

Modern Algebra I – Homework 3

Junwoo Yang

April 3, 2019

Problem 1. Find all generators of \mathbb{Z}_6 , \mathbb{Z}_8 , \mathbb{Z}_{20} .

Proof. If n is generator of \mathbb{Z}_k , then $\gcd(n, k) = 1$ for $n \in \mathbb{Z}_k$.

(1) $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$. $\langle 1 \rangle = \langle 5 \rangle = \mathbb{Z}_6$.

\therefore generators of $\mathbb{Z}_6 = \{1, 5\}$.

(2) $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$. $\langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle = \mathbb{Z}_8$.

\therefore generators of $\mathbb{Z}_8 = \{1, 3, 5, 7\}$.

(3) $\mathbb{Z}_{20} = \{0, 1, 2, \dots, 19\}$.

\therefore generators of $\mathbb{Z}_{20} = \{1, 3, 7, 9, 11, 13, 17, 19\}$. ■

Problem 2. List the elements of the subgroups $\langle 3 \rangle$, $\langle 7 \rangle$ in $U(20)$.

Proof. $U(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$.

$\therefore \langle 3 \rangle = \{1, 3, 9, 7\}$, $\langle 7 \rangle = \{1, 7, 9, 3\}$. ■

Problem 3. Let a be an element of a group and let $|a| = 15$. Compute the orders of a^3 , a^5 , a^6 , a^{10} of G .

Proof. $|a| = 15 \Rightarrow a^{15} = e$. $(a^3)^5 = (a^5)^3 = (a^6)^5 = (a^{10})^3 = e$.
 $\therefore |a^3| = 5$, $|a^5| = 3$, $|a^6| = 5$, $|a^{10}| = 3$. ■

Problem 4. In \mathbb{Z}_{24} list all generators for the subgroup of order 8. Let $G = \langle a \rangle$ and let $|a| = 24$. List all generators for the subgroup of order 8.

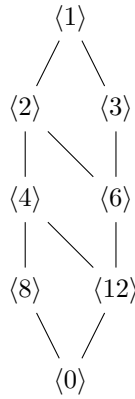
Proof. $\mathbb{Z}_{24} = \langle 1 \rangle$ is cyclic group of order 24. Subgroup of order 8 is $|\langle 1^k \rangle| = \frac{24}{\gcd(24, k)} = 8$. $\gcd(24, k) = 3$. Therefore $k = 3, 9, 15, 21$. $\langle 3 \rangle = \langle 9 \rangle = \langle 15 \rangle = \langle 21 \rangle$. All generators of $\langle 3 \rangle$ are of the form $k \cdot 3$ where $\gcd(8, k) = 1$. Thus, $k = 1, 3, 5, 7$ and the generators of $\langle 3 \rangle$ are $3, 9, 15, 21$. In $\langle a \rangle$, there is a unique subgroup of order 8 which is $\langle a^3 \rangle = \langle a^9 \rangle = \langle a^{15} \rangle = \langle a^{21} \rangle$. All generators of $\langle a^3 \rangle$ are of the form $(a^3)^k$ where $\gcd(8, k) = 1$. Therefore, $k = 1, 3, 5, 7$ and the generators of $\langle a^3 \rangle$ are a^3, a^9, a^{15} , and a^{21} . ■

Problem 5. Determine the subgroup lattices for \mathbb{Z}_{24} .

Proof. Subgroup of \mathbb{Z}_{24} are

$$\{0, 1, 2, \dots, 23\}, \{0, 2, 4, \dots, 22\}, \{0, 3, 6, \dots, 21\}, \{0, 4, 8, \dots, 22\}, \\ \{0, 6, 12, 18\}, \{0, 8, 16\}, \{0, 12\}, \{0\}.$$

The lattices is



■

Problem 6. Let p be a prime number. Find the number of generators of the cyclic group \mathbb{Z}_{p^r} , where r is a positive integer.

Proof. For any x in the set of generators of \mathbb{Z}_{p^r} , $\gcd(x, p^r) = 1$. Since p is prime, $x \in \mathbb{Z}_{p^r}$. If $\gcd(x, p^r) \neq 1$, then $x = np$ for $n = 0, 1, \dots$.

$$\therefore \underbrace{0, p, 2p, \dots, p^r - p}_{p^{r-1} - 1} \text{ are not generator.}$$

Therefore, the number of generators of \mathbb{Z}_{p^r} is $|\mathbb{Z}_{p^r}| - (p^{r-1} - 1 + 1) = p^r - p^{r-1}$. ■

Problem 7. Show that \mathbb{Z}_p has no proper nontrivial subgroups if p is a prime number.

Proof. $\mathbb{Z}_p = \{0, 1, 2, \dots, p-1\}$. For all $x \in \mathbb{Z}_p \setminus \{0\}$, $\gcd(x, p) = 1$. Thus, all x are generator,

$$|\langle x \rangle| = |x| = \frac{p}{\gcd(x, p)} = \frac{p}{1} = p.$$

Since \mathbb{Z}_p is cyclic, H must be cyclic. Thus, $H = \langle a \rangle$ for $a \in \mathbb{Z}_p$.

(i) $a = 0$, H is trivial subgroup.

(ii) $a \neq 0$, $a \in \mathbb{Z}_p^*$, $|H| = |\langle a \rangle| = |a| = p = |\mathbb{Z}_p| \Rightarrow H = \mathbb{Z}_p$.

Therefore, subgroup of \mathbb{Z}_p is always either $\{0\}$ or \mathbb{Z}_p . ■

Problem 8. Let a and b be elements of a group. If $|a| = 10$ and $|b| = 21$, show that $\langle a \rangle \cap \langle b \rangle = \{e\}$.

Proof. $\langle a \rangle \cap \langle b \rangle$ is a group. Let $c \in \langle a \rangle \cap \langle b \rangle$. Then, $c \in \langle a \rangle$, $c \in \langle b \rangle$. Thus, $|c| \mid \gcd(10, 21) = 1 \Rightarrow |c| = 1$. So, $c' = c = e$. Therefore, only elements of $\langle a \rangle \cap \langle b \rangle$ is e . ■

Problem 9. Suppose that $|x| = n$. Find a necessary and sufficient condition on r and s such that $\langle x^r \rangle \subseteq \langle x^s \rangle$.

Proof. $\langle x^r \rangle \subseteq \langle x^s \rangle$ if and only if $x^r \in \langle x^s \rangle$. $|x^s| = \frac{n}{(n,s)} \mid n$. $\langle x^s \rangle = \langle x^{(n,s)} \rangle = \{1, x^{(n,s)}, x^{2(n,s)}, \dots\}$.

$$\therefore \forall k \mid n, \text{ subgroup of } \langle a \rangle : \left\{ 1, a^{\frac{n}{k}}, a^{\frac{2n}{k}} \dots a^{\frac{(k-1)n}{k}} \right\} = \langle a^{\frac{n}{k}} \rangle.$$

$$\therefore x^r \in \langle x^s \rangle = \langle x^{(n,s)} \rangle \Leftrightarrow (n,s) \mid r. \quad \blacksquare$$