Fall 2022 MATH410 Homework

Arya Wang

October 22, 2022

Contents

1 Homework 1

Problem 1

Find a formula for the following

$$\begin{bmatrix} 1 & 1 & 1 \\ & 1 & 1 \\ & & 1 \end{bmatrix}^n$$

Prove that the formula is correct using induction.

Solution

Formula:

$$\begin{bmatrix} 1 & n & \frac{n(n+1)}{2} \\ 0 & 1 & n \\ 0 & 0 & 1 \end{bmatrix}$$

Prove by induction: Suppose the product of k such matrices is:

$$P(k) = \begin{bmatrix} 1 & k & \frac{n(k+1)}{2} \\ 0 & 1 & k \\ 0 & 0 & 1 \end{bmatrix}$$

We have:

$$P(k+1) = \begin{bmatrix} 1 & k & \frac{k(k+1)}{2} \\ 0 & 1 & k \\ 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1+k & 1+k+\frac{k(k+1)}{2} \\ 0 & 1 & 1+k \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1+k & \frac{(k+2)(k+1)}{2} \\ 0 & 1 & 1+k \\ 0 & 0 & 1 \end{bmatrix}$$

So $P(k+1)$ holds.

Problem 2

A square matrix A is **nilpotent** if A^k is the zero matrix for some $k > 0$. Prove that if A is nilpotent, then $I + A$ is invertible, where I is the identical matrix. Do this by finding the inverse of $I + A$.

Solution

Given $A^k = 0$, we can construct the inverse of $I + A$ as: $\sum_{i=1}^{k-1}(-1)^{i+1}A^{k-i}$, because:

$$\begin{aligned}(I+A)(\sum_{i=1}^{k-1}(-1)^{k+1}A^{k-i}) =& (\sum_{i=1}^{k-1}(-1)^{i+1}A^{k-i+1})(\sum_{i=1}^{k-1}(-1)^{i+1}A^{k-i}) \\ =& A^k - A^{k-1} + A^{k-2} \ldots \pm A \\ & + A^{k-1} - A^{k-1} \ldots \mp A \pm I \\ =& A^k \pm I \\ =& I\end{aligned}$$

So $I + A$ is invertible.

Problem 3

The matrix below is based on Pascal's triangle. Find its inverse:

$$\begin{bmatrix} 1 & & & & \\ 1 & 1 & & & \\ 1 & 1 & 2 & & \\ 1 & 3 & 3 & 1 & \\ 1 & 4 & 6 & 4 & 1 \end{bmatrix}$$

Solution

$$\left[\begin{array}{ccccc|ccccc} 1 & & & & & 1 & & & & \\ 1 & 1 & & & & 0 & 1 & & & \\ 1 & 2 & 1 & & & 0 & 0 & 1 & & \\ 1 & 3 & 3 & 1 & & 0 & 0 & 0 & 1 & \\ 1 & 4 & 6 & 4 & 1 & 0 & 0 & 0 & 0 & 1 \end{array}\right] \to \left[\begin{array}{ccccc|ccccc} 1 & & & & & 1 & & & & \\ 0 & 1 & & & & -1 & 1 & & & \\ 0 & 2 & 1 & & & -1 & 0 & 1 & & \\ 0 & 3 & 3 & 1 & & -1 & 0 & 0 & 1 & \\ 0 & 4 & 6 & 4 & 1 & -1 & 0 & 0 & 0 & 1 \end{array}\right] \to$$

$$\left[\begin{array}{ccccc|ccccc} 1 & & & & & 1 & & & & \\ 0 & 1 & & & & -1 & 1 & & & \\ 0 & 0 & 1 & & & 1 & -2 & 1 & & \\ 0 & 0 & 3 & 1 & & 2 & -3 & 0 & 1 & \\ 0 & 0 & 6 & 4 & 1 & 3 & -4 & 0 & 0 & 1 \end{array}\right] \to \left[\begin{array}{ccccc|ccccc} 1 & & & & & 1 & & & & \\ 0 & 1 & & & & -1 & 1 & & & \\ 0 & 0 & 1 & & & 1 & -2 & 1 & & \\ 0 & 0 & 0 & 1 & & -1 & 3 & -3 & 1 & \\ 0 & 0 & 0 & 4 & 1 & -3 & 8 & -6 & 0 & 1 \end{array}\right] \to$$

$$\left[\begin{array}{ccccc|ccccc} 1 & & & & & 1 & & & & \\ 0 & 1 & & & & -1 & 1 & & & \\ 0 & 0 & 1 & & & 1 & -2 & 1 & & \\ 0 & 0 & 0 & 1 & & -1 & 3 & -3 & 1 & \\ 0 & 0 & 0 & 0 & 1 & 1 & -4 & 6 & -4 & 1 \end{array}\right]$$

The inverse matrix is:

$$\begin{bmatrix} 1 & & & & \\ -1 & 1 & & & \\ 1 & -2 & 1 & & \\ -1 & 3 & -3 & 1 & \\ 1 & -4 & 6 & -4 & 1 \end{bmatrix}$$

Problem 4

Prove that if a product AB of $n \times n$ matrices is invertible, then so are the factors A and B.

Solution

If AB invertible, we have $\det(AB) \neq 0$. Since $\det(AB) = \det(A)\det(B)$, $\det(A)$ and $\det(B)$ cannot equal to zero. Therefore, they are invertible.

Problem 5

A matrix is called symmetric if $A^t = A$. Prove that for any square matrix A, both AA^t and $A + A^t$ are symmetric. Further, prove that if A is invertible, then $(A^{-1})^t = (A^t)^{-1}$.

Solution

1. AA^t symmetric:
$$(AA^t)^t = (A^t)^t A^t = AA^t$$
2. $A + A^t$ symmetric:
$$(A + A^t)^t = A^t + (A^t)^t = A^t + A = A + A^t$$
3. Prove the equation:
$$A^t(A^{-1})^t = (A^{-1}A)^t = I^t = I$$

So $(A^{-1})^t$ is the inverse of A^t.

