Math 307 Abstract Algebra Homework 9 **Sample solution**

1. Suppose G is an Abelian group. Show that $H = \{g \in G : |g| \text{ is finite}\}$ is a subgroup.

   Solution. Let $H = \{g \in G : |g| \text{ is finite}\}$. We have $e \in H$ because $|e| = 1$. If $a, b \in H$, then $|a| = n$ and $b| = m$ for some $n, m \in \mathbb{N}$. By commutativity, $(ab^{-1})^{nm} = a^{mn}(b^{-1})^{mn} = e^m e^n = e$. Thus ab^{-1} has finite order, and belongs to H. Hence, H is a subgroup.

2. Suppose G is a finite Abelian group, and $m||G|$. Show that G has a subgroup of order m.

   Up to isomorphism, we may assume $G = \mathbb{Z}_{p_1^{r_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{r_k}}$, where $p_1, \ldots, p_k$ are primes, so that $n = p_1^{r_1} \cdots p_k^{r_k}$. If $m|n$, we may assume that $m = p_1^{t_1} \cdots p_k^{t_k}$ with $0 \le t_j \le r_j$ for $j = 1, \ldots, k$. Now, for every cyclic group $\mathbb{Z}_{p_j^{r_j}}$, we can find a subgroup H_j of order $p_j^{t_j}$. It follows that $H_1 \oplus \cdots \oplus H_k$ in G with order m.

3. (10 points) Compare the number of isomorphic classes of subgroups of an Abelian group of orders m and n for each of the following if p, q are primes, and $r \in \mathbb{N}$.

   (a) $n = 3^2, m = 5^2$. (b) $n = 2^4, m = 5^4$, (c) $n = p^r, m = q^r$,

   (d) $n = p^r$ and $m = p^r q$, (e) $n = p^r$ and $m = p^r q^2$.

   Solution. (a) and (b) follow from (c).

   (c) Every isomorphic class of G_1 has the form $\mathbb{Z}_{p^{r_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{r_k}}$ with $r_1 \ge \cdots \ge r_k > 0$ such that $r = r_1 + \cdots + r_k$, It will correspond to the isomorphic class of G_2 of the form $\mathbb{Z}_{q^{r_1}} \oplus \cdots \oplus \mathbb{Z}_{q^{r_k}}$, and vice versa. Thus, G_1 and G_2 have the same number of isomorphic classes of groups.

   (d) Every isomorphic class of G_1 has the form $\mathbb{Z}_{p^{r_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{r_k}}$ with $r_1 \ge \cdots \ge r_k > 0$ such that $r = r_1 + \cdots + r_k$, It will correspond to an isomorphic class of G_2 of the form Thus, G_1 and G_2 have the same number of the isomorphic classes of groups.

   (e) Every isomorphic class of G_1 has the form $\mathbb{Z}_{p^{r_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{r_k}}$ with $r_1 \ge \cdots \ge r_k > 0$ such that $r = r_1 + \cdots + r_k$, It will correspond to two isomorphic class of G_2 of the form $\mathbb{Z}_{p^{r_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{r_k}} \oplus \mathbb{Z}_{q^2}$ and $\mathbb{Z}_{p^{r_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{r_k}} \oplus \mathbb{Z}_q \oplus \mathbb{Z}_q$, and vice versa. Thus, G_2 has twice the number of isomorphic classes of groups as G_1.

4. (a) Give an example of a subset of a ring that is a subgroup under addition but not a subring.

   (b) Give an example of a finite non-commutative ring.

   Solution. (a) Example 1. Let $R = \mathbb{C}$ and $S = \{ix : x \in \mathbb{R}\}$. Then $0 \in S$ and $a - b \in S$ whenever $a, b \in S$. But $i \cdot i = -1 \notin S$.

   Example 2. Let $H = \langle (2, 3) \rangle \in \mathbb{Z} \oplus \mathbb{Z}$. Then $H = \{(2k, 3k) : k \in \mathbb{Z}\}$ is a subgroup under addition. But $(2, 3)(2, 3) = (4, 9) \notin H$.

   (b) Let $R = M_2(\mathbb{Z}_2)$. Then there are 2^4 elements because each entries has two choices. Clearly, $AB \ne BA$ if $A = B^t = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$.

