MA 407 Homework

Vasudev Menon

Contents

Homework 1

Problem 1

Let n and a be positive integers, and let $d = \gcd(n, a)$. Show that the equation $ax \mod n = 1$ has a solution if and only if $d = 1$.

Proof. Assume $d = 1$, so $gcd(n, a) = 1$ and so $\exists s, t \in \mathbb{Z}$ such that $as + nt = 1$, or $as = -nt + 1$, which implies that $as \mod n = 1$, and thus the equation $ax \mod n = 1$ has the solution $x = a$. Now assume $ax \mod n = 1$. Then, $\exists q \in \mathbb{Z}$ such that $ax = nq + 1$, so $ax - nq = 1$. This means that for $s = x$ and $t = -n$, we have $as + nt = 1$, thus $gcd(n, a) = 1$. □

Problem 2

Prove the uniqueness portion of the Fundamental Theorem of Arithmetic (for a precise statement, see Theorem 0.3). The existence portion is done by induction in Example 13 of Chapter 0.

Proof. Assume, for the sake of contradiction, that $n = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$ where $p_1, p_2, ..., p_n$ and $q_1, q_2, ..., q_m$ are all primes but there exists at least one element that is different between $\{p_1, p_2, ..., p_n\}$ and $\{q_1, q_2, ..., q_n\}$. According to the Generalized Euclid's Lemma, if p is a prime and p divides $a_1 a_2 \cdots a_n$, then p divides a_i for some i. So, since p_1 is a prime that divides $p_1, p_2, ..., p_n$, p_1 divides q_i for some i, and since the products are unordered, we can suppose p_1 divides q_1. Then, we have that $p_2 p_3 \cdots p_n = q_2 q_3 \cdots q_m$. Repeating this process, we have that $p_n = q_m$ and thus, $n = m$. So $\{p_1, p_2, ..., p_n\} = \{q_1, q_2, ..., q_n\}$ and thus, the prime factorization is unique. □

Problem 3

Show that $\gcd(a, bc) = 1$ if and only if $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$.

Proof. Assume $\gcd(a, bc) = 1$, so $\exists s, t \in \mathbb{Z}$ such that $as + bct = 1$. Let $u = ct$. Then, we have shown that $\exists s, u \in \mathbb{Z}$ such that $as + bu = 1$, and thus, $gcd(a, b) = 1$. Now, let $v = bt$. Then, we have shown that $\exists s, v \in \mathbb{Z}$ such that $as + cv = 1$, and thus, $gcd(a, c) = 1$. Now assume, for the sake of contradiction, that $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$, but $\gcd(a, bc) \neq 1$. Since $\gcd(a, bc) \neq 1$, a and b are not relatively prime, and so there exists a prime

$p > 1$ that divide both a and bc. Since p divides bc, it either divides b or c or both. However, since $\gcd(a, b) = 1$, there does not exists a prime $p > 1$ such that p divides b, and since $\gcd(a, c) = 1$, p does not divide c, a contradiction. So $\gcd(a, bc) = 1$ □

Problem 4

Use induction (instead of the modular arithmetic trick we did in class) to prove that the sum of the cubes of any three consecutive positive integers is divisible by 9.

Proof. We will prove that for any $n > 1$, $n^3 + (n+1)^3 + (n+2)^3 = 9m$ for some $m \in \mathbb{Z}$ by induction. Note that for the base case $n = 1$, $n^3 + (n+1)^3 + (n+2)^3 = 1^3 + 2^3 + 3^3 = 1 + 8 + 27 = 36 = 9(4)$, so we have proven the base case. For the inductive case, assume $n^3 + (n+1)^3 + (n+2)^3 = 9m$. So $n^3 + n^3 + 3n^2 + 3n + 1 + n^3 + 6n^2 + 12n + 8 = 3n^3 + 9n^2 + 15n + 9 = 9m$. Then, $(n+1)^3 + (n+2)^3 + (n+3)^3 = n^3 + 3n^2 + 3n + 1 + n^3 + 6n^2 + 12n + 8 + n^3 + 9n^2 + 27n + 27 = 3n^3 + 18n^2 + 42n + 36 = 9n^2 + 27n + 27 + (3n^3 + 9n^2 + 15n + 9) = 9(n^2 + 3n + 3) + 9m = 9(m + n^2 + 3n + 3)$, which is divisible by 9 since $m + n^2 + 3n + 3$ is an integer. Therefore, the sum of the cubes of any three consecutive positive integers is divisible by 9. □

Problem 5

Prove that every set with n elements has exactly 2^n subsets.

Proof. We will prove the statement by induction. For the base case $n = 0$, the set with n elements, the empty set, has $2^0 = 1$ subsets (only itself). Now, assume that the set with n elements has 2^n subsets. Now consider a set with $n + 1$ elements. Excluding the additional element, there are n elements which yields 2^n subsets. For each of these subsets, the additional element can either be included or excluded from them, so there are $2 \cdot 2^n = 2^{n+1}$ subsets. Therefore, the set with $n + 1$ elements has 2^{n+1} elements. So we have proven the inductive case. Therefore, every set with n elements has 2^n subsets. □

Homework 2

Problem 1

Let $f : X \to Y$ be a function. Prove that f is a bijection if and only if there exists a function $g : Y \to X$ such that $f \circ g = \mathrm{id}_Y$ and $g \circ f = \mathrm{id}_X$, where id_X denotes the identity function on X.

Proof. We will prove both directions of the statement.
($\Rightarrow$) Assume that f is a bijection. Since it is a bijection, define $g : Y \to X$ to be the inverse function of f, that is, for all $y \in Y$, define $g(y) = x$ such that $f(x) = y$. Then, for all $y \in Y$, $f(g(y)) = y = \mathrm{id}_Y$. So $f \circ g = \mathrm{id}_Y$. Next, we know there exists a $x \in X$ such for all $y \in Y$, $f(x) = y$ and $g(y) = x$. So $g(f(x)) = g(y) = x = \mathrm{id}_X$, and thus, $g \circ f = \mathrm{id}_X$. Therefore, there exists a function $g : Y \to X$ such that $f \circ g = \mathrm{id}_Y$ and $g \circ f = \mathrm{id}_X$.
($\Leftarrow$) Suppose that there exists a function $g : Y \to X$ such that $f \circ g = \mathrm{id}_Y$ and $g \circ f = \mathrm{id}_X$. Since $f \circ g = \mathrm{id}_Y$, for every $y \in Y$, we have that $f(g(y)) = y$. So we know that for every $y \in Y$, there exists an $x = g(y) \in X$ such that $f(x) = y$, and thus, f is surjective. Now, since $g \circ f = \mathrm{id}_X$, for every $x \in X$, we have that $g(f(x)) = x$. Assume that $f(a) = f(b)$ for some two elements $a, b \in X$. Then, apply g to both sides of the equation, so $g(f(a)) = g(f(b))$, which simplifies to $a = b$. Therefore, f is injective. Since f is both surjective and injective, f is a bijection. □

Problem 2

Let D_3 denote the group of symmetries of a regular 3-gon (i.e., an equilateral triangle). Explicitly write out the elements, and determine if the group is abelian.