Problem 6

Let A be an $n \times n$ matrix. Determine $\det(-A)$ in terms of $\det(A)$.

Solution

We have:
$$\det(-I_n) = \begin{vmatrix} -1 & & & \\ & -1 & & \\ & & \cdots & \\ & & & -1 \end{vmatrix}_{n\times n} = -1 \times \begin{vmatrix} -1 & & \\ & \cdots & \\ & & -1 \end{vmatrix} = (-1)^n$$

So,
$$\begin{aligned} \det(-A) &= \det(-I_n \times A) \\ &= \det(-I_n)\det(A) \\ &= (-1)^n \det(A) \end{aligned}$$

Problem 7

Write the following permutations from S_5 as products of disjoint cycles

(a) (12)(13)(14)(15)

(b) (123)(234)(345)

(c) (1234)(2345)

(d) (12)(23)(34)(45)(51)

Solution

(a) (12)(13)(14)(15)=(15432)

(b) (123)(234)(345)=(12)(3)(45)=(12)(45)

(c) (1234)(2345) = (12453)

(d) (12)(23)(34)(45)(51) = (2345)

Problem 8

Let P be a permutation matrix. Prove that its inverse is its transpose P^t.

Solution

We can write an arbitrary permutation matrix as:

$$\begin{pmatrix} -X_{p(1)}- \\ -X_{p(2)}- \\ \dots \\ -X_{p(n)} \end{pmatrix}$$

where each $X_{p(k)}$ stands for a row of zeros with only a 1 in $p(k)$th place. Then its transpose looks like:

$$\begin{pmatrix} Y_{p(1)} & Y_{p(2)} & \dots & Y_{p(n)} \end{pmatrix}$$

where each $Y_{p(k)}$ stands for a column of zeros with a 1 in $p(k)$th place. So,

$$PP^t = \begin{pmatrix} -X_{p(1)}- \\ -X_{p(2)}- \\ \dots \\ -X_{p(n)} \end{pmatrix} \times \begin{pmatrix} Y_{p(1)} & Y_{p(2)} & \dots & Y_{p(n)} \end{pmatrix} = \begin{pmatrix} 1 & & \\ & 1 & \\ & & \dots \end{pmatrix} = I_n$$

according to the algorithm of matrix multiplication. Similar for P^tP.

Problem 9

Which of the following subset is a subspace of the vector space $M_n(\mathbb{R})$, the set of matrices with entries from $\mathbb{R}$?

(a) Symmetric matrices

(b) Invertible matrices

(c) Upper triangular matrices

Solution

(a) Yes. Let A, B be two symmetric matrices. $(A+B)^t = A^t + B^t$. So the set is closed under addition. $(cA)^t = cA^t$. So the set is also closed under scalar multiplication.

(b) No, the sum of two invertible matrices I and $-I$ is 0 which is not invertible. So the set is not closed over addition.

(c) Yes. The set is closed over addition because the zeros in lower triangle will remain zero during all possible addition (0+0=0). And it is closed under scalar multiplication because $0 \times c = 0$, so all the zeros in the under triangle will also remain zero.

Problem 10

Find a basis for the space of $n \times n$ symmetric matrices.

Solution

$$\left\{\begin{bmatrix} 1 & 0 & \dots \\ 0 & 0 & \dots \\ & & \dots \end{bmatrix}, \begin{bmatrix} 0 & 0 & \dots \\ 0 & 1 & \dots \\ \dots & \dots & \dots \end{bmatrix}, \dots, \begin{bmatrix} 0 & 0 & \dots \\ 0 & \dots & \dots \\ \dots & \dots & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & \dots \\ 1 & 0 & \dots \\ \dots & \dots & 0 \end{bmatrix}, \begin{bmatrix} 0 & \dots & \dots \\ \dots & \dots & 1 \\ \dots & 1 & 0 \end{bmatrix}\right\}$$

Basically, the basis consists of all $e_{i,i}$, each containing only a 1 somewhere on the diagonal, and all $e_{i,j} + e_{j,i}$ for $i < j$, each contains a pair of 1s symmetric to the diagonal.

Problem 11

Let $W \subseteq \mathbb{R}^4$ be the subspace of solutions to the linear equation $Ax = 0$ where

$$A = \begin{bmatrix} 2 & 1 & 2 & 4 \\ 1 & 1 & 3 & 0 \end{bmatrix}$$

Find a basis for W.

Solution

$$A \to \begin{bmatrix} 1 & 0 & -1 & 4 \\ 1 & 1 & 3 & 0 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & -1 & 4 \\ 0 & 1 & 4 & 4 \end{bmatrix}$$

Suppose the column vector $x = (x_1, x_2, x_3, x_4)$, then according to the A_{rref}, we have

$$x_1 = x_3 - 4x_4;$$

$$x_2 = -4x_3 - 4x_4$$

So we can write x as:

$$x = \begin{pmatrix} x_3 - 4x_4 \\ -4x_3 - 4x_4 \\ x_3 \\ x_4 \end{pmatrix} = x_3 \begin{pmatrix} 1 \\ -4 \\ 1 \\ 0 \end{pmatrix} + x_4 \begin{pmatrix} -4 \\ -4 \\ 0 \\ 1 \end{pmatrix}$$

So $(1,-4,1,0)$ and $(-4,-4,0,1)$ span the solution space and they are linearly independent. So they are also the basis for W.

