Abstract Algebra HW3

Yu Fan Mei · MATH-3210

2. Find the order of each of the following elements.

Problem 2.1. $5 \in \mathbb{Z}_{12}$.

- The order of $5 \in \mathbb{Z}_{12}$ is $\frac{12}{\texttt{gcd}(5,12)} = \frac{12}{1} = 12$.

Problem 2.2. $\sqrt{3} \in \mathbb{R}$.

- We will prove that the order is infinite via contradiction. Suppose the order of $\sqrt{3}$ is finite. This would mean there exists a positive integer k such that $k\sqrt{3} = 0$.
- Dividing both sides of this equality by $\sqrt{3}$, we get $k = 0$, which contradicts the statement that $k > 0$. This means $\sqrt{3}$ must be infinite.

Problem 2.3. $\sqrt{3} \in \mathbb{R}*$.

- We will prove that the order is infinite, also via contradiction. Suppose the order of $\sqrt{3}$ in the group $\mathbb{R}*$ was finite. Then there exists a positive integer k such that $\sqrt{3}^k = 1$.
- Taking the natural logarithm of both sides, we get $k \ln \sqrt{3} = 0$. From this, we get $k = 0$, which is a contradiction.

Problem 2.4. $-i \in \mathbb{C}*$.

- The order of $-i$ in the group of complex numbers under multiplication is 4.
- $(-i)^2 = -1$, and $(-i)^3 = i$. $(-i)^4 = 1$.

Problem 2.5. $72 \in \mathbb{Z}_{240}$.

- The order of $72 \in \mathbb{Z}_{240}$ is $\frac{240}{\texttt{gcd}(240,72)}$.
- The gcd of 240 and 72 is 24:

$$\begin{aligned} 240 &= 72(3) + 24 \\ 72 &= 24(3) + 0. \end{aligned}$$

- So, the order of $72 \in \mathbb{Z}_{240}$ is $\frac{240}{24} = 10$.

Problem 2.6. $312 \in \mathbb{Z}_{471}$.

- The order of 312 in $\mathbb{Z}_{471}$ is $\frac{471}{\texttt{gcd}(471,312)}$.
- And the greatest common divisor of 471 and 312 is 1:

$$\begin{aligned} 471 &= 312(1) + 59 \\ 312 &= 59(5) + 17 \\ 59 &= 17(3) + 8 \\ 17 &= 8(2) + 1 \\ 8 &= 1(8) + 0. \end{aligned}$$

- This means the order of $312 \in \mathbb{Z}_{471}$ is 471.

3. List all of the elements in each of the following subgroups.

Problem 3.1. The subgroup of $\mathbb{Z}$ generated by 7.

- The elements in this subgroup are $\{..., -14, -7, 0, 7, 14, ...\}$.
- This subgroup is infinite.

Problem 3.2. The subgroup of $\mathbb{Z}_{24}$ generated by 15.

- The subgroup is $\{15, 6, 21, 12, 3, 18, 9, 0\}$.

Problem 3.3. All subgroups of $\mathbb{Z}_{12}$.

- The subgroups of $\mathbb{Z}_{12}$ are:
  - $\langle 0 \rangle = \{0\}$
  - $\langle 1 \rangle = \{1, 2, 3, ..., 11, 0\}$
  - $\langle 2 \rangle = \{2, 4, 6, 8, 10, 0\}$
  - $\langle 3 \rangle = \{3, 6, 9, 0\}$
  - $\langle 4 \rangle = \{4, 8, 0\}$
  - $\langle 6 \rangle = \{6, 0\}$

Problem 5. Find the order of every element in $\mathbb{Z}_{18}$.

- The order of any element $k \in \mathbb{Z}_{18}$ is given by $\frac{18}{\texttt{gcd}(k,18)}$.

- $\text{ord}(1) = 18$
- $\text{ord}(2) = 9$
- $\text{ord}(3) = 6$
- $\text{ord}(4) = 9$
- $\text{ord}(5) = 18$
- $\text{ord}(6) = 3$
- $\text{ord}(7) = 18$
- $\text{ord}(8) = 9$
- $\text{ord}(9) = 2$
- $\text{ord}(10) = 9$
- $\text{ord}(11) = 18$
- $\text{ord}(12) = 3$
- $\text{ord}(13) = 18$
- $\text{ord}(14) = 9$
- $\text{ord}(15) = 6$
- $\text{ord}(16) = 9$
- $\text{ord}(17) = 18$
- $\text{ord}(0) = 1$

Problem 26. Prove that $\mathbb{Z}_p$ has no nontrivial subgroups if p is prime.