Solution : The group D_3 consists of the six symmetries of the equilateral triangle:

1. e: The identity
2. r: A rotation by 120° clockwise.
3. r_2: A rotation by 240° clockwise.
4. s: A reflection across the vertical axis

5. s_2: A reflection across an axis that is at 120° to the vertical.

6. s_3: A reflection across an axis that is at 240° to the vertical.

Therefore, D_3 contains the elements $\{e, r, r_2, s, s_2, s_3\}$. Now, using the operation of composition, note that $r \cdot s = s_3$, but $s \cdot r = s_2$, so the group is not commutative and thus is not abelian.

Problem 3

Make a Cayley table for the group $U(8)$.

Solution : $U(8)$ includes all integers less than 8 with and relatively prime to 8. So $U(8) = \{1, 2, 3, 4, 5, 6, 7, 8\} \setminus \{2, 4, 6, 8\} = \{1, 3, 5, 7\}$.
Thus, the group $U(8)$ includes the integers $\{1, 3, 5, 7\}$ under the operation multiplication modulo 8. The following is its Cayley table:

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Problem 4

Prove the set of 3×3 real matrices

$$\mathcal{H} := \left\{ \begin{bmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix} : a, b, c \in \mathbb{R} \right\}$$

is a group under matrix multiplication. This is called the *Heisenberg group.*

Proof. To show that $(\mathcal{H}, \times)$ is a group, we verify the group axioms:
(1) Closure: Suppose $A, B \in \mathcal{H}$. Then,

$$A = \begin{bmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & d & f \\ 0 & 1 & e \\ 0 & 0 & 1 \end{bmatrix}, \quad \text{where } a, b, c, d, e, f \in \mathbb{R}.$$

The product is given by:

$$A \times B = \begin{bmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & d & f \\ 0 & 1 & e \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+d & c+ea+f \\ 0 & 1 & b+e \\ 0 & 0 & 1 \end{bmatrix}.$$

Since $a + d, b + e, c + ea + f \in \mathbb{R}$, it follows that $A \times B \in \mathcal{H}$. Thus, $(\mathcal{H}, \times)$ satisfies closure.
(2) Associativity: Let $A, B, C \in \mathcal{H}$, where:

$$A = \begin{bmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & d & f \\ 0 & 1 & e \\ 0 & 0 & 1 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & g & i \\ 0 & 1 & h \\ 0 & 0 & 1 \end{bmatrix}.$$

First, compute $(A \times B) \times C$:

$$A{\times}B = \begin{bmatrix} 1 & a+d & c+ea+f \\ 0 & 1 & b+e \\ 0 & 0 & 1 \end{bmatrix}, \quad (A{\times}B){\times}C = \begin{bmatrix} 1 & a+d+g & c+ea+f+h(a+d)+i \\ 0 & 1 & b+e+h \\ 0 & 0 & 1 \end{bmatrix}.$$

Next, compute $A \times (B \times C)$:

$$B{\times}C = \begin{bmatrix} 1 & d+g & f+hd+i \\ 0 & 1 & e+h \\ 0 & 0 & 1 \end{bmatrix}, \quad A{\times}(B{\times}C) = \begin{bmatrix} 1 & a+d+g & c+ea+f+h(a+d)+i \\ 0 & 1 & b+e+h \\ 0 & 0 & 1 \end{bmatrix}.$$

Since $(A \times B) \times C = A \times (B \times C)$, the operation is associative.
(3) Identity: Let $E = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \in \mathcal{H}$. For any $A \in \mathcal{H}$,

$$A \times E = \begin{bmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix},$$

and

$$E \times A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix}.$$

Thus, E is the identity element.

(4) Inverses: Let $A = \begin{bmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix} \in \mathcal{H}$. Define

$$A^{-1} = \begin{bmatrix} 1 & -a & -c+ab \\ 0 & 1 & -b \\ 0 & 0 & 1 \end{bmatrix}.$$

Then,

$$A \times A^{-1} = \begin{bmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & -a & -c+ab \\ 0 & 1 & -b \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = E.$$

Similarly, $A^{-1} \times A = E$. Thus, every element in $\mathcal{H}$ has an inverse.
Since $\mathcal{H}$ satisfies closure, associativity, has an identity, and every element has an inverse, $(\mathcal{H}, \times)$ is a group. $\square$

Homework 3

Problem 1

Let G be a group with the property that for any $x, y, z \in G$, $xy = zx$ implies $y = z$. Prove this implies G is abelian.

Proof. Consider $xy = zx$. Multiplying both sides by x^{-1} we have that $xyx^{-1} = zxx^{-1}$, so $xyx^{-1} = ze$ and thus $z = xyx^{-1}$. So we know that $z = xyx^{-1}$ implies that $z = y$, and thus, $y = xyx^{-1}$ must be true. Multiplying both sides by x, we have that $yx = xyx^{-1}x$, which means $yx = xy(x^{-1}x)$, and thus, $yx = xye = xy$, so we have that $yx = xy$, and thus, G is abelian. □

Problem 2

Prove that the Cayley table of a group is a *Latin Square*, i.e., each group element appears exactly once in every row and every column.

Proof. Consider the group $(G, *)$, and it's Cayley Table, where the entry in the row corresponding to a and the column corresponding to b is $a * b$. We will first show that each row contains all elements of G exactly once. Let $a \in G$ be any element in G. Suppose there exist elements $b, c \in G$ such that $a * b = a * c$. Multiply both sides of the equation by a^{-1} on the left. Then, we have $a^{-1} * a * b = a^{-1} * a * c$, which simplifies to $e * b = e * c$, and thus $b = c$. This means that no two elements in a row can be the same. Since the row contains $|G|$ entries and there are only $|G|$ elements in G and each element appears uniquely, it follows that each element must appear exactly once in every row. Now we will similarly prove that each column contains all elements of G exactly once. If $a*b = c*b$ for some $a, c \in G$, multiplying both sides on the right by b^{-1} leads to: $a * b * b^{-1} = c * b * b^{-1}$, which simplifies to $a = c$. This shows that no two elements in each row are the same, and since the column contains contains $|G|$ entries and there are only $|G|$ elements in G, every element appears exactly once in each column. Thus, the Cayley table is a latin square. □

Problem 3

Find all the subgroups of D_4 (the symmetries of the square).

Solution : The dihedral group D_4 consists of the following elements:

$$D_4 = \{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$$

The following are all of its subgroups:

- $\{e\}$
- $\{e, r^2\}$
- $\{e, s\}$
- $\{e, sr^2\}$
- $\{e, sr\}$
- $\{e, sr^3\}$
- $\{e, r, r^2, r^3\}$
- $\{e, r^2, s, sr^2\}$
- $\{e, r^2, sr, sr^3\}$
- D_4 itself

Problem 4

Let G be a group. For $a \in G$, define $C(a) = \{g \in G : ga = ag\}$. This is called the *centralizer* of a in G. Prove $C(a)$ is a subgroup of G.