Problem 12

(a) Determine the change of basis matrix going from the standard basis $\epsilon = (\vec{i}, \vec{j})$ of $\mathbb{R}^n$ to the basis $B = (\vec{i}+\vec{j}, \vec{i}-\vec{j})$

(b) Determin the hange of basis matrix going from the standard basis $\epsilon = (\vec{e_1}, \vec{e_2}, ..., \vec{e_n})$ of $\mathbb{R}^n$ to the basis $B = (\vec{e_n}, e_{\vec{n-1}}, ..., \vec{e_1})$

Solution

(a)

$$B = \begin{pmatrix} \vec{i}+\vec{j} \\ \vec{i}-\vec{j} \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \vec{i} + \begin{pmatrix} 1 \\ -1 \end{pmatrix} \vec{j} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{pmatrix} \vec{i} \\ \vec{j} \end{pmatrix}$$

So change of basis matrix is

$$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

(b) Since basis B contains only a 1 in each row and each line, it is of the form of a permutation matrix. So, as proved in problem 8, $BB^t = I_n = \epsilon$. And B, by definition, looks like:

$$\begin{pmatrix} & & & & 1 \\ & & & 1 & \\ & & \cdots & & \\ & 1 & & & \\ 1 & & & & \end{pmatrix}$$

Thus, the change of basis matrix $P = B^t = B$

Problem 13

Prove that the vector space $M_n(\mathbb{R})$ pf all $n \times n$ matrices with entries from $\mathbb{R}$ is the direct sum of the space of symmetric matrices $(A^t = A)$ and the space of skew-symmetric matrices $(A^t = A)$

Solution

Let S denotes the space of symmetric matrices and K denotes the space of skew-symmetric matrices.
First prove $S + K = M$. For any square matrices $A \in M_n(\mathbb{R})$, we have

$$(A + A^t)^t = A^t + A$$
$$(A - A^t)^t = A^t - A$$

So $A + A^t \in S, A - A^t \in K$. And for any matrices A, we have:

$$A = \frac{A + A^t}{2} + \frac{A - A^t}{2}$$

So any matrices in M_n can be written as the sum of matrices from S and K. So $S + K = M$.

Second, prove S, K independent. If not, there exists some non-zero matrix M such that $M \in S$ and $M \in K$. Then $M^t = M = -M \implies M = 0$. Contradict to the assumption. So, S, K are independent.

Therefore, $M_n(\mathbb{R})$ is the direct sum of S and K.

2 Homework 2

Problem 14

Let x, y, z and w be elements of a group G with identity element e.

(1) Solve for y given that $xyz^{-1}w = e$.

(2) Suppose that $xyz = e$. Does it follow that $yzx = e$? Does it follow that $yxz = e$?

Solution

(1) Since x, y, z, w are all elements of a group, their inverse also exists in the group.

$$\begin{aligned} xyz^{-1}w &= e \\ x^{-1}xyz^{-1}ww^{-1} &= x^{-1}ew^{-1} \\ eyz^{-1}e &= x^{-1}zw^{-1} \\ yz^{-1}z &= x^{-1}w^{-1}z \\ y &= x^{-1}w^{-1}z \end{aligned}$$

(2)

$$\begin{aligned} xyz &= e \\ x^{-1}xyz &= x^{-1}e \\ yz &= x^{-1} \\ yzx &= x^{-1}x \\ yzx &= e \end{aligned}$$

So $yzx = e$ holds. According to the equations above,

$$\begin{aligned} yz &= x^{-1} \\ y &= x^{-1}z^{-1} \\ yxz &= x^{-1}z^{-1}xz \end{aligned}$$

Commutative is not necessarily hold for matrix multiplication in a group. Therefore $yxz = e$ might not be true.

Problem 15

In which of the following cases is H as subgroup of G?

(1) $G = GL_n(\mathbb{C})$ and $H = GL_n(\mathbb{R})$.

(2) $G = \mathbb{R}^\times$ and $H = \{-1, 1\}$.

(3) $G = \mathbb{Z}^+$ and H is the set of positive integers.

(4) $G = \mathbb{R}^\times$ and H is the set of positive real numbers.

(5) $G = GL_2(\mathbb{R})$ and H is the set of matrices $\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$ with $a \neq 0$.

Solution

(1) Yes. **Closure:** For every $A, B \in H$, $AB \in H$ because H is a group itself according to the lecture's example. **Identity:** The identity is I_n. $I_n \in H$ and any for $A \in H$, $AI = IA = A$. **Inverse:** For every $A \in H$, $A^{-1} \in H$ since H is a group itself.
(2) Yes. **Closure:** $1 \times 1 = 1 \in H$, $(-1) \times (-1) = 1 \in H$, $1 \times (-1) = -1 \in H$. **Identity:** the identity is $1 \in H$. **Inverse:** $(-1)^{-1} = 1 \in H$, $1^{-1} = 1 \in H$.
(3) No. **No identity:** identity should be 0, since $0 + x = x$. However, 0 is not positive integer.
(4) Yes. **Closure:** For any $x, y \in \mathbb{R}^*$, $x \times y \in \mathbb{R}^*$. **Identity:** the identity is 1 since $1 \times x = x$ for any $x \in H$. **Inverse:** every real number except 0 has a multiplicative inverse.
(5) No. **No inverse:** For any $A \in H$, $\det A = 0$. So, the matrices in H don't have inverse.

Problem 16

In the definition of a subgroup H of a group G, the identity element in H is required to be the identity element of G.
One might require only that H have an identity element, not that it need be the same as the identity in G. Show that if H has an identity at all, then it must be the identity in G.

Solution

Suppose H has identity e_H, G has identity e_G. Since $e_H \in H$, we have

$$e_H e_H = e_H$$

Since $e_H \in H \subseteq G$, so $e_H \in G$. Then,

$$e_H e_G = e_H$$

So, let e_H^{-1} be the inverse of e_H in group G

$$e_H e_H = e_H e_G$$
$$e_H^{-1} e_H e_H = e_H^{-1} e_H e_G$$
$$e_H = e_G$$

Problem 17

Prove that if a and b are positive integers such that $a + b = p$ for a prime p then their gcd is 1.