- Let $\mathbb{Z}_{p_0}$ be the additive group of integers mod p_0 such that p_0 is a prime integer.
- Let H_0 be any subgroup of $\mathbb{Z}_{p_0}$. Since every subgroup of a cyclic group is also cyclic, this means there exists an integer $k_0 \in \mathbb{Z}_{p_0}$ such that k_0 generates H_0, or in other words, $\langle k_0 \rangle = H_0$.
- Because $\mathbb{Z}_{p_0}$ is a modulus group, we know $0 \leq k_0 < p_0$. If $k_0 = 0$, this means $H_0 = \{0\}$, which is a trivial subgroup. Let's suppose $0 < k_0 < p_0$. Then the order of k_0 is

$$\begin{aligned} ord(k_0) &= \frac{p_0}{\texttt{gcd}(k_0, p_0)} \\ &= \frac{p_0}{1} \\ &= p_0. \end{aligned}$$

- The above is true because p_0 is prime, so its greatest common divisor with k_0 is 1 because $0 < k_0 < p_0$. Since the order of k_0 is p_0, this means $|H_0| = |\mathbb{Z}_{p_0}|$.
- Following from this and using the fact that H_0 is a subgroup, this must mean H_0 is the subgroup with all the elements in $\mathbb{Z}_{p_0}$, which is a trivial subgroup.

Problem 28. Let a be a generator in group G. What is a generator for $\langle a^m \rangle \cap \langle a^n \rangle$?

- A generator for $\langle a^m \rangle \cap \langle a^n \rangle$ would be $\langle a^{\texttt{lcm}(m,n)} \rangle$, and we'll show this by proving equality of subgroups.
- Set $x_0 = \texttt{lcm}(m, n)$, and set $H = \langle a^{x_0} \rangle$. We will prove $H \subseteq \langle a^m \rangle \cap \langle a^n \rangle$ and $H \supseteq \langle a^m \rangle \cap \langle a^n \rangle$. Because of how we defined x_0, there exist integers k_1, k_2 such that $x_0 = k_1 m = k_2 n$.
- Let $h_0 \in H$. Then there exists $l \in \mathbb{Z}$ such that $h_0 = a^{x_0 l}$. Since $x_0 = k_1 m = k_2 n$, we can see that $h_0 = a^{k_1 l m} \in \langle a^m \rangle$ and $h_0 = a^{k_2 l n} \in \langle a^n \rangle$. Thus, $H \subseteq \langle a^m \rangle \cap \langle a^n \rangle$.
- Let $j_0 \in \langle a^m \rangle \cap \langle a^n \rangle$. Then there exist integers s_1, s_2 such that $j_0 = a^{m s_1} = a^{n s_2}$. This means $m s_1 = n s_2$. But this also means $j_0 = a^{m x_0 t}$, where $t \in \mathbb{Z}$.
- Rewriting the last equality, we can see that $j_0 = (a^{x_0})^{mt}$. This means $j_0 \in H$, and thus $a^{\texttt{lcm}(m,n)}$ is a generator.

Problem 30. Suppose G is a group and let $a, b \in G$. Prove that if $|a| = m$ and $|b| = n$ with $\texttt{gcd}(m, n) = 1$, then $\langle a \rangle \cap \langle b \rangle = \{e\}$.

- Let $x_0 \in \langle a \rangle \cap \langle b \rangle$. By definition, there exist integers $k_1 < m$ and $k_2 < n$ such that $x_0 = a^{k_1} = b^{k_2}$. Since $\langle a \rangle$ and $\langle b \rangle$ have finite orders, they are also cyclic. Because it is a cyclic group, if we were to pick $k_1 \geq m$, you could rewrite a^{k_1} as $a^{k_1 \mod m}$. This is also true for k_2 and n.
- This means $\langle a^m \rangle = \langle b^n \rangle = e$. From this, it follows that $x_0^{k_1 m} = x_0^{k_2 n} = e$. This means $k_1 m = k_2 n$.
- We know $m, n > 0$, because they are orders of a and b. Since $\texttt{gcd}(m, n) = 1$, and because of our restrictions on k_1 and k_2, this means $k_1 = k_2 = 0$. This means $x_0 = e$.