Proof. To show $C(a)$ is a subgroup, we will show that it satisfies all properties of a subgroup. Let $e \in G$ be the identity element. Note that $ea = ae = a$ due to the properties of the identity, and so $C(a)$ is non empty and has an identity. Now let $x, y \in C(a)$, we will show $xy \in C(a)$. Note that $xa = ax$ and $ya = ay$, and so $(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy)$. So $xy \in C(a)$, and thus, $C(a)$ is closed under the group operation. Now let $g \in C(a)$. We will show that $g^{-1} \in C(a)$. Note that $g^{-1}a = g^{-1}a(gg^{-1}) = g^{-1}(ag)g^{-1} = g^{-1}(ga)g^{-1} = (g^{-1}g)ag^{-1} = ag^{-1}$, and so $g^{-1} \in C(a)$, so $C(a)$ has an inverse. Since $C(a)$ satisfies all the properties of a subgroup, we have shown that $C(a)$ is a subgroup of G. □

Problem 5

Let H and K be non-trivial subgroups of $(\mathbb{Q}, +)$. Show that $H \cap K$ is also non-trivial.

Proof. To show $H \cap K$ is also non-trivial, we will show that $H \cap K$ contains a nonzero element. Since H and K are nontrivial, they each contain at least one nonzero rational number. Let $h \in H$ and $k \in K$ both nonzero rational numbers. Since h and k are nonzero and rational, $h = \frac{a}{b}$ where $a, b \in \mathbb{Q} \setminus \{0\}$, and $k = \frac{c}{d}$ where $c, d \in \mathbb{Q} \setminus \{0\}$. Note that for any element in either H or K, since they are closed by addition, repeated addition of k in K and h in H also fall inside their respective groups. So for any $n \in \mathbb{Z}$, $nh \in H$ and $nk \in K$. This means that for $n = b$, $nh = bh = b\frac{a}{b} = a \in H$, and for $n = d$, $nk = dk = d\frac{c}{d} = c \in K$. Now, consider $a \cdot c \in \mathbb{Z}$. Since $a \in H$, adding a to itself c gives an element in H, therefore, $a \cdot c \in H$. Since $c \in K$, adding c to itself a times gives an element in K, so $a \cdot c \in K$. Since $a \cdot c \in H$ and $a \cdot c \in K$, $a \cdot c \in H \cap K$. Since $a \neq 0$ and $c \neq 0$, $a \cdot c \neq 0$. Thus, $H \cap K$ contains a nonzero element, proving that it is non-trivial. □

Homework 4

Problem 1

Find an n such that $U(n)$ is not cyclic, but every proper subgroup is.

Proof. Consider $n = 8$. Then $U(8) = \{1, 3, 5, 7\}$. The order of this is 4. We know $U(8)$ is cyclic if $U(8) = \langle g \rangle$ for some $g \in G$. However, we know the following:

- $\langle 3 \rangle = \{3, 1\}$ and so $|\langle 3 \rangle| = 2$.
- $\langle 5 \rangle = \{5, 1\}$ and so $|\langle 5 \rangle| = 2$.
- $\langle 1 \rangle = \{1\}$ and so $|\langle 1 \rangle| = 1$.
- $\langle 7 \rangle = \{7, 1\}$ and so $|\langle 7 \rangle| = 2$.

Since none of them equal 4, $U(8)$ is not cyclic. Then, we know that the order of any subgroup must divide the order of $U(8)$, which leaves us with subgroups of length 1,2 and 4, but for the subgroup to be a proper subgroup, we only have subgroups of length 1 and 2. We have the trivial group $\{1\} = \langle 1 \rangle$ of order 1. A subgroup of order 2 must contain 1 and an element of order 2. Since 3,5, and 7 all have order 2, we have

- $H_1 = \{1, 3\} = \langle 3 \rangle$
- $H_2 = \{1, 5\} = \langle 5 \rangle$
- $H_3 = \{1, 7\} = \langle 7 \rangle$

So all proper subgroups are cyclic. □

Problem 2

Suppose $G = \langle a \rangle$ has order n. For $1 \leq m, k \leq n - 1$, find a cyclic generator for the subgroup $\langle a^m \rangle \cap \langle a^k \rangle$.

Proof. Since $G = \langle a \rangle$, every element of G is a power of a. Additionally, all subgroups are also cyclic, and thus, an intersection of any two subgroups is cyclic. We can define the subgroups $A = \langle a^m \rangle = \{a^{mi} \mid i \in \mathbb{Z}\}$ and $A = \langle a^k \rangle = \{a^{kj} \mid j \in \mathbb{Z}\}$. For an element to be in the intersection of A and

B, it must be expressed as both a^{mi} and a^{kj} for integers i and j, thus, this element is $a^{p\,\mathrm{lcm}(m,k)}$ where $p \in \mathbb{Z}$. The smallest such exponent is $\mathrm{lcm}(m,k)$, and thus, the cyclic generator for the subgroup $\langle a^m \rangle \cap \langle a^k \rangle$ is $a^{\mathrm{lcm}(m,k)}$ □

Problem 3

Prove that any group of order 3 is cyclic.

Proof. Let G be a group with $|G| = 3$. We know that the order of any subgroup must divide 3, so we are left with subgroups that have an order that is either 1 or 3. If it has order 1, it must be the trivial subgroup $\{e\}$. If it has order 3, then it must be the entire subgroup G, since $|G| = 3$. Let $g \in G$ be an arbitrary non-identity element. If $|g| = 1$, then $g = e$, which is a contradiction, and thus, $|g| = 3$, meaning $g^3 = e$. So $G = \{e, g, g^2\}$ with g generating the entire group. This means that $G = \langle g \rangle$, and so G is cyclic. □

Problem 4

Suppose that G is a finite group, such that the only subgroups are G and e. Prove that G must be cyclic and have prime order.

Proof. Since G is a finite group, then $|G| = n$. We know that the order of any subgroup must divide n, but since the only subgroups are G and e, with orders n and 1 respectively, we have that the only divisors of n are n and 1, which implies that n is prime, and thus, the order of G is prime. Let $g \in G$ be an arbitrary non-identity element. Since the order of g must divide n, and since n is prime, then the only numbers that can divide n is 1 and n. Since $g \neq e$, g cannot have an order of 1, so $|g| = n$. Since $|g| = |G|$, g must generate the entire group G, so $G = \{e, g, \ldots, g^{n-1}\} = \langle g \rangle$, and thus, G is cyclic. □

Problem 5

Suppose G is a cyclic group of order 15, and $a \in G$ such that exactly two of a^3, a^5, and a^9 are equal. Determine $|a^{13}|$.