Solution

Let $d = \gcd(a, b)$, then $d \mid a, d \mid b$. That is, $a = md, b = nd$ for some integer m, n. Then $a + b = (m + n)d$, which means $d|(a + b) \implies d \mid p$. Then $d = 1$ or p. If $d = p$, then $d > a, d > b$, which is definitely not true. So $d = 1$.

Problem 18

Let a and b be elements of a group G. Assume that a has order 7 and that $a^3 b = ba^3$. Prove that $ab = ba$.

Solution

$$a^3 b = ba^3$$
$$a^6 b = a^3 ba^3$$
$$a^6 b = (a^3 b)a^3 = (ba^3)a^3 = ba^6$$
$$a^7 b = b = aba^6$$
$$ba = aba^7 = ab$$

Problem 19

An n**th root of unity** is a complex number $z \in \mathbb{C}$ such that $z^n = 1$.

(1) Prove that the n th roots of unity form a cyclic subgroup of $\mathbb{C}^\times$ of order n.

(2) Determine the product of all the nth roots of unity.

Solution

(1) First, I want to prove that the roots form a subgroup H. **Closure:** if $z_1, z_2 \in H$, $z_1^n = z_2^n = 1$, so $(z_1 z_2)^n = z_1^n z_2^n = 1 \implies z_1 z_2 \in H$. **Identity:** the identity is 1 $(1 \times z = 1)$. Since $z \in H$, $z^n = 1 \in H$. **Inverse:** for any $z \in H$, $z^{n-1} \times z = z^n = 1$. $z^{n-1} \in H$.
Second, prove that H is cyclic. Since $z^n = 1$, $(z^2)^n = (z^n)^2 = 1$, $(z^3)^n = 1$,... Therefore,$z, z^2, z^3, \ldots, z^k$ for $k \in \mathbb{Z}$

are all nth roots of unity. According to the definition, the nth roots form a cyclic group.

We have $z^{n+1} = z^n z = z$. Similarly, $z^{qn+k} = z^k$ for $q \in \mathbb{Z}$. Therefore the group has at most order of n. Now we want to prove the order is exactly n. Since $z^n = 1$, $|z| = 1$. We can write $z = e^{\frac{2\pi}{n}i} = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$, $z^s = e^{2\pi\frac{s}{n}i} = \cos(2\pi\frac{s}{n}) + i\sin(2\pi\frac{s}{n})$ for $0 < s < n$. According to the polar coordinates of these complex numbers $z, z^2, z^3, \ldots$, the first n terms, $z, z^2, \ldots, z^n$ are distinct to each other since the angle θ has a period of 2π. So H has a order of 4.

(2)

$$\begin{aligned}
\prod_{i=1}^{n} z^i &= z^{\sum_{i=1}^{n} i} \\
&= z^{\frac{(1+n)n}{2}} \\
&= z^{n\times\frac{1+n}{2}}
\end{aligned}$$

Apply the result to polar form of complex number, we get:

$$\begin{aligned}
z^{\frac{n(1+n)}{2}} &= e^{2\pi\frac{n(1+n)}{2n}i} \\
&= e^{(1+n)\pi i}
\end{aligned}$$

Therefore, if n is odd, the product equals to 1. If n is even, the product equals to -1. We can write it as

$$(-1)^{n+1}$$

Problem 20

Let a and b be elements of a group G. Prove that ab and ba have the same order.

Solution

Suppose ab has order n, ba has order m. That is, $(ab)^n = (ba)^m = e$. So we have,

$$\begin{aligned}
(ab)(ab)\ldots(ab) &= 1 \ \text{ (The product of } n\ ab\text{'s)} \\
(ba)(ba)\ldots(ba) &= a^{-1}b^{-1} \ \text{ (The product of } n-1 \text{ (ba)'s)} \\
(ba)^{n-1}ba &= a^{-1}b^{-1}ba \\
(ba)^n &= 1
\end{aligned}$$

Since ba has order m, m must be the smallest positive integer s.t. $(ba)^m = 1$. So $m \leqslant n$.

Similarly,

$$\begin{aligned}
(ba)(ba)\ldots(ba) &= 1 \ \text{ The product of } m\ ba\text{'s} \\
(ab)(ab)\ldots(ab) &= b^{-1}a^{-1} \ \text{ The product of } m-1\ ab\text{'s} \\
(ab)^m &= b^{-1}a^{-1}ab = 1
\end{aligned}$$

So we have $n \leqslant m$. Conclude: $m = n$.

Problem 21

Describe all groups that contain no proper subgroups.

Solution

The group G with no proper subgroups must be a cyclic group with prime order.
For any $x \in G$, we can obtain a subgroup $H = \langle x \rangle \subseteq G$ with $|H| = \text{ord}(x)$. So if G has no proper subgroups, then x must generate G for any $x \neq e$ in G. So this G must be cyclic.
Assume G has non-prime order n, then there exists at least an integer k s.t. $k \mid n$ and $0 < k < n$. Then $\text{ord}(x^k) = \frac{n}{\gcd(k,n)} = \frac{n}{k} =$ some integer $d < n$. Therefore, there exists a subgroup $S = \langle x^k \rangle$ with order less than n. This subgroup S is a proper subgroup of G. So, G must have prime order.

Problem 22

Let x and y be elements of a group G with identity element e. Assume that each of the elements x, y, and xy have order 2. Prove that the set $H = \{e, x, y, xy\}$ is a subgroup of G of order 4.

