Math 453 Abstract Algebra sample 2 with solutions to some problems

Groups

1. Show that if \( f : G \to H \) is a surjective homomorphism and \( K \triangleleft G \) then \( f(K) \triangleleft H \).

2. Show that intersection \( H_1 \cap H_2 \) of two subgroups \( H_1, H_2 \leq G \). Show that if \( H_1 \triangleleft G \) then \( H_1 \cap H_2 \triangleleft H_2 \).

3. If \( r \) is a divisor of \( m \) and \( s \) is a divisor of \( n \), find a subgroup of \( \mathbb{Z}_m \oplus \mathbb{Z}_n \) that is isomorphic to \( \mathbb{Z}_r \oplus \mathbb{Z}_s \).

4. (a) Prove that \( \mathbb{R} \oplus \mathbb{R} \) under addition in each component is isomorphic to \( \mathbb{C} \).
   
   (b) Prove that \( \mathbb{R}^* \oplus \mathbb{R}^* \) under multiplication in each component is not isomorphic to \( \mathbb{C}^* \).

   (c) Show that there is no isomorphism from \( \mathbb{Z}_8 \oplus \mathbb{Z}_2 \to \mathbb{Z}_4 \oplus \mathbb{Z}_4 \).

   Soln: (a) \( \phi : \mathbb{R} \oplus \mathbb{R} \to \mathbb{C} \), \( \phi(a, b) \to a + ib \) is an isomorphism. For, \( \phi((a, b) + (a', b')) = a + a' + i(b + b') = \phi((a, b) + \phi(a', b')) \) \( \phi \) is bijective: the inverse \( \phi^{-1} : \mathbb{C} \to \mathbb{R} \oplus \mathbb{R} \) is given by \( \phi^{-1}(a + ib) = (a, b) \).

   (b) If \( a \in \mathbb{R}^* \) then the order of \( a \) is infinite if the absolute value \( |a| \neq 1 \) and if \( a = -1 \) the order is 2 and if \( a = 1 \) the order is 1. Then the order of \( (a, b) \) is the lcm of the orders \( |a|, |b| \).

   Thus it can be 1, 2 on \( \infty \). On the other hand \( \mathbb{C}^* \) contains the element \( i \) of order 4. Thus the groups \( \mathbb{R}^* \oplus \mathbb{R}^* \) and \( \mathbb{C}^* \) are not isomorphic.

   (c) Similarly as before \( \mathbb{Z}_8 \oplus \mathbb{Z}_2 \) contain an element of order 8, and \( \mathbb{Z}_4 \oplus \mathbb{Z}_4 \) does not.

5. Prove that if \( H \leq G \) and \( |G : H| = 2 \), then \( H \) is normal.

   Soln: \( G \) is a union of its disjoint left cosets and right cosets. If \( g \not\in H \) then \( G = H \cup gH = H \cup Hg \). Thus \( gH = G \setminus H = Hg \). If \( g \in H \) then \( gH = H = Hg \). In any case \( gH = Hg \) for \( g \in G \). Thus \( H \) is normal in \( G \).

6. Let \( G = \mathbb{Z}_4 \oplus \mathbb{Z}_2, H = \langle (2, 1) \rangle \) and \( K = \langle (2, 0) \rangle \). Show that \( G/H \) is not isomorphic to \( G/K \).

   Soln: The group \( G/H \) contains 4 = 8/2 elements. Moreover \( G/H = \{H, (1, 0) + H, (2, 0) + H, (3, 0) + H\} \) is cyclic generated by \( (1, 0) + H \) of order 4. Similarly the group \( G/K \) contains 4 = 8/2 elements. But \( G/K = \{K, (1, 0) + K, (0, 1) + K, (1, 1) + K\} \), with all nonzero elements having order 2. Thus the groups are not isomorphic.

7. Let \( G \) be a finite group, and \( H \) be a normal subgroup of \( G \).

   (a) Show that the order of \( aH \) in \( G/H \) must divide the order of \( a \) in \( G \).

   (b) Show that it is possible that \( aH = bH \), but \( |a| \neq |b| \).

   Soln: (a) Let \( |a| = n \) then \( a^n = e \), and \( (aH)^n = a^nH = H \). Thus the order of \( aH \) divides \( n = |a| \).
(b) If $a \in H$ and $a \neq e$ then $|a| \neq 1 = |e|$, but the order $aH = H$ is the same as the order of $eH = H$.

8. Suppose that $N \triangleleft G$ and $|G/N| = m$, show that $x^m \in N$ for all $x \in G$.

Soln: The order of $xN \in G/N$ divides $|G/N| = m$, and thus $(xN)^m = x^mN = eN = N$. The latter implies that $x^m \in N$.