Proof. Since G is cyclic, then there exists a generator element $g \in G$ such that every element in G can be expressed as g^k for some $k \in \mathbb{Z}$. Then, suppose $a = g^k$, then $a^3 = g^{3k}$, $a^5 = g^{5k}$, and $a^9 = g^{9k}$. Since exactly two

of these elements are equal, then we can either have $g^{3k} = g^{5k}$, $g^{5k} = g^{9k}$, or $g^{3k} = g^{9k}$.
Case 1: $g^{3k} = g^{5k}$
If $g^{3k} = g^{5k}$, then $3k \equiv 5k \mod n$, and thus, $-2k \equiv 0 \mod n$, and since -2 and 15 are relatively prime, $k \equiv 0 \mod 15$. This means that $a = g^0 = e$, which implies that $a^3 = a^5 = a^9$, a contradiction.
Case 2: $g^{5k} = g^{9k}$
If $g^{5k} = g^{9k}$, then $5k \equiv 9k \mod n$, and thus, $-4k \equiv 0 \mod n$, and since -4 and 15 are relatively prime, $k \equiv 0 \mod 15$. This means that $a = g^0 = e$, which implies that $a^3 = a^5 = a^9$, a contradiction.
Case 3: $g^{3k} = g^{9k}$
If $g^{3k} = g^{9k}$, then $3k \equiv 9k \mod n$, and thus, $-6k \equiv 0 \mod n$, and since $\gcd(-6, 15) = 3$, $k \equiv 0 \mod 5$. This means that $a = g^{5m}$ for some $m \in \mathbb{Z}$. The order of g^{5m} is $|g^{5m}| = \frac{15}{\gcd(15,5)} = 3$
Since Case 3 is the only one that is valid, we know that $g^{3k} = g^{9k}$. Note that $a^{13} = g^{13k} = g^{13(5m)} = g^{65m}$. Since $|G| = 15$, $g^{65m} = g^{(65 \mod 15)m} = g^{5m}$, and so $|a^{13}| = |g^{5m}| = 3$. □

Homework 5

Problem 1

How many elements of order 12 are in S_{10}?

Solution : Elements in S_{10} with order 12 can be written as a product of disjoint cycle such that the LCM of the disjoint cycles is 12. For S_{10}, this can be done in 4 ways:

1. (6)(4)
2. (4)(3)(3)
3. (4)(3)(1)(1)(1)
4. (4)(3)(2)(1)

Now, we will count how many permutations can exist with (6)(4), (4)(3)(3), (4)(3)(1)(1)(1), and (4)(3)(2)(1).
For the first case, the product of disjoint cycles (6)(4) can be expressed as $(a_1a_2a_3a_4a_5a_6)(a_7a_8a_9a_{10})$. The number of ways to choose this is

$$\frac{10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5}{6} \cdot \frac{4 \cdot 3 \cdot 2 \cdot 1}{4} = 151200$$

Next, for the second case, the product of disjoint cycles (4)(3)(3) can be expressed as $(a_1a_2a_3a_4)(a_5a_6a_7)(a_8a_9a_{10})$. The number of ways to choose this is

$$\frac{10 \cdot 9 \cdot 8 \cdot 7}{4} \cdot \frac{6 \cdot 5 \cdot 4}{3} \cdot \frac{3 \cdot 2 \cdot 1}{3} \cdot \frac{1}{2} = 50400$$

Now, for the third case, the product of disjoint cycles (4)(3)(1)(1)(1) can be expressed as $(a_1a_2a_3a_4)(a_5a_6a_7)(a_8)(a_9)(a_{10})$. The number of ways to choose this is

$$\frac{10 \cdot 9 \cdot 8 \cdot 7}{4} \cdot \frac{6 \cdot 5 \cdot 4}{3} \cdot 1 \cdot 1 \cdot 1 = 50400$$

Finally, for the last case, the product of disjoint cycles (4)(3)(2)(1) can be expressed as $(a_1a_2a_3a_4)(a_5a_6a_7)(a_8a_9)(a_{10})$. The number of ways to choose this is

$$\frac{10 \cdot 9 \cdot 8 \cdot 7}{4} \cdot \frac{6 \cdot 5 \cdot 4}{3} \cdot \frac{3 \cdot 2}{2} \cdot 1 = 151200$$

Summing up these counts, we have

$$151200 + 50400 + 50400 + 151200 = 403200$$

elements in S_{10} with order 12.

Problem 2

What are the possible orders of elements in the groups

(a) S_6

(b) A_6

(c) A_7

Solution : In S_6, we have the following (where (a) represents a cycle with length a):

- $(6) \xrightarrow{order} 6$
- $(5)(1) \xrightarrow{order} 5$
- $(4)(2) \xrightarrow{order} 4$
- $(4)(1)(1) \xrightarrow{order} 4$
- $(3)(3) \xrightarrow{order} 3$
- $(3)(2)(1) \xrightarrow{order} 6$
- $(3)(1)(1)(1) \xrightarrow{order} 3$
- $(2)(2)(2) \xrightarrow{order} 2$
- $(2)(2)(1)(1) \xrightarrow{order} 2$
- $(2)(1)(1)(1)(1) \xrightarrow{order} 2$
- $(1)(1)(1)(1)(1)(1) \xrightarrow{order} 1$

So the possible orders of S_6 are $1, 2, 3, 4, 5, 6$

Now, in A_6, we have:

- $(5)(1) \xrightarrow{order} 5$
- $(4)(2) \xrightarrow{order} 4$
- $(3)(3) \xrightarrow{order} 3$
- $(3)(1)(1)(1) \xrightarrow{order} 3$
- $(2)(2)(1)(1) \xrightarrow{order} 2$
- $(2)(1)(1)(1)(1) \xrightarrow{order} 2$
- $(1)(1)(1)(1)(1)(1) \xrightarrow{order} 1$

So the possible orders of A_6 are $1, 2, 3, 4, 5$

Finally, in A_7, we have:

- $(7) \xrightarrow{order} 7$
- $(5)(1)(1) \xrightarrow{order} 5$
- $(4)(2)(1) \xrightarrow{order} 4$
- $(3)(3)(1) \xrightarrow{order} 3$
- $(3)(2)(2) \xrightarrow{order} 6$
- $(3)(1)(1)(1)(1) \xrightarrow{order} 3$
- $(2)(2)(1)(1)(1) \xrightarrow{order} 2$
- $(1)(1)(1)(1)(1)(1)(1) \xrightarrow{order} 1$

So the possible orders of A_7 are $1, 2, 3, 4, 5, 6, 7$

Problem 3

Show that a permutation of odd order must be an even permutation.