Solution

First prove H is a subgroup of G. Since $x, y \in G$ and G is a group, $xy \in G$. So $H \subseteq G$. **Closure:** e times everything is the thing itself which is in the group. Other cases:

$$
\begin{aligned}
x \times y &= xy \in H \\
x \times xy &= x^2 y = y \in H \\
y \times x &= yx = (x^{-1}y^{-1})^{-1} = (xy)^{-1} = xy \\
y \times xy &= yxy = xyy = x \\
xy \times x &= xyx = xxy = y \\
xy \times y &= xyy = yxy = x
\end{aligned}
$$

Identity: $e \in H$. **Inverse:** Since $x^2 = y^2 = (xy)^2 = e$, $x^{-1} = x; y^{-1} = y; (xy)^{-1} = xy$, all in H. So H is a subgroup of G.
Next prove H has order 4, which means the four elements are all distinct from each other. We know $x, y, xy \neq e$. Otherwise their order should be 1. Suppose $x = xy$, then $y = e$, which contradicts previous conclusion. So $x \neq xy$. Similarly, we can prove $y \neq xy$. Suppose $x = y$, then $xy = x^2 = e$, which is proved to be wrong previously. Therefore, $x \neq y$. So the four elements are distinct to each other and H has order 4.

Problem 23

(1) Adapt the method of row reduction to prove that the transpositions generate the symmetric group S_n.

(2) Prove that, for $n \geqslant 3$, the 3-cycles generate the alternating group A_n.

Solution

(a) For any n-cycle, $(x_1x_2...x_n)$, we can decompose it to the product like $(x_1x_2)(x_2x_3)...(x_{n-1}x_n)$. Any 2-cycle (x_nx_m) can be written as a transposition which swap the mth and nth rows of the identity matrix. So the symmetric group can be generated by some transpositions.

(b) By definition, the elements in group A_n have even number of transpositions. So we can divide the transpositions into pairs. There are three cases for a pair of transpositions:

Case 1: $(ab)(ab) = ()$. **Case 2:** $(ab)(ac) = (bac)$. **Case 3:** $(ab)(cd) = (abc)(bcd)$.

So each pair can be written as a (product of) 3-cycle. Therefore, A_n can be generated by 3-cycles.

3 Homework 3

Problem 24

Let $\phi : G_1 \to G_2$ be a surjective homomorphism. Prove that if G_1 is cyclic, then G_2 is cyclic and if G_1 is abelian, then G_2 is abelian.

Solution

Suppose G_1 is generated by element a, $G_1 = \langle a \rangle$. We know $\phi(a) \in G_2$. Since ϕ is a surjective mapping, all elements y in G_2 can find an x in G_1 such that $\phi(x) = y$. We also have any $x \in G_1$ can be written as a^k. $a^k \in G_1 \implies \phi(a^k) = \phi(a)^k \in G_2$ since ϕ is a homomorphism from G_1 to G_2. Therefore, for any element $y \in G_2$ we can find $x \in G_1$ such that $\phi(x) = y = \phi(a^k) = \phi(a)^k$. So G_2 can be generated by $\phi(a)$. Conclude: if G_1 is cyclic, then G_2 is cyclic.

Let G_1 be abelian, let $x, y \in G_2$ so there exist $a, b \in G_1$ such that$\phi(a) = x, \phi(b) = y$. We have $ab = ba \implies \phi(ab) = \phi(ba) \implies \phi(a)\phi(b) = \phi(b)\phi(a)$. So G_2 is also abelian.

Problem 25

Prove that the intersection $K \cap H$ of two subgroups $H, K \leqslant G$ is also a subgroup of H, and that if K is a normal subgroup of G, then $K \cap H$ is a normal subgroup of H.

Solution

Prove $K \cap H$ is also a subgroup of H. $K \cap H$ is a subset of H. **Closure:** Let $x, y \in K \cap H$, then $x, y \in K$ and $x, y \in H$. So $xy \in K$ and $xy \in H \implies xy \in K \cap H$. **Identity:** Let e_k be the identity of K. e_k is also an identity for $K \cap H$. For any element $x \in K \cap H$, $xe_k = e_kx = x$ because $x \in K$. **Inverse:** In previous homework, we have proved that K, H, G have same identity e, so does $K \cap H$. For any $x \in K \cap H$, since $x \in K$ and $x \in H$, x^{-1} also exists in K and H, such that $x^{-1}x = e = xx^{-1}$. That is, $x^{-1} \in K \cap H$.

Let $h \in H, k \in K \cap H$, $hkh^{-1} \in H$ since H is a subgroup. If K is a normal subgroup of G, then for any $g \in G, k \in K \cap H$, $gkg^{-1} \in K$. Since $h \in H \leqslant G$, $hkh^{-1} \in K$. So $hkh^{-1} \in K \cap H$. By definition, $K \cap H$ is a normal subgroup of H.

Problem 26

Let U denote the group of matrices in $GL_2(\mathbb{R})$ of the form $A = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$, and let $\phi : U \to \mathbb{R}^\times$ be the function defined by $\phi(A) = a^2$. Prove that ϕ is a homomorphism, and determine its kernel and image.

Solution

Let $A = \begin{bmatrix} a & m \\ 0 & n \end{bmatrix}$, $B = \begin{bmatrix} b & s \\ 0 & t \end{bmatrix} \in U$, $AB = \begin{bmatrix} ab & as+mt \\ 0 & nt \end{bmatrix}$. So $\phi(AB) = ab = \phi(A)\phi(B)$. Therefore, ϕ is a homomorphism.

The identity of $\mathbb{R}^\times$ is 1.

$$\ker(\phi) = \{A \in U \mid \phi(A) = 1\} = \left\{ \begin{bmatrix} \pm 1 & b \\ 0 & d \end{bmatrix} \mid b, d \in \mathbb{R} \right\}$$

And,

$$\operatorname{im}(\phi) = \phi(U) = \left\{a^2 \mid a \in R\right\} = \{a \in \mathbb{R} \mid a \geqslant 0\}$$

Problem 27

Determine the center of $GL_n(\mathbb{R})$.

