MATH 1530 Problem Set 3

Tanish Makadia
(Collaborated with Esmé and Kazuya)

February 2023

Problem 1. Consider $U(40)$. Find a subgroup which is cyclic of order 4. Find a subgroup which is noncyclic of order 4.

Proof. $U(40)$ is defined as follows:

$$U(40) = \{1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39\}$$

- **Cyclic subgroup:** We will create a cyclic subgroup of order 4 using 7 as the generator.

$$\langle 7 \rangle = \{7, 9, 23, 1\} \qquad \text{(Gallian, 3.4)}$$

- **Non-cyclic subgroup:** We will show that $\{1, 9, 11, 19\}$ is a noncyclic subgroup.

Cayley Table:

	1	9	11	19
1	1	9	11	19
9	9	1	19	11
11	11	19	1	9
19	19	11	9	1

Since $\{1, 9, 11, 19\}$ is finite and closed under multiplication mod 40, we have proven that it is subgroup of $U(40)$. Additionally, since $|9| = |11| = |19| = 2$, there is no element in this group which can generate the entire group, proving that it is noncyclic.

□

Problem 2. If H and K are subgroups of a group G, prove that $H \cap K$ is a subgroup of G. If $H \not\subset K$ and $K \not\subset H$, prove that $H \cup K$ is never a subgroup of G.

1. $H \cap K$ is a subgroup of G.

Proof. We will use the two-step subgroup test.

- **Closed over inverses:** $x \in H \cap K \implies x \in H$ and $x \in K$. Since H and K are subgroups, we have the existence of $x^{-1} \in H$ and $x^{-1} \in K \implies x^{-1} \in H \cap K$.
- **Closed under group operation:** $a, b \in H \cap K \implies a, b \in H$ and $a, b \in K$. Since H and K are subgroups, we have that $ab \in H$ and $ab \in K \implies ab \in H \cap K$.

□

2. If $H \not\subset K$ and $K \not\subset H$, $H \cup K$ is never a subgroup of G.

Proof. We will show that $H \cup K$ is not closed under the group operation. Since neither H nor K are subsets of each other, we have the existence of some $a, a^{-1} \in H \setminus K$ and $b, b^{-1} \in K \setminus H$.

If $H \cup K$ is a subgroup, it must be closed. This implies that $ab \in H \cup K \implies ab \in H$ or $ab \in K$. Thus, we have two cases:

- Case 1 ($ab \in H$): Since H is closed, $a^{-1} \cdot ab \in H \implies b \in H$. This is a contradiction.
- Case 2 ($ab \in K$): Since K is closed, $ab \cdot b^{-1} \in K \implies a \in K$. This is a contradiction.

Because both cases lead to a contradiction, we have proven that $H \cup K$ is not closed and is therefore not a subgroup. □

Problem 3. Prove that a group G is Abelian if and only if $G = Z(G)$.

Proof. $\Rightarrow$ Assume G is an Abelian group. Of course, $Z(G) \subset G$ by definition. Since G is Abelian, $a \in G \implies ax = xa$ for all $x \in G \implies a \in Z(G)$. Therefore, $G \subset Z(G)$, completing the double inclusion.

$\Leftarrow$ Assume $G = Z(G)$. Thus, $a \in G \implies a \in Z(G) \implies ax = xa$ for all $x \in G$. Therefore, G must be Abelian. $\square$

Problem 4. Suppose G is a group with exactly 8 elements of order 3. how many subgroups of order 3 does G have?

Proof. Let $H \subset G$ be a subgroup of order 3:

$$H = \{e, a, b\}$$

Since e is unique, we have that $ab \neq a$ and $ab \neq b$. In order for H to be closed, the only remaining choice is $ab = e$. Thus, for any subgroup of order 3, the two elements besides the identity must be each other's inverse.

Now, we will show that $|a| = |b| = 3$. Consider $a^2 \in H$. Since identities and inverses are unique, $a^2 \neq a$ and $a^2 \neq e$. The only remaining choice is $a^2 = b$. Therefore,

$$\begin{aligned} a^3 &= a \cdot a^2 & \qquad b^3 &= (a^2)^3 \\ &= a \cdot b & &= (a^3)^2 \\ &= e & &= e \end{aligned}$$

We have that there are exactly 8 elements of G of order 3. Because a subgroup of order 3 requires two distinct elements of order 3, we can conclude that the number of distinct subgroups of order 3 in G is $8/2 = 4$. □

Problem 5. Let G be a finite group with more than one element. Show that G has an element of prime order.

Proof. Let $a \in G$ such that $a \neq e$. Let $|a| = n$ where n is the smallest positive integer such that $a^n = e$ (such an integer exists because G is finite).

Because a is not the identity, we have that $n > 1$. By the fundamental theorem of arithmetic, n can be separated into a unique product of primes $p_1 \cdots p_m$:

$$\begin{aligned} e &= a^n && \text{(definition of order)} \\ &= a^{p_1 \cdots p_m} && \text{(fundamental theorem of arithmetic)} \\ &= (a^{p_1 \cdots p_{m-1}})^{p_m} && \text{(power rule for exponents)} \end{aligned}$$

Let $b = a^{p_1 \cdots p_{m-1}}$. We have that $b \in G$ because $b \in \langle a \rangle \subset G$. Thus, we have that $b^{p_m} = e$. We will now show that $|b| = p_m$.

$$\begin{aligned} |b| &= |a^{p_1 \cdots p_{m-1}}| && \text{(definition of } b\text{)} \\ &= n/\gcd(n, p_1 \cdots p_{m-1}) && \text{(Gallian, 4.2)} \\ &= p_1 \cdots p_m / \gcd(p_1 \cdots p_m, p_1 \cdots p_{m-1}) && (n = p_1 \cdots p_m) \\ &= p_1 \cdots p_m / p_1 \cdots p_{m-1} && \text{(definition of } \gcd\text{)} \\ &= p_m && \text{(division)} \end{aligned}$$

Therefore, we have proven that G has an element of prime order. □