Proof. A permutation α of odd order can be expressed as $\alpha = \alpha_1, \ldots, \alpha_k$ where α_i are pairwise disjoint cycles. Since this permutation has odd order, then the $\text{lcm}(|\alpha_i|)_{1 \leq i \leq k}$ must be odd. This implies that each a_i is odd (since if any of the a_i were even, then $\text{lcm}(|\alpha_i|)_{1 \leq i \leq k}$ would be a multiple of an even number, which is a contradiction). So we have that all the disjoint cycles α_i are odd. Note that each α_i can be represented as

$$\alpha_i = (a_1 a_2 \cdots a_l) = \underbrace{(a_1 a_l) \cdots (a_1 a_2)}_{l-1 \text{ terms}}$$

Note that there are $l - 1$ of these terms. In our case, since l is odd, $l - 1$ is even, and thus, each α_i is an even permutation. Since α is the product of even permutation, it is itself an even permutation. □

Problem 4

Prove S_4 is not isomorphic to D_{12}.

Proof. In S_4, we have the following (where (a) represents a cycle with length a):

- (4) which has order 4
- (3)(1) which has order 3
- (2)(2) which has order 2
- (2)(1)(1) which has order 2
- (1)(1)(1)(1) which has order 1

So the possible orders of S_4 are $1, 2, 3, 4$. On the other hand, consider the r^2 operation, where we rotate a 12-sided regular polygon by 30° twice. Note that this element has order 6, since r^2 composed with itself 6 time returns the polygon back to its original orientation. Since S_4 does not contain an element with order 6, it is not isomorphic to D_{12} □

Homework 6

Problem 1

Show that $\mathbb{Z}$ has infinitely many distinct subgroups isomorphic to $\mathbb{Z}$.

Proof. Consider the subgroup $H = \{nk \mid k \in \mathbb{Z}\}$, where $n \in \mathbb{N}$. Note that for different values of n, H is distinct, and since there are an infinite number of n, then $\mathbb{Z}$ has an infinite number of subgroups H. Now we will show that each of these subgroups are isomorphic to $\mathbb{Z}$. Consider the following bijective function $\varphi : \mathbb{Z} \to H$ defined as $\varphi(x) = nx$. Note that $\varphi(r + s) = nr + ns = \varphi(r) + \varphi(s)$. Then, we know that φ is an isomorphism under the addition group operation. Since there exists an isomorphism from all distinct subgroups H to $\mathbb{Z}$, then $\mathbb{Z}$ has infinitely many distinct subgroups isomorphic to $\mathbb{Z}$. □

Problem 2

Show that if G is isomorphic to H, then $\mathrm{Aut}(G)$ is isomorphic to $\mathrm{Aut}(H)$.

Proof. Since G is isomorphic to H, there we know that there exists an isomorphism $\varphi : G \to H$. We will need to find an isomorphism $\Omega : \mathrm{Aut}(G) \to \mathrm{Aut}(H)$. Let $a \in \mathrm{Aut}(G)$, and define $\Omega(a) = \varphi \circ a \circ \varphi^{-1}$. Since φ and a are both isomorphisms, $\Omega(a) \in \mathrm{Aut}(H)$. Now, let $a, b \in \mathrm{Aut}(G)$. Then, $\Omega(a \circ b) = \varphi \circ (a \circ b) \circ \varphi^{-1} = (\varphi \circ a \circ \varphi^{-1}) \circ (\varphi \circ b \circ \varphi^{-1}) = \Omega(a) \circ \Omega(b)$. So Ω is a homomorphism. Now we will prove injectivity and surjectivity. First, assume $\Omega(a) = \Omega(b)$. Then $\varphi \circ a \circ \varphi^{-1} = \varphi \circ b \circ \varphi^{-1}$. Multiplying on the right by φ and on the left by φ^{-1} yields $a = b$, which means that Ω is injective. Second, let $a \in \mathrm{Aut}(H)$, and let $b = \varphi^{-1} \circ a \circ \varphi$. Then, $b \in \mathrm{Aut}(G)$, and $\Omega(b) = \varphi \circ (\varphi^{-1} \circ a \circ \varphi) \circ \varphi^{-1} = a$, and thus, Ω is surjective. So Ω is a bijection, and thus is an isomorphism. So $\mathrm{Aut}(G)$ is isomorphic to $\mathrm{Aut}(H)$. □

Problem 3

Suppose G is a finite abelian group, which has no elements of order 2. Show that the mapping $g \mapsto g^2$ is an automorphism of G. Show by example that there is an infinite abelian group with no elements of order 2 such that $g \mapsto g^2$ is not an automorphism.

Proof. For the first part of the problem, let $\varphi(g) = g^2$ be the mapping. Then, since G is abelian, then $\varphi(ab) = (ab)^2 = a^2b^2 = \varphi(a)\varphi(b)$, and thus, this is a homomorphism. Now we will show that φ is bijective. Assume $\varphi(a) = \varphi(b)$, then $x^2 = y^2 \implies x^2y^{-2} = y^2y^{-2} \implies x^2y^{-2} = e \implies (xy^{-1})^2 = e$. This means that the element xy^{-1} has order 2, but the group has no nontrivial elements of order 2, and so, this must imply that $xy^{-1} = e$, and so $xy^{-1}y = ey \implies x = y$. So φ is injective. Since φ maps G to itself and is injective, then it is also surjective, and so, φ is a bijection. This means that φ is an automorphism and thus the mapping $g \mapsto g^2$ is an automorphism of G.
For the second part, consider the infinite abelian group $\mathbb{Z}$ under the addition operation. Our map then becomes $\varphi : \mathbb{Z} \to \mathbb{Z}$ defined as $n \mapsto 2n$. Note that if an element n has order 2, then $2n = 0$, so $n = 0$, which is the trivial element. So there is no nontrivial element with order 2. Now consider the element $1 \in \mathbb{Z}$. Note that there is no element $n \in \mathbb{Z}$ such that $2n = 1$, so φ is not a surjection, and so it is not a bijection and thus is not a automorphism. So, there is an infinite abelian group with no elements of order 2 such that $g \mapsto g^2$ is not an automorphism. □

Problem 4

Prove that the group of rationals with addition $(\mathbb{Q}, +)$ is not isomorphic to any proper subgroup of itself.

Proof. Suppose $\varphi : \mathbb{Q} \to H$ is an isomorphism where $H \subseteq \mathbb{Q}$ is a proper subgroup of $\mathbb{Q}$. Now, suppose $\varphi(1) = \frac{a}{b} \in \mathbb{Q}$. Let $\frac{c}{d} \in \mathbb{Q}$. Note that $\frac{c}{d} = \frac{1}{d} + \cdots + \frac{1}{d}$, so $\varphi(\frac{c}{d}) = \varphi(\frac{1}{d} + \cdots + \frac{1}{d}) = \varphi(\frac{1}{d}) + \cdots + \varphi(\frac{1}{d}) = c\varphi(\frac{1}{d})$. Similarly, since $1 = \frac{1}{d} + \cdots + \frac{1}{d}$, we have that $\varphi(1) = d\varphi(\frac{1}{d})$. Then, $\varphi(\frac{c}{d}) = c\varphi(\frac{1}{d}) = \frac{c}{d}d\varphi(\frac{1}{d}) = \frac{c}{d}\varphi(1)$. Then, for some $q = \frac{j}{k} \in \mathbb{Q}$, we have that $\varphi(\frac{j}{k}\frac{b}{a}) = \varphi(\frac{jb}{ka}) = \frac{jb}{ka}\varphi(1) = \frac{jb}{ka}\frac{a}{b} = \frac{j}{k}$. So we showed that for some arbitrary $\frac{j}{k} \in \mathbb{Q}$, there exists an element q such that $\varphi(\text{element}) = q$, and thus, every rational number is covered in the range, and thus, φ in surjective onto all of $\mathbb{Q}$, which implies that $H = \mathbb{Q}$, and thus $H \subsetneq \mathbb{Q}$. So the group of rationals with addition $(\mathbb{Q}, +)$ is not isomorphic to any proper subgroup of itself. □

Homework 7

Problem 1

Let G be the dihedral group D_n of symmetries of the regular n-gon. Determine explicitly the cosets of the rotation subgroup (make sure you give a proof!).

