# Abstract Problem Set 5

Rippy

March 2019

## 1 Problems

### 1.1 Problem 1

Let G be a group. Dene the group $\text{Aut}(G) := \{\phi : G \to G \mid \phi \text{ is an isomorphism}\}$. Prove that $\text{Aut}(G)$ is a group with composition as the operation.

*Proof.* $\text{Aut}(G)$ is associative, as we know function composition is associative by Theorem 2.29.

Let $\alpha, \phi \in \text{Aut}(G)$. By Theorem 3.54, we know if $\alpha, \phi$ are isomorphisms, then their composite function will also be an isomorphism. We also know by Theorem 3.54, if $\alpha$ maps $G_1 \to G_2$ and $\phi$ maps $G_2 \to G_3$, their composite function will map $G_1 \to G_3$. Since both $\alpha, \phi$ map $G \to G$, their composition $\in \text{Aut}(G)$, thus $\text{Aut}(G)$ is closed.

Let $\alpha \in \text{Aut}(G)$ and $g \in G$, such that $\alpha(g) = g$. (Identity mapping) Thus, the identity $\in \text{Aut}(G)$, and $G$ is nonempty.

By Theorem 3.53, if the function $\phi : G_1 \to G_2$ is an isomorphism, then the function $\phi^{-1} : G_2 \to G_1$ is also an isomorphism. Thus, since $\phi$ maps $G \to G$, $\phi^{-1}$ will also map $G \to G$. Thus since $\phi^{-1}$ is an isomorphism, and maps $G \to G$, it exists within $\text{Aut}(G)$, proving inverses.

Thus, since $\text{Aut}(G)$ is Associative, contains inverses, contains the identity, is nonempty, and is closed, $\text{Aut}(G)$ is a group.

□

## 1.2 Problem 2

Show that a group $G$ has finitely many subgroups if and only if $G$ is finite.

*Proof.* Claim: If $G$ is finite, then $G$ has finitely many subgroups. If $G$ is finite, then there exists a finite amount of elements within $G$. If there is a finite amount of elements, then there is a finite amount of subsets that can be created with those elements. Because a subgroup is also a subset, this implies that there must also be a finite amount of subgroups. Thus, if $G$ is finite, $G$ has finitely many subgroups.

Claim: If $G$ has finitely many subgroups, then $G$ is finite.

Say a cyclic subgroup of $G$ was infinite, then it is isomorphic to $\mathbb{Z}$. $\mathbb{Z}$ has infinite subgroups, thus the cyclic subgroup in question would also have infinite subgroups. However, there are finitely many subgroups in $G$, thus any cyclic subgroup of $G$ must be finite. We know $G$ is a union of proper subgroups if and only if $G$ is not cyclic, then if $G$ is not cyclic, $G$ must be a union of proper subgroups. Because the cyclic subgroups generated by each element of $G$ must be finite, and $G$ can be created by a finite amount of unions of finite cyclic subgroups generated by each element, $G$ must be finite.

On the other hand, if $G$ is cyclic, and infinite, then $G$ is isomorphic to $\mathbb{Z}$. Since we know that $\mathbb{Z}$ has an infinitely many subgroups, $n\mathbb{Z}$, then if $G$ is infinite and cyclic, $G$ has infinitely many subgroups. Since $G$ is cyclic and has finitely many subgroups, then $G$, by the contrapositive, must be finite. Thus, if $G$ has finitely many subgroups, then $G$ is finite. □

## 1.3 Problem 3

(a) Find all elements in the subgroup $\langle 30 \rangle$ inside $\mathbb{Z}_{42}$.

(b) Find the elements in $U_{20}$ and find the subgroup $\langle 7 \rangle$ inside $U_{20}$.

(c) Let $p$ be a prime. Find the number of generators of $\mathbb{Z}_{p^r}$, where $r$ is an integer greater than or equal to 1.

(d) Give an example of (or explain why no example exists) a finite cyclic group with 4 distinct generators and an infinite cyclic group with 4 distinct generators.