9. For each pair of positive integer $m$ and $n$, show that the map $\phi$ from $\mathbb{Z} \rightarrow \mathbb{Z}_m \oplus \mathbb{Z}_n$ defined by $x \mapsto (x \mod m, x \mod n)$ is a homomorphism. Find its kernel.

Soln:

$$\phi(x+y) = (x+y \mod m, x+y \mod n) = (x \mod m, x \mod n)+(y \mod m, y \mod n) = \phi(x)+\phi(y)$$

which shows that $\phi$ is a homomorphism.

If $x \in \mathbb{Z}$ is in the kernel of $\phi$ iff $x \mod m = 0$, $x \mod n = 0$ iff $m$ divides $x$ and $n$ divides $x$. The latter is equivalent the fact that $x$ is a multiple of $\text{lcm}(m,n)$. Thus $\text{Ker}(\phi) = \text{lcm}(m,n) \cdot \mathbb{Z}$.

10. How many (group) homomorphisms are there from $\mathbb{Z}_{20}$ onto (surjective to) $\mathbb{Z}_8$. How many are there to $\mathbb{Z}_8$? Soln: If $\phi : \mathbb{Z}_{20} \rightarrow \mathbb{Z}_8$ is onto then there is $a \in \mathbb{Z}_{20}$, such that $\phi(a) = 1 \in \mathbb{Z}_8$. This implies that the order $|\phi(a)|$ is 8 and divides order of $a$. But the order of $a$ divides 20. This implies 8 divides 20, which is a contradiction. There is no homomorphism from $\mathbb{Z}_{20}$ onto $\mathbb{Z}_8$.

If $\phi : \mathbb{Z}_{20} \rightarrow \mathbb{Z}_8$ is a homomorphism then the order of $\phi(1)$ divides $\text{gcd}(8,20) = 4$ so $\phi(1)$ is in a unique subgroup of order 4 which is $2\mathbb{Z}_8$. Thus possible homomorphisms are of the form $x \mapsto 2i \cdot x$ where $i = 0, 1, 2, 3$. One can easily see (please check) that all the functions define homomorphisms, and thus there are 4 homomorphisms.

11. Prove that $\phi : \mathbb{Z} \oplus \mathbb{Z} \rightarrow \mathbb{Z}$ by $\phi(a,b) = a - b$ is a homomorphism. Determine the kernel.

Soln: $\phi((a,b) + (a',b')) = a + a' - (b + b') = \phi(a,b) + \phi(a',b')$, and thus $\phi$ is a homomorphism. The kernel of $\phi$ is given by $\{(a,b) \mid \phi(a,b) = 0\} = \{(a,b) \mid a - b = 0\} = \{(a,a) \mid a \in \mathbb{Z}\}$.

12. (a) Let $G$ be the group of nonzero real numbers under multiplication. Suppose $r$ is a positive integer. Show that $x \mapsto x^r$ is a homomorphism. Determine the kernel, and determine $r$ so that the map is an isomorphism.

(b) Let $G$ be the group of polynomial in $x$ with real coefficients. Define the map $p(x) \mapsto P(x) = \int p(x)$ such that $P(0) = 0$. Show that $f$ is an homomorphism, and determine its kernel.

Soln: (a) $\phi_r(xy) = (xy)^r = x^ry^r = \phi_r(x)\phi_r(y)$, and thus $\phi$ is a homomorphism.

$$\text{Ker}(\phi_r) = \{x \mid \phi_r(x) = 1\} = \{x \mid x^r = 1\}$$
The equation $x^r = 1$ has one solution $x = 1$ if $r$ is odd, and two solns $x = 1$ or $x = -1$ if $r \neq 0$ is even. Finally If $r = 0$ the $x^r = 1$ for all $x \in \mathbb{Z}$. Consequently $Ker(\phi_r) = 1$ is trivial if $r$ is odd , $Ker(\phi_r) = \{-1, 1\}$ if $r \neq 0$ is even, and $Ker(\phi_r) = \mathbb{Z}$ if $r = 0$. Also if $r$ is odd then $\phi_r$ is bijective with inverse given by $x \mapsto \sqrt[3]{x}$. This implies that $\phi_r$ is an isomorphism if $r$ is odd.

(b) $p(x) \mapsto P(x) = \int p(x)$ such that $P(0) = 0$, and $p_1(x) \mapsto P_1(x) = \int p_1(x)$ such that $P_1(0) = 0$. $p(x) + p_1(x) \mapsto \overline{P(x)} = \int (p(x) + p_1(x))$ such that $P(0) = 0$. Then we have equality (up to constant) of the indefinite integrals $\overline{P(x)} + c = \int (p(x) + p_1(x)) = \int p(x) + \int p_1(x) = P(x) + p_1(x)$. But $\overline{P(0)} + c = 0 + c = P(0) + p_1(0) = 0 + 0$ which implies $c = 0$ and $\overline{P(x)} = P(x) + p_1(x)$. The latter means that $p(x) \mapsto P(x)$ is a homomorphism.