Proof. The rotation subgroup of D_n is $R = \langle r \rangle = \{e, r, r^2, \ldots, r^{n-1}\}$. Note that this is a cyclic group since $r^n = e$. The left coset of R in G_n is in the form gR. If g is a rotation, then we have $gR = eR = \{e, r, r^2, \ldots, r^{n-1}\} = \mathrm{R}$. If g is some refection, note that any reflection can be denoted as sr^k for some $k \in \mathbb{N}$. So the left coset is $sr^kR = s(r^kR) = sR = \{s, sr, sr^2, \ldots, sr^{n-1}\}$. Also, D_n has $2n$ elements, and both sR and R have n elements each, so together, they constitute the $2n$ elements in D_n. So the only two cosets of D_n are $R = \langle r \rangle = \{e, r, r^2, \ldots, r^{n-1}\}$ and $sR = \{s, sr, sr^2, \ldots, sr^{n-1}\}$. □

Problem 2

Suppose G is an abelian group with an odd number of elements. Show that the product of all the elements is the identity in G.

Proof. Suppose G is an abelian group with an odd number of elements. Since G is abelian, then every element has a inverse, and so every element (that is not an identity) can be mapped a unique inverse element. If $g \neq g^{-1}$, then we have that its product $gg^{-1} = e$. Since G is odd, then there is one element g such that $g = g^{-1}$, and thus, $g = e$. The product of all elements is thus a multiplication of e, resulting in e. So the product of all the elements is the identity in G. □

Problem 3

Prove that A_5 has no subgroup of order 30.

Proof. Suppose, for the sake of contradiction, that A_5 has a subgroup H of order 30. Since $|A_5| = 60$, $[A_5 : H] = \frac{60}{30} = 2$. So H is a subgroup of index 2 and is therefore normal in A_5. However, A_5 is a simple group, so it has no nontrivial normal subgroups, which is a contradiction. So A_5 has no subgroup of order 30. Uses 3/21 lecture. □

Problem 4

Explicitly find a subgroup of $\mathbb{Z}_{12} \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{15}$ of order 9.

Solution : Let $G = \mathbb{Z}_{12} \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{15} = \text{lcm}(12, 4, 15) = 720$. The order of an element (a, b, c) in this group is $\text{lcm}(|a|, |b|, |c|)$, so we need to find where $\text{lcm}(|a|, |b|, |c|) = 9$. So $|a|, |b|, |c| \in \{1, 3, 9\}$. Since $\mathbb{Z}_{12}$ has elements of order $1, 2, 3, 4, 6, 12$ that divide 12, then $1, 3$ are our only candidates. Since $\mathbb{Z}_4$ has orders $1, 2, 4$, then 1 is our only candidate. Since $\mathbb{Z}_{15}$ has orders $1, 3, 5, 15$, then $1, 3$ is our only candidate. An element in $\mathbb{Z}_{12}$ with order 3 is 4. An element in $\mathbb{Z}_4$ with order 1 is 0. An element in $\mathbb{Z}_{15}$ with order 3 is 5. Then we have the subgroup $(4x, 0, 5y)$ where $x, y \in \{0, 1, 2\}$ to make a subgroup isomorphic to $\mathbb{Z}_{\not 9} \times \mathbb{Z}_{\not 9}$ which has order 9. So the subgroup is

$$(0,0,0),\ (0,0,5),\ (0,0,10),\ (4,0,0),\ (4,0,5),\ (4,0,10),\ (8,0,0),\ (8,0,5),\ (8,0,10)$$

of $\mathbb{Z}_{12} \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{15}$ with order 9.

Problem 5

Let $G = \{1, 7, 17, 23, 49, 55, 65, 71\}$, with group operation given by multiplication modulo 96. Express this as a direct product of cyclic groups.

Solution : Let $G = \{1, 7, 17, 23, 49, 55, 65, 71\}$ under multiplication modulo 96 with $|G| = 8$. Then, the abelian groups of order 8 are: $\mathbb{Z}_8,\ \mathbb{Z}_4 \oplus \mathbb{Z}_2,\ \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Now, the following are the orders of the elements in G.

- $\text{ord}(1) = 1$
- $\text{ord}(7) = 4$
- $\text{ord}(17) = 2$
- $\text{ord}(23) = 4$
- $\text{ord}(49) = 2$
- $\text{ord}(55) = 4$
- $\text{ord}(65) = 2$
- $\text{ord}(71) = 2$

Note that since are no elements of order 8, G is not cyclic. Additionally, there are three elements of order 4 and four of order 2, which matches the structure of $\mathbb{Z}_4 \oplus \mathbb{Z}_2$. So $G \cong \mathbb{Z}_4 \oplus \mathbb{Z}_2$, which is a product of cyclic groups.

Homework 8

Problem 1

Show that if a subgroup $H \leq G$ has exactly two left cosets, then H is normal.

Proof. We know that the index $[G : H] = 2$, so $|G| = 2 \cdot |H|$. This means that G is partitions in a way $G = H \cup gH$ for some $g \in G \setminus H$. Since $[G : H] = 2$, every element in G is either in one of two left cosets, H or gH. Additionally, since $[G : H] = 2$, we hae two right cosets, H and Hg. Now, for any $x \in G$, if $x \in H$, then $xH = H = Hx$. If $x \notin H$, then $x \in gH$ and $x \in Hg$, since $gH = G \setminus H$ and $Hg = G \setminus H$, we have that $gH = Hg$. So the left coset $xH = gH$ and the right coset $Hx = Hg$, and thus, $xH = Hx$ for all $x \in G$. This implies that H is normal. □

Problem 2

Find an example of a group G, a normal subgroup $H \trianglelefteq G$, two elements $a, b \in G$ such that $aH = bH$, but $|a| \neq |b|$.

Solution : Let $G = \mathbb{Z}_6$ with the addition operation. Let $H = \langle 3 \rangle = \{0, 3\}$. Now let $a = 1$ and $b = 4$. Then $aH = \{1, 4\}$, and $bH = \{1, 4\}$, so $aH = bH$, but $|a| = 6$ and $|b| = 3$.

