Homework 2 **John Waczak**
PH 431 Date: October 16, 2017
Prof. Ren Guo

4.4.8

List all of the cyclic subgroups of U(30).

Recall that U(30) is the set of elements in $\mathbb{Z}_{30}$ that are relatively prime to 30. Thus:

$$U(30) = \{1, 7, 11, 13, 17, 19, 23, 29\}$$

We have that $1 = id$ for U(30) but $\langle 1 \rangle$ is a trivial subgroup. We can calculate the other cyclic subgroups by analyzing powers of each element of U(30). We have that:

$$\begin{aligned}
&7 \\
&7^2 \mod (30) = 19 \\
&7^3 \mod (30) = 13 \\
&7^4 \mod (30) = 1 \\
&11 \\
&11^2 \mod (30) = 1 \\
&13 \\
&13^2 \mod (30) = 19 \\
&13^3 \mod (30) = 7 \\
&13^4 \mod (30) = 1 \\
&17 \\
&17^2 \mod (30) = 19 \\
&17^3 \mod (30) = 23 \\
&17^4 \mod (30) = 1 \\
&23 \\
&23^2 \mod (30) = 19 \\
&23^3 \mod (30) = 17 \\
&23^4 \mod (30) = 1 \\
&29 \\
&29^2 \mod (30) = 1
\end{aligned}$$

Thus from this information we can conclude that the cyclic subgroups of U(30) are:

$$\begin{aligned}
\langle 7 \rangle = \langle 13 \rangle &= \{1, 7, 13, 19\} \\
\langle 11 \rangle &= \{1, 11\} \\
\langle 17 \rangle = \langle 23 \rangle &= \{1, 17, 19, 23\} \\
\langle 29 \rangle &= \{1, 29\}
\end{aligned}$$

4.4.25

Let p be prime and r be a positive integer. How many generators does $\mathbb{Z}_{p^r}$ *have?*

Note that $\mathbb{Z}_{p^r}$ has exactly p^r elements. Now, an element g of $\mathbb{Z}_{p^r}$ is a generator if $1 \leq g < p^r$ and $gcd(g, p^r) = 1$. Since p is prime, the only possible values of $gcd(g, p^r)$ are $p, p^2, p^3, ..., p^r$. The only way $gcdg, p^r \neq 1$ is if $g = mp$ for some integer m. This set is:

$$\{p, 2p, 3p...pp, 2pp, 3pp...p^3, 2p^3, 3p^3...p^{r-1}, 2p^{r-1}, ...pp^{r-1}\}$$

We can see this set has p^{r-1} elements and so the set of values with $gcd(g, p^r) = 1$ has $p^r - p^{r-1}$ elements. Thus by definition, $\mathbb{Z}_{p^r}$ has $p^r - p^{r-1}$ elements.

4.3.2.d

evaluate (1423)(34)(56)(1324)*.*

To evaluate this composition of cycles, I will first name each one and then list out the full mapping for each cycle as I'm still getting used to cycle notation.

$$\delta = (1432) \quad \gamma = (34) \quad \beta = (56) \quad \alpha = (1324)$$

And the mappings are:

$$\begin{array}{cccc}
\delta(1) = 4 & \gamma(1) = 1 & \beta(1) = 1 & \alpha(1) = 3 \\
\delta(2) = 3 & \gamma(2) = 2 & \beta(2) = 2 & \alpha(2) = 4 \\
\delta(3) = 1 & \gamma(3) = 4 & \beta(3) = 3 & \alpha(3) = 2 \\
\delta(4) = 2 & \gamma(4) = 3 & \beta(4) = 4 & \alpha(4) = 1 \\
\delta(5) = 5 & \gamma(5) = 5 & \beta(5) = 6 & \alpha(5) = 5 \\
\delta(6) = 6 & \gamma(6) = 6 & \beta(6) = 5 & \alpha(6) = 6
\end{array}$$

Thus we have that the following is the mapping for the composition of cycles $\delta\gamma\beta\alpha$:

$$\begin{array}{c}
\delta\gamma\beta\alpha(1) = \delta\gamma\beta(3) = \delta\gamma(3) = \delta(4) = 2 \\
\delta\gamma\beta\alpha(2) = \delta\gamma\beta(4) = \delta\gamma(4) = \delta(3) = 1 \\
\delta\gamma\beta\alpha(3) = \delta\gamma\beta(2) = \delta\gamma(2) = \delta(2) = 3 \\
\delta\gamma\beta\alpha(4) = \delta\gamma\beta(1) = \delta\gamma(1) = \delta(1) = 4 \\
\delta\gamma\beta\alpha(5) = \delta\gamma\beta(5) = \delta\gamma(6) = \delta(6) = 6 \\
\delta\gamma\beta\alpha(6) = \delta\gamma\beta(6) = \delta\gamma(5) = \delta(5) = 5
\end{array}$$