If $p(x)$ is in the kernel of the given homomorphism then $P(x) = 0$, and consequently $p(x) = P'(x) = 0$. This implies that the kernel is trivial.

13. (a) Determine all (group) homomorphisms from $\mathbb{Z}_n$ to itself

(b) Determine all (group) homomorphisms from $\mathbb{Z}_{30}$ to itself with kernel $3\mathbb{Z}_{30}$.

Soln: (a) Let $\phi : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ be a homorphism. Denote $a := \phi(1) \in \mathbb{Z}_n$. Then the homomorphism $\phi$ is given by $\phi(x) = ax$. Conversely (please check) for any $a \in \mathbb{Z}_n$ the function $x \mapsto ax$ defines a homomorphism,

(b) Let $\phi : \mathbb{Z}_{30} \rightarrow \mathbb{Z}_{30}$ be a homomorphism, $\phi(x) = ax$. If $3\mathbb{Z}_{30} \subset Ker(\phi)$ then $\phi(3) = 3a = 0 \in \mathbb{Z}_{30}$. Thus $30|3a$, and $10|a$. This means $a = 10, 20, 0$. If $a = 0$ then $Ker(\phi) = \mathbb{Z}_{30}$.

If $a = 10$, then $x \in Ker(\phi)$ iff $30|ax$ iff $3|x$ iff $x \in 3\mathbb{Z}_{30}$.

If $a = 20$, then $x \in Ker(\phi)$ iff $30|20x$ iff $3|2x$ iff $3|x$ iff $x \in 3\mathbb{Z}_{30}$.

Thus if $a = 10, 20$ then $Ker(\phi) = 3\mathbb{Z}_{30}$. 

3
Rings

14. Find all the ring homomorphisms: a) \( \mathbb{Z}_5 \to \mathbb{Z}_{10} \), b) \( \mathbb{Z}_{10} \to \mathbb{Z}_{10} \).

15. Let \( R \) be a ring.
   (a) Suppose \( a \in R \). Shown 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.

16. 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 \( a \in R \).

17. Show that every nonzero element of \( \mathbb{Z}_n \) is a unit (element with multiplicative inverse) or a zero-divisor.

18. Find the characteristic of \( \mathbb{Z}_n \oplus \mathbb{Z}_m \).

19. An element \( a \) of a ring \( R \) is nilpotent if \( a^n = 0 \) for some \( n \in \mathbb{N} \).
   (a) Show that if \( a \) and \( b \) are nilpotent elements of a commutative ring, then \( a + b \) is also nilpotent.
   (b) Show that a ring \( R \) has no nonzero nilpotent element if and only if \( 0 \) is the only solution of \( x^2 = 0 \) in \( R \).
   (c) Show that the set of all nilpotent elements of a commutative ring is an ideal.

20. Let \( R_1 \) and \( R_2 \) be rings, and \( \phi : R_1 \to R_2 \) be a ring homomorphism such that \( \phi(R) \neq \{0\} \).
   (a) Show that if \( R_1 \) has unity and \( R_2 \) has no zero-divisors, then \( \phi(1) \) is a unity of \( R_2 \).
   (b) Show that the conclusion in (a) may fail if \( R_2 \) has zero-divisors.

21. Let \( R_1 \) and \( R_2 \) be rings, and \( \phi : R_1 \to R_2 \) be a ring homomorphism.
   (a) Show that if \( A \) is an ideal of \( R_1 \), then \( \phi(A) \) is an ideal of \( \phi(R_1) \).
   (b) Give an example to show that \( \phi(A) \) may not be an ideal of \( R_2 \).
   (c) Show that if \( B \) is an ideal of \( R_2 \), then \( \phi^{-1}(B) \) is an ideal of \( R_1 \).

22. Let \( D \) be an integral domain.
   Show that a nonconstant polynomial in \( D[x] \) has no multiplicative inverse.

23. Solve the equations in \( \mathbb{Z}_7 \): (a) \( x^2 = 2 \), (b) \( 3x = 4 \)

24. Show that \( I = \{ a_0 + \cdots + a_n x^n : a_i \in \mathbb{Q}, a_0 + \cdots + a_n = 0 \} \) is an ideal. Show that \( A = \{ a_0 + \cdots + a_n x^n : a_i \in \mathbb{Q}, a_0 + \cdots + a_n \in \mathbb{Z} \} \) is an subring of \( \mathbb{Q}[x] \).