*Proof.* (a)
$\langle 30 \rangle = \{30, 18, 6, 36, 24, 12, 0\} \in \mathbb{Z}_{42}$ □

*Proof.* (b)
$U_{20} = \{1, 3, 7, 9, 11, 13, 17, 19\}$
$\langle 7 \rangle = \{1, 7, 9, 3, \} \in U_{20}$ □

*Proof.* (c)

The number of generators for $Z_{p^r} = p^r - p^{r-1}$. There are $p^r$ elements in $Z_{p^r}$ that could possibly generate the group. Then we must subtract all elements that are not relatively prime to the modulo, $p^r$, which is multiples of $p^r$. Thus, the number of these non-generating elements is given by $p^{r-1}$, so the total number of generators is (total number of elements) - (non-generating elements), which is $p^r - p^{r-1}$.

□

*Proof.* (d)

All infinite cyclic groups are isomorphic to $\mathbb{Z}$. Because $\mathbb{Z}$ only has two distinct generators, in order to remain isomorphic, all other infinite cyclic groups must also only have two generators. Thus, there is no infinite cyclic group with four distinct generators.

$\mathbb{Z}_8 = \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle$

$\mathbb{Z}_8$ is finite and cyclic, and there are exactly four generators.

□

## 1.4 Problem 4

(a) Write the following permutation in cycle notation:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 2 & 4 & 8 & 3 & 1 & 7 \end{pmatrix}$$

(b) Find the maximum possible order of an element in $S_5$ and $S_7$.

(c) Find a 1-1 homomorphism from $\mathbb{Z}_n$ to $S_n$ and from $S_{n-1}$ to $S_n$. (The former shows that an isomorphic copy of a finite cyclic group can be found inside a symmetric group. The latter shows, by induction, that the symmetric group $S_n$ contains an isomorphic copy of $S_k$ for all $1 \leq k \leq n$.)

*Proof.* (a)
$(1, 5, 8, 7)(6, 3, 2)$ □

*Proof.* (b)
Maximum order of an element in $S_5 = 6$, Maximum order of an element in $S_7 = 12$.
An element in $S_n$ must have its disjoint cycle lengths add to $n$. Meaning, for $S_5$, the disjoint cycles of an element in $S_5$ must add to 5. To find the order of the element, find the least common multiple, by multiplying the lengths of each of the disjoint cycle that compose the element together. So, the numbers that 5 can be split into that when multiplied yield the highest number are 2 and 3, and $2 * 3 = 6$, thus the maximum order of an element in $S_5 = 6$. Similarly, 7 can be split into 3 and 4, and $3 * 4 = 12$, thus the maximum order of an element in $S_7 = 12$.

□

*Proof.* (c)

Let $\sigma \in S_n$ be the cycle $(1, 2, \ldots, n)$. Let $a \in \mathbb{Z}_n$ and $\phi(a) = \sigma^a$

Let $a, b \in Z_n$
$\phi(a + b) = \sigma^{a+b} = \sigma^a \sigma^b = \phi(a)\phi(b)$ thus $\phi$ is homomorphic.

$\phi(a) = \phi(b)$
$\sigma^a = \sigma^b$
$\sigma^a \sigma^{-b} = e$
$\sigma^{a-b} = \sigma_e$
$a - b = kn$
Thus $a = kn + b$, since $a, b \in \mathbb{Z}_n$, $b$ modn $= b$ and $a$ modn $= b$, thus $a = b$
Thus $\phi$ is 1-1

Let $\alpha \in S_{n-1}$, let $\phi(\alpha) = (\alpha)(n) \in S_n$
Let $\alpha, \beta \in S_{n-1}$
$\phi(\alpha\beta) = (\alpha)(\beta)(n) = (\alpha)(\beta)(n)^2 = (\alpha)(n)(\beta)(n) = \phi(\alpha)\phi(\beta)$, thus $\phi$ is homomorphic.
$\phi(\alpha) = \phi(\beta)$
$(\alpha)(n) = (\beta)(n)$
$\alpha = \beta$

□