Problem 3

Determine all homomorphisms from $\mathbb{Z}_4$ to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Solution : Suppose $f : \mathbb{Z}_4 \to \mathbb{Z}_2 \oplus \mathbb{Z}_2$ is a function. Since 1 is the generator of $\mathbb{Z}_4$, let $f(1) = a$ for some $a \in \mathbb{Z}_2 \oplus \mathbb{Z}_2$, so $f(x) = xa$. Then $f(x + y) = (x + y)a = xa + ya = f(x) + f(y)$. Then, since f depends on the choice of $a \in \mathbb{Z}_2 \oplus \mathbb{Z}_2$, in order for f to be a homomorphism, the order of a must divide the order of $|1| = 4$, but all choices of a have orders that divide 4. Since there are 4 such choices, there are 4 homomorphisms: $f_1(x) = x \cdot (0, 0)$, $f_2(x) = x \cdot (0, 1)$, $f_3(x) = x \cdot (1, 0)$, $f_4(x) = x \cdot (1, 1)$.

Problem 4

Let G be a finite group and $\phi : A_4 \to G$ a homomorphism. Show that if 3 does not divide $|G|$, then ϕ is the trivial homomorphism, i.e. $\phi(a) = e_G$ for all $a \in A_4$.

Proof. Suppose $a \in A_4$ is an element with order 3. Then $\phi(a) \in G$ must have an order than divides 3, so it either has order 1 or order 3. But since 3 does not divide $|G|$, no elements in G has order 3, so $\phi(a)$ only has order 1. So for any $a \in A_4$ with $|a| = 3$, $\phi(a) = e_G$. Now, note that the group A_4 is generated by elements with 3-cycles, so A_4 is generated by elements with order 3. Since ϕ maps elements with order 3 to e_G, and A_4 is generated by those elements, $\phi(a) = e_G$ for all $a \in A_4$. □

Problem 5

Show that if M, N are both normal subgroups of G and in addition N is a subgroup of M, then $(G/N)/(M/N) \cong G/M$.

Proof. Let $f : G/N \to G/M$ be a function with $f(gN) = gM$. Then, $f(gN \cdot hN) = f(ghN) = ghM = gM \cdot hM = f(gN) \cdot f(hN)$, so f is a homomorphism. Additionally, every element in the range is the image of $gN \in G/N$, so f is onto. Then, $\ker f = \{gN \in G/N \mid gM = M\} = \{gN \mid g \in M\} = M/N$. Then, using the First Isomorphism Theorem, since $f : G/N \to G/M$ is a homomorphism, onto, and $\ker f = M/N$, then $(G/N)/(M/N) \cong G/M$. □

Homework 9

Problem 1

Determine whether the ring consisting of $\{0, 2, 4, 6, 8\}$ with addition and multiplication modulo 10 has unity (if so, find it).

Proof. To check for unity, we need to find $e \in R$ such that for all $r \in R$, $er \equiv r \mod 10$.

Check each element in R:

- $e = 2$: $2 \cdot 2 = 4 \neq 2$, so not identity.
- $e = 4$: $4 \cdot 2 = 8 \neq 2$, so not identity.
- $e = 6$: $6 \cdot 0 = 0, 6 \cdot 2 = 2, 6 \cdot 4 = 4, 6 \cdot 6 = 6, 6 \cdot 8 = 8$. Since all products equal the original elements, so 6 acts as a multiplicative identity on R.
- $e = 8$: $8 \cdot 2 = 6 \neq 2$, so not identity.

Thus, the ring R has unity, and it is 6. □

Problem 2

Show that any ring whose additive group $(R, +)$ is cyclic must have commutative multiplication.

Proof. Suppose $(R, +)$ is a cyclic group. Then there exists an element $g \in R$ such that every element $r \in R$ can be written as $r = ng$ for some integer n. In other words, $R = \{ng \mid n \in \mathbb{Z}\}$.

Let $a = mg$ and $b = ng$ be elements of R, where $m, n \in \mathbb{Z}$. Then the product ab is: $ab = (mg)(ng) = mn(g \cdot g) = mng^2$. Then, $ba = (ng)(mg) = nm(g \cdot g) = nmg^2$. Since multiplication of integers is commutative, we have: $ab = mng^2 = nmg^2 = ba$. Thus, multiplication in R is commutative.

□

Problem 3

Suppose that R is a ring such that $x^3 = x$ for all $x \in R$. Prove that $6x = 0$ for all $x \in R$.

Proof. Since $x^3 = x$ for all $x \in R$, then $(x+x)^3 = (x+x)$. This means that $(2x)^3 = 2x \implies 8x^3 = 2x$. Then, since $x^3 = x$, $8x^3 = 2x \implies 8x = 2x \implies 6x = 0$. □

Problem 4

Let R be a ring with unity and $a \in R$ such that $a^n = 0$ for some positive n. Show that $1 - a$ has a multiplicative inverse.

Proof. Let $b = 1+a+a^2+\cdots+a^{n-1}$. Then, $(1-a)b = (1-a)\left(\sum_{k=0}^{n-1} a^k\right) \implies \sum_{k=0}^{n-1} a^k - \sum_{k=0}^{n-1} a^{k+1} \implies 1-a^n$, and since $a^n = 0$, this equals 1. So we have that $(1-a)b = 1$. The same logic can be applied to show that $b(1-a) = 1$.

Thus, $b = 1 + a + a^2 + \cdots + a^{n-1} = \sum_{k=0}^{n-1} a^k$ is the inverse of $1 - a$, so $1 - a$ has a multiplicative inverse.

□

Problem 5

Find a 0-divisor in the ring $\mathbb{Z}_5[i] = \{a + bi : a, b \in \mathbb{Z}_5\}$, where $i^2 = -1$.

Solution : We will find an element in the ring $x \in \mathbb{Z}_5[i]$ such that there exists another element $y \in \mathbb{Z}_5[i]$ where $xy = 0$. Consider the element $x = 2 + i \in \mathbb{Z}_5[i]$. Now consider the element $y = 3 + i \in \mathbb{Z}_5[i]$. Then, note that $xy = (2+i)(3+i) = 2(3+i)+i(3+i) = 6+2i+3i+i^2 = 6+5i+i^2 = 5+5i = 0$ in $\mathbb{Z}_5[i]$. So $x = 2 + i$ is a 0-divisor in $\mathbb{Z}_5[i]$.

Homework 10

Problem 1

Let R be a commutative ring and let A be any ideal of R. Show that set $N(A) := \{r \in R : r^n \in A\}$ is also an ideal of R.