Solution

Suppose the matrix A is in the center. Then it must commute with $E_{i,j}$, where $E_{i,j}$ has a 1 in row i column j, and zeros in all other places. So $E_{i,j}A$ = a matrix where the i^{th} row is A's row j and other rows are zeros. $AE_{i,j}$ is a matrix where the j^{th} column is A's column i and other columns are zeros. Since $E_{i,j}A = AE_{i,j}$, $E_{i,j}A$ and $AE_{i,j}$ should have zeros other than the element at row i column j, A's row j should have all zeros except $a_{j,j}$ and A's column i should have all zeros except $a_{i,i}$. And the element of row i column j in $E_{i,j}A$ is $a_{j,j}$ and the element of row i column j in $AE_{i,j}$ is $a_{i,i}$. So $a_{i,i} = a_{j,j}$. Since i, j are arbitrary numbers, A must have zeros except $a_{i,i}$ for all $i \leqslant n$ and $a_{i,i}$ are the same for all $i \leqslant n$. That is, A contains identical elements on its diagonal and zeros at other positions. So we can write A as aI_n for $a \in \mathbb{R} \backslash \{0\}$.

Now we want to confirm that aI_n commutes with all the matrices in $GL_n(\mathbb{R})$. Since matrices in $GL_n(\mathbb{R})$ are all invertible, they can all be written as a product of elementary matrices. Suppose B is an arbitrary matrix in $GL_n(\mathbb{R})$, $B = E_1 E_2 ... E_k I_n$. We know A commutes with any elementary matrix, and identity matrix commutes with any matrix, so

$$AB = AE_1E_2...E_kI_n = E_1AE_2...I_n = E_1E_2...E_kAI_n = E_1E_2...E_kI_nA = BA$$

Problem 28

Let G be the group of matrices of the form $\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$. Is the function $\phi : \mathbb{R} \to G$ defined by $\phi(x) = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$ an isomorphism? ($\mathbb{R}$ is the group of real numbers under addition).

Solution

Let $x, y \in R$, we have $\phi(x) = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}, \phi(y) = \begin{bmatrix} 1 & y \\ 0 & 1 \end{bmatrix}, x * y = x + y$. So

$$\phi(x * y) = \phi(x + y) = \begin{bmatrix} 1 & x + y \\ 0 & 1 \end{bmatrix}$$

$$\phi(x)\phi(y) = \begin{bmatrix} 1 & x + y \\ 0 & 1 \end{bmatrix}$$

So, ϕ is a homomorphism.
Let $x, y \in \mathbb{R}^+$ such that $\phi(x) = \phi(y)$. So,

$$\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & y \\ 0 & 1 \end{bmatrix}$$

Then $x = y$. So ϕ is injective.
And ϕ is obviously surjective because it can generate such a matrix for any real number. So ϕ is an isomorphism.

Problem 29

Describe all homomorphisms $\phi : \mathbb{Z} \to \mathbb{Z}$. Determine which are injective, which are surjective, and which are isomorphisms.

Solution

(In this question, I assume $\phi : \mathbb{Z}^+ \to \mathbb{Z}^+$, partially because the original problem in textbook uses $\mathbb{Z}^+$ and partially because $\mathbb{Z}^+$ is a group with identity 0.
First of all, since the identity of $\mathbb{Z}^+$ is 0, $\phi(0) = 0$ according to the proposition about homomorphism. Let $\phi(1) = k \in \mathbb{Z}$. We can prove our previous claim again since if ϕ is a homomorphism:

$$k = \phi(1) = \phi(1 + 0) = \phi(1) + \phi(0) = k + \phi(0) \implies \phi(0) = 0$$

Also,

$$0 = \phi(1 + (-1)) = \phi(1) + \phi(-1) = k + \phi(-1) \implies \phi(-1) = -k$$

And for every $n \in \mathbb{Z}$, we have

$$\phi(n) = \phi(\underbrace{1 + 1 + \ldots + 1}_{n \text{ times}}) = n \times \phi(1) = kn$$

So the homomorphism $\phi:\mathbb{Z}\to\mathbb{Z}$ is of the form $\phi(n)=kn$ for some $k\in\mathbb{Z}$.

If ϕ is injective: $\phi(x)=\phi(y) \implies x=y$. That is $kx=ky \implies x=y$, so $k\neq 0$.

If ϕ is surjective: for some $k,x\in\mathbb{Z}$, $\phi(x)=1$ and $\phi(-x)=-1$. So $kx=1 \implies k=\pm 1$.

Therefore, if ϕ is bijective, $k=\pm 1$

Problem 30

Show that the functions $f(x)=\frac{1}{x}$ and $g(x)=\frac{x-1}{x}$ generate a group of functions (where the group operation is composition of functions) that is isomorphic to the symmetric group S_3.

Solution

We notice that

$$f\circ f = f(f(x)) = f(\frac{1}{x}) = x$$

So f has order 2. And

$$g\circ g\circ g = g(g(g(x))) = g(g(\frac{x-1}{x})) = g(-\frac{1}{x-1}) = x$$

So g has order 3.

x	e	f	g	$f\circ g$	$g\circ f$	$g\circ g$
e	x	$\frac{1}{x}$	$\frac{x-1}{x}$	$1+\frac{1}{x-1}$	$1-x$	$\frac{1}{1-x}$
f	$\frac{1}{x}$	x	$1+\frac{1}{x-1}$	$\frac{x-1}{x}$	$\frac{1}{1-x}$	$1-x$
g	$\frac{x-1}{x}$	$1-x$	$\frac{1}{1-x}$	$\frac{1}{x}$	$1+\frac{1}{x-1}$	x
$f\circ g$	$1+\frac{1}{x-1}$	$\frac{1}{1-x}$	$1-x$	x	$\frac{x-1}{x}$	$\frac{1}{x}$
$g\circ f$	$\frac{1}{1-x}$	$\frac{x-1}{x}$	$\frac{1}{x}$	$\frac{1}{1-x}$	x	$1+\frac{1}{x-1}$

Table 1: Multiplicative Table of G

So

$$G=\{e,f,g,f\circ g,g\circ f,g\circ g\}$$

We know

$$S_3=\left\{e,(12),(123),(12)(123),(123)(12),(123)^2\right\}$$

Let $\phi: G\to S_3$ such that $\phi(f(x))=(12)$ and $\phi(g(x))=(123)$. It's obvious that ϕ is bijective by comparing the two sets and $\phi(gh)=\phi(g)\phi(h)$ for any $g,h\in G$. So ϕ is an isomorphism of G to S_3.