From this mapping we can see that 3 and 4 are fixed and therefore this cycle is equivalent to:

$$\delta\gamma\beta\alpha = (12)(56)$$

5.3.3.d

Express the following permutation as a product of transpositions and identify then as even or odd

To begin we will first simplify the cycle as much as possible.

$$\rho = (17254) \quad \tau = (1423) \quad \sigma = (154632)$$

$$\begin{aligned} \rho(1) &= 7 & \tau(1) &= 4 & \sigma(1) &= 5 \\ \rho(2) &= 5 & \tau(2) &= 3 & \sigma(2) &= 1 \\ \rho(3) &= 3 & \tau(3) &= 1 & \sigma(3) &= 2 \\ \rho(4) &= 1 & \tau(4) &= 2 & \sigma(4) &= 6 \\ \rho(5) &= 4 & \tau(5) &= 5 & \sigma(5) &= 4 \\ \rho(6) &= 7 & \tau(6) &= 6 & \sigma(6) &= 3 \\ \rho(7) &= 2 & \tau(7) &= 7 & \sigma(7) &= 7 \end{aligned}$$

$$\begin{aligned} \rho\tau\sigma(1) &= \rho\tau(5) = \rho(5) = 4 \\ \rho\tau\sigma(2) &= \rho\tau(1) = \rho(4) = 1 \\ \rho\tau\sigma(3) &= \rho\tau(2) = \rho(3) = 3 \\ \rho\tau\sigma(4) &= \rho\tau(6) = \rho(6) = 6 \\ \rho\tau\sigma(5) &= \rho\tau(4) = \rho(2) = 5 \\ \rho\tau\sigma(6) &= \rho\tau(3) = \rho(1) = 7 \\ \rho\tau\sigma(7) &= \rho\tau(7) = \rho(7) = 2 \end{aligned}$$

$$\rho\tau\sigma = (14672)$$

Now that we have one cycle, we can easily decompose it as follows:

$$(14672) = (12)(17)(16)(14)(31)(13)(51)(15)$$

Counting the number of 2-cycles gives that the original cycle must be an even permutation.

5.3.4

Find $(a_1a_2a_3...a_{n-1}a_n)^{-1}$.

Let $\sigma = (a_1a_2a_3...a_{n-1}a_n)$. I claim that $\sigma^{-1} = (a_na_{n-1}...a_3a_2a_1) = (a_1a_na_{n-1}...a_3a_2)$ is the inverse to σ. Let $x = a_i$ then $\sigma(a_{i-1}) = a_i$ and so $\sigma^{-1}(a_i) = a_{i-1}$ hence, the 'reverse order' of σ^{-1}. For $x = a_1$ we have the special case of $\sigma(a_k) = a_1$ and so by definition $\sigma^{-1}(a_1) = a_k$ if $x \neq a_i$ then $\sigma(x) = x$ which implies $\sigma^{-1}(x) = x$. Thus σ^{-1} is the inverse for σ because:

$$\begin{aligned} \sigma^{-1}\sigma(a_{i-1}) &= \sigma^{-1}(a_i) = a_{i-1} \\ \sigma\sigma^{-1}(a_i) &= \sigma(a_{i-1}) = a_i \end{aligned}$$

So every element maps to itself, i.e. $\sigma\sigma^{-1} = \sigma^{-1}\sigma = id$

5.3.18

Show A_n is non-Abelian for $n \geq 4$.

Note that it is sufficient to find two examples from A_4 that do not commute because if they are in A_4 they must also be in every A_n with $r \geq 4$. Let us examine the even permutations $\alpha = (123) = (13)(12)$ and $\beta = (234) = (24)(23)$.

$$\begin{aligned} \alpha\beta = (123)(234) &= (12)(34) \\ \beta\alpha = (234)(123) &= (13)(24) \\ &\Rightarrow \alpha\beta \neq \beta\alpha \end{aligned}$$

Thus since $\alpha, \beta \in A_n, n \geq 4$ we have that A_n is non-Abelian.