Proof. Since $0 \in A$, then $0^1 = 0 \in A$, so when $n = 1$, $0 \in N(A)$, and thus, $N(A)$ is non-empty. Now suppose $a, b \in N(A)$. We will show that $a+b \in N(A)$. Since $a, b \in N(A)$, then there exists $n, m \in \mathbb{N}$ such that $a^n \in A$ and $b^m \in A$. Let $N = m+n$. Then $(a+b)^N = \sum_{k=0}^{N} \binom{N}{k} a^k b^{N-k}$. In each term of this sum, either $k \geq n$ or $N - k \geq m$. In the first case, $a^k = a^n \cdot a^{k-n} \in A$ (since A is an ideal), and in the second, $b^{N-k} = b^m \cdot b^{N-k-m} \in A$. So every part of the summation is in A, and so $(a+b)^N \in A$, so $a + b \in N(A)$. Now, let $r \in N(A)$ with $r^n \in A$ and suppose $a \in R$. Then $(ar)^n = a^n r^n \in A$, and thus, $ar \in N(A)$. So $N(A)$ is an ideal. □

Problem 2

In the polynomial ring $\mathbb{Z}_5[x]$, consider the ideal $I = \langle x^2 + x + 2 \rangle$. Find the multiplicative inverse of $(2x + 3) + I$ in $\mathbb{Z}_5[x]/I$.

Solution : We need to find a function $f(x)$ such that $(2x+3)f(x) = 1$ when modded by $x^2 + x + 2$. So we will set $(2x + 3 + I)(ax + b + I) = 1 + I$. Then we will solve for a and b. Note that $(2x+3)(ax+b) = 2ax^2 + (2b+3a)x + 3b$. Since $x^2 = -x - 2 \mod I$, then we have $2a(-x - 2) + (2b + 3a)x + 3b = (a + 2b)x + (-4a + 3b)$. We then need the coefficient of x to be 0 and the constant to be 1. So we have the linear system of equations $a + 2b = 0$ and $-4a + 3b = 1$ in $\mathbb{Z}_5$. So we get $a = 3$ and $b = 1$. So $f(x) = 3x + 1$ is the multiplicative inverse of $(2x + 3) + I$ in $\mathbb{Z}_5[x]/I$.

Problem 3

Consider

$$K := \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\} \subseteq \mathbb{R}$$

and

$$H := \left\{ \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} : a, b \in \mathbb{Z} \right\} \subseteq M_2(\mathbb{Z}),$$

which are subrings of $\mathbb{R}$ and $M_2(\mathbb{Z})$ respectively. Show that H is isomorphic to K as rings.

Proof. Let $\varphi : K \to H$ be a function with $\varphi(a + b\sqrt{2}) = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix}$. We will show that φ is an isomorphism. Let $x = a + b\sqrt{2}$ and $y = c + d\sqrt{2}$. Then $\varphi(x + y) = \varphi((a + c) + (b + d)\sqrt{2}) = \begin{bmatrix} a + c & 2(b + d) \\ b + d & a + c \end{bmatrix}$, and $\varphi(x) + \varphi(y) = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} + \begin{bmatrix} c & 2d \\ d & c \end{bmatrix} = \begin{bmatrix} a + c & 2(b + d) \\ b + d & a + c \end{bmatrix}$. Thus, $\varphi(x + y) = \varphi(x) + \varphi(y)$.

Now, consider $xy = (a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$, so $\varphi(xy) = \begin{bmatrix} ac + 2bd & 2(ad + bc) \\ ad + bc & ac + 2bd \end{bmatrix}$. On the other hand, $\varphi(x)\varphi(y) = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \begin{bmatrix} c & 2d \\ d & c \end{bmatrix} = \begin{bmatrix} ac + 2bd & 2ad + 2bc \\ ad + bc & ac + 2bd \end{bmatrix}$. So $\varphi(xy) = \varphi(x)\varphi(y)$. Now suppose $\varphi(a + b\sqrt{2}) = \varphi(c + d\sqrt{2})$. Then $\begin{bmatrix} a & 2b \\ b & a \end{bmatrix} = \begin{bmatrix} c & 2d \\ d & c \end{bmatrix}$, which implies $a = c$ and $b = d$, so $a + b\sqrt{2} = c + d\sqrt{2}$. Thus φ is injective. Next, every element of H is of the form $\begin{bmatrix} a & 2b \\ b & a \end{bmatrix}$, which is the image of $\varphi(a + b\sqrt{2})$. So φ is surjective. So φ is a ring isomorphism and thus $H \cong \mathbb{Z}[\sqrt{2}]$.

□

Problem 4

Show that the subrings of $\mathbb{R}$ given by $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ and $\mathbb{Q}[\sqrt{5}] = \{a + b\sqrt{5} : a, b \in \mathbb{Q}\}$ are **not** isomorphic.

Proof. Assume for the sake of contradiction that there exists an isomorphism $\varphi : \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{5}]$. Then $\varphi(\sqrt{2}) = a + b\sqrt{5}$, so $2 = (a + b\sqrt{5})^2 = a^2 + 5b^2 + 2ab\sqrt{5}$. This gives us the system of equations $a^2 + 5b^2 = 2$, $2ab = 0$. In the second equation, either $a = 0$ and/or $b = 0$. If $a = 0$, then $5b^2 = 2$, so $b = \sqrt{\frac{2}{5}} \notin \mathbb{Q}$. If $b = 0$, then $a^2 = 2$, so $a = \sqrt{2} \notin \mathbb{Q}$. So there are no valid $a, b \in \mathbb{Q}$ that satisfy the system of equations, which is a contradiction. So there does not exist an isomorphism $\varphi : \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{5}]$, so $\mathbb{Q}[\sqrt{2}]$ and $\mathbb{Q}[\sqrt{5}]$ are not isomorphic. □

Problem 5

Consider the polynomial ring $R := \mathbb{Q}[x]$, and consider the principal ideal $A := \langle x^2 - 2 \rangle$. Show that $R/A \cong \mathbb{Q}[\sqrt{2}]$. (Hint: consider the evaluation homomorphism $\mathbb{Q}[x] \to \mathbb{R}$ defined by $p(x) \mapsto p(\sqrt{2}) \in \mathbb{R}$...)

Proof. We are given the homomorphism $\varphi : \mathbb{Q}[x] \to \mathbb{R}$ defined by $p(x) \mapsto p(\sqrt{2}) \in \mathbb{R}$. Every element $a + b\sqrt{2}$ equals $\varphi(a + bx)$, so $\mathrm{Im}(\varphi) = \mathbb{Q}[\sqrt{2}]$. Then, since $p(x) \in \ker \varphi$ implies that $p(\sqrt{2}) = 0$, then $\sqrt{2}$ is a root of $p(x)$, however the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2$, which is irreducible in $\mathbb{Q}[x]$. So $f(x) \in \ker \varphi$ must be divisible by $x^2 - 2$, so $\ker \varphi = \langle x^2 - 2 \rangle$. Then, by the first isomorphism theorem, $\mathbb{Q}[x]/\ker \varphi \cong \mathrm{Im}(\varphi)$, so $R/A \cong \mathbb{Q}[\sqrt{2}]$. $\square$