   If we consider the subring S of R consisting of matrices with the second row equal zero. Then S has four elements and is not commutative.

5. Show that if m, n are integers and a, b are elements in a ring. Then $(ma)(nb) = (mn)(ab)$. [Note that for positive m, $ma = a + \cdots + a$ (m times and $(-m)a = m(-a)$.]

Solution. If m or n is zero, then both sides equal 0. If $m, n \in \mathbb{N}$, then

$$(\underbrace{a + \cdots + a}_{m})(\underbrace{b + \cdots + b}_{n}) = (\underbrace{ab + \cdots + ab}_{mn}) = (mn)(ab).$$

If m is negative and n is positive, then $(ma)(nb) + (|m|a)(nb) = ((m + |m|)a)(nb) = 0$ so that $(ma)(nb) = -(|m|n)(ab) = (mn)(ab)$. Similarly, if m is positive and n is negative, then $(ma)(nb) = (mn)(ab)$. Finally, if m, n are negative, then $(ma)(nb) = (-|m|a)(-|n|b) = |mn|(ab) = (mn)(ab)$.

6. Let R be a ring.

   (a) Suppose $a \in R$. Show that $S = \{x \in R : ax = xa\}$ is a subring.

   (b) Show that the center of R defined by $Z(R) = \{x \in R : ax = xa \text{ for all } a \in R\}$ is a subring.

   Solution. (a) Note that $0 \in S_a$ is non-empty. Suppose $x, y \in S_a$. Then $ax = xa$ and $ay = ya$. So, $a(x - y) = ax - ay = xa - ya = (x - y)a$. So, $x - y \in S_a$. Also, $a(xy) = (xa)y = (xy)a$. So, $xy \in S_a$. It follows that S_a is a subring.

   (b) Note that $0 \in S$ is non-empty. Suppose $x, y \in Z(R)$. Then $ax = xa$ and $ay = ya$. So, $a(x - y) = ax - ay = xa - ya = (x - y)a$ for any $a \in R$. So, $x - y \in Z(R)$. Also, $a(xy) = (xa)y = (xy)a$ for any $a \in R$. So, $xy \in Z(R)$. It follows that $Z(R)$ is a subring.

   Alternatively, we can show that intersection of subrings is a subring, and use the fact that $Z(R) = \cap_{a \in R} S_a$.

7. Let R be a ring.

   (a) Prove that R is commutative if and only if $a^2 - b^2 = (a + b)(a - b)$ for all $a, b \in R$.

   (b) Prove that R is commutative if $a^2 = a$ for all $a \in R$.

   (Such a ring is called a Boolean ring.)

   Solution. (a) If R is commutative, then $(a + b)(a - b) = a^2 + ab - ba - b^2 = a^2 - b^2$ for any $a, b \in R$. Suppose $(a + b)(a - b) = a^2 + ab - ba - b^2 = a^2 - b^2$ for any $a, b \in R$. Then $ab - ba = 0$, i.e., $ab = ba$.

   (b) Suppose $a^2 = a$ for all $a \in R$. Then for any $a, b \in R$, $a^2 + b^2 = a + b = (a + b)^2 = a^2 + ab + ba + b^2$ so that $ab + ba = 0$. Hence, $ab = -ba = (-ba)^2 = (ba)^2 = ba$.

8. Give an example of a Boolean ring with 4 elements. Give an example of a Boolean ring with infinitely many elements.

   Solution. Let $B = \mathbb{Z}_2 = \{0, 1\}$ such that $0 + 0 = 0$ and $0 + 1 = 1 + 0 = 1 + 1 = 1$, and $00 = 01 = 10 = 0$ and $11 = 1$. Then B is a Boolean ring with 2 elements, and $B \oplus B$ is a Boolean ring with 4 elements.

   Let $R = B^\infty = \{(a_1, a_2, \dots) : a_i \in B \text{ for each } i\}$. One can show that R is a ring under the entrywise addition and multiplication operation. Also, $(a_1, a_2, \cdots)^2 = (a_1, a_2, \dots)$. So, R is a Boolean ring with infinitely many elements.