ if and only if $gcd(n, k) = 1$.

Hence, there are exactly $\phi(n)$ generators in a finite cyclic group which is more or less the definition of the Euler-phi function. In our case, $n = 45 = \sum_{\substack{k \geq 1 \\ k|45}} \phi(k)$. $\square$