Problem 31

Let G be a group. Prove that the relation $a\sim b$ if $b=gag^{-1}$ for some g in G is an equivalence relation on G.

Solution

Transitive: Suppose $a \sim b, b \sim c$, so $gag^{-1} = b$ and $hbh^{-1} = c$ for some g, h in G. So,

$$\begin{aligned} hb &= ch \\ b &= h^{-1}ch \\ gag^{-1} &= h^{-1}ch \\ hgag^{-1} &= ch \\ hgag^{-1}h^{-1} &= c \\ c &= (hg)a(hg)^{-1} \end{aligned}$$

Since G is a group, so hg and $(hg)^{-1}$ both in G. So $a \sim c$.
Symmetric: Let $a \sim b$,

$$\begin{aligned} b &= gag^{-1} \\ g^{-1}b &= ag^{-1} \\ g^{-1}bg &= a \end{aligned}$$

So $b \sim a$.
Reflexive: We have

$$eae^{-1} = a$$

So $a \sim a$. Therefore, $a \sim b$ is an equivalence equation.

4 Homework 4

Problem 32

An equivalence relation on S is determined by the subset R of the set $S \times S$ consisting of the pairs (a, b) such that $a \sim b$. Each of the following subsets R of the plane $\mathbb{R}^2$ defines a relation on the set $\mathbb{R}$ of real numbers. For each set, determine which of the axioms for an equivalence relation are satisfied:

(a) $R = \{(x, y) \mid x = y\}$

(b) $R = \varnothing$

(c) $R = \{(x, y) \mid xy + 1 = 0\}$

(d) $R = \left\{(x, y) | x^2y - xy^2 - x + y = 0\right\}$

Solution

(a) **Transitive:** If $a \sim b, b \sim c$, we have $a = b, b = c$. So $a = b = c \implies a \sim c$.
Symmetric: If $a \sim b$, we have $a = b$, so $b = a \implies b \sim a$.
Reflexive: Since $a = a$, $a \sim a$.

(b) All satisfied because no element in $R \implies$ no contradictions to the axioms.

(c) **Transitive:** If $a \sim b, b \sim c$, we have $ab + 1 = 0, bc + 1 = 0$. So $ab = -1 = bc \implies a = c$. So $ac + 1 = a^2 + 1 > 0$. So it's **not** transitive.
Symmetric: If $a \sim b$, $ab + 1 = 0 \implies ba + 1 = 0 \implies b \sim a$.
Reflexive: $a^2 + 1 > 0$, so $a \nsim a$. It's **not** reflexive.

(d) **Transitive:** If $a \sim b, b \sim c$, we have $a^2b - ab^2 - a + b = 0, b^2c - bc^2 - b + c = 0$. Solving the equation, we get $a = b$ or $a = \frac{1}{b}$, $b = c$ or $b = \frac{1}{c}$. That is,

$$a_1 = b; a_2 = \frac{1}{b}$$
$$c_1 = b; c_2 = \frac{1}{b}$$

Therefore $a = c$ or $a = \frac{1}{c}$, which satisfies the equation $\implies a \sim c$.
Symmetric: If $a \sim b$, from the previous axiom, we know $a = b$ or $a = \frac{1}{b}$. That is, $b = a$ or $b = \frac{1}{a} \implies b \sim a$.
Reflexive: $a^2a - aa^2 - a + a = 0 \implies a \sim a$.

Problem 33

Let H be the cyclic subgroup of the alternating group A_4 generated by the permutation (123). Exhibit the left and the right cosets of H in A_4 explicitly.

Solution

$H = \{(), (123), (132)\}$ and

$$A_3 = \{(), (13)(24), (12)(34), (14)(23), (243), (134), (123), (142), (234), (132), (124), (143)\}$$

We can find the cosets without repeating by using the theorem that cosets partition the group. So right cosets:

$$H() = \{(), (123), (132)\}$$
$$H(234) = \{(234), (13)(24), (142)\}$$
$$H(243) = \{(243), (143), (12)(34)\}$$
$$H(124) = \{(124), (14)(23), (134)\}$$

Left cosets:

$$()H = \{(), (123), (132)\}$$
$$(234)H = \{(234), (12)(34), (134)\}$$
$$(243)H = \{(243), (124), (13)(24)\}$$
$$(142)H = \{(142), (143), (14)(23)\}$$

Problem 34

In the additive group $\mathbb{R}^n$ of vectors, let W be the set of solutions of a system of homogeneous linear equations:

$$W = \left\{\vec{x} \in \mathbb{R}^n \mid A\vec{x} = \vec{0}\right\}$$

Show that the set of solutions of a non-homogeneous equation $A\vec{X} = \vec{b}$ is either empty or an (additive) coset of W in $\mathbb{R}^n$

Solution

Let $V = \left\{\vec{v} \in \mathbb{R}^n \mid A\vec{v} = \vec{b}\right\}$. If A is non-invertible, $A\vec{v} = \vec{b}$ will have no solution and $A\vec{x} = \vec{0}$ still has solution. In this case, $V = \varnothing$. If A is invertible, the equation has solution. Let $\vec{v} = A^{-1}\vec{b} \in V$ and $\vec{x} \in W$, we have

$$\begin{aligned} A\vec{v} + A\vec{x} &= \vec{b} + \vec{0} = \vec{b} \\ A(\vec{v} + \vec{x}) &= \vec{b} \\ \vec{v} + \vec{x} &\in V \end{aligned}$$

So the elements in V can be written as $\vec{v} + \vec{x}$ for any $\vec{x} \in W$. So $V = \vec{v} + W$ which is additive coset of W.

Problem 35

Does every group whose order is a power of a prime p contain an element of order p?

Solution

By Lagrange's theorem, the subgroup of G must have order that divides the order of G. Suppose the group G has order p^k, then it's subgroups can have order p^r for $0 \leqslant r \leqslant k$. If there is no element of order p, let $g \in G$ be a non-identity element, it must have order p^{r_1} such that $r_1 > 1$. Then $g^{p^{r_1 - 1}} \in G$ has order p. Contradiction. So G must have subgroups of order p.

Problem 36

Let $\phi : G \to G'$ be a group homomorphism. Suppose that $|G| = 18$, $|G'| = 15$, and ϕ is non-trivial. What is the order of the kernel of ϕ?

Solution

Since ϕ is a homomorphism, according to the proposition in lecture, $|\mathrm{im}(\phi)|\big||G|$ and $|\mathrm{im}(\phi)|\big||G'|$. So $|\mathrm{im}(\phi)|$ can only be 1 or 3. Since ϕ is non-trivial, $|\mathrm{im}(\phi)| = 3$. And we also have $|G| = |\ker(\phi)||\mathrm{im}(\phi)|$, so $|\ker(\phi)| = 6$.

Problem 37

A group G of order 22 contains elements x and y, where $x \neq e$ and y is not a power of x. Prove that the subgroup generated by x and y is the whole group G.

Solution

Let $H = \langle x, y \rangle$. Since $x, y \in G$, $H \leqslant G$. So by Lagrange's theorem, $|H|$ can be $1, 2, 11, 22$.
If $|H| = 1$: then $x = y$, contradict to the assumption.
If $|H| = 2$: Since y is not a power of x, $y \neq x$. So x, y must have order $1 \implies x = e$. Contradiction
If $|H| = 11$: Let $X = \langle x \rangle$, $Y = \langle y \rangle$, then $X, Y \leqslant H$. So by Lagrange's theorem, $|X|\big||H|$, $|Y|\big||H|$. So x must have order 11 since $x \neq e$. Then $H = \langle x \rangle$. In this case, y must be a power of x, which leads to contradiction.
If $|H| = 22$: In this case, $H = G$, so x, y generate the group G.

Problem 38

Let G be a group of order 25. Prove that G has at least one subgroup of order 5, and that if it contains only one subgroup of order 5, then it is a cyclic group.

Solution

Let $g \neq e \in G$, and $H = \langle g \rangle$, then $H \leqslant G$. By Lagrange, $|H| = 1$ or 5 or 25. Since $g \neq e$, H must have order 5 or 25. If it has order 25, then $\langle g^5 \rangle$ has order 5. So, G has at least one subgroup of order 5.
If G has only one subgroup $\langle g \rangle$ of order 5 but it's not a cyclic group, then there exists another generator $h \neq e \in G$ with order other than $5 \implies |\langle h \rangle| = 25$. Then $G = \langle h \rangle$. G is cyclic. Contradiction.

Problem 39

Prove that every subgroup of index 2 is normal, and show by example that a subgroup of index 3 need not be normal.

Solution

We want to prove there exists $g \in G$ such that for $H \leqslant G$ we have $gHg^{-1} \leqslant H \implies gH \leqslant Hg$.
Case 1: If $g \in H$. Since H is a group itself, for any $h \in H$, $gh \in H, g^{-1} \in H \implies ghg^{-1} \in H \implies gHg^{-1} \leqslant H$
Case 2: If $g \in G \backslash H$. Then $gh \notin H$ (otherwise, $ghh^{-1} = g \in H$). Similarly, $hg \notin H$. We know H is a coset of H in G. Since the index of G is 2, and left cosets partition G. Then the second coset is $G - H$. Since $gH \neq H$, and $Hg \neq H$, $gH = G - H = Hg$. So $gHg = H$. We can conclude that G is normal.

Let $G = S_3, H = \{(), (12)\} = \langle(12)\rangle$. Then $[G : H] = |G|/|H| = \frac{6}{2} = 3$. And H is not normal:

$$(23)(12)(23)^{-1} = (23)(12)(23) = (13) \notin H$$

Problem 40

For which integers n does 2 have a multiplicative inverse in $\mathbb{Z}/n\mathbb{Z}$?

Solution

If x is the inverse, we want to make sure the following equation has solution:

$$2x \equiv 1 (\text{mod } n)$$

In another word, we want to solve:

$$nk = 1 - 2x$$
$$2x + nk = 1,$$

where $x, n, k \in \mathbb{Z}$. By Bezout's, $\gcd(2, n) \mid 1$. So n must be odd numbers.

Problem 41

What are the possible values of a^2 modulo 4? modulo 8?

Solution

If $a \equiv 0 (\text{mod } 4)$, then a^2 is divisible by 4. If $a \equiv 2 (\text{mod } 4)$, which means a is even, then a^2 is also divisible by 4. Then if $a \equiv 1 (\text{mod } 4)$, we can write a as $a = 4k + 1 \implies a^2 = 16k^2 + 8k + 1 \equiv 1 (\text{mod } 4)$. If $a \equiv 3 (\text{mod } 4)$, we write $a = 4k + 3 \implies a^2 = 16k^2 + 24k + 9 \equiv 1 (\text{mod } 4)$. So $a^2 \equiv 0$ or $1 (\text{mod } 4)$.

$$\begin{aligned}
a \equiv 0 (\text{mod } 8) &\implies a^2 \equiv 0 (\text{mod } 8) \\
a \equiv 1 (\text{mod } 8) &\implies a^2 = 64k^2 + 16k + 1 \equiv 1 (\text{mod } 8) \\
a \equiv 2 (\text{mod } 8) &\implies a^2 = 64k^2 + 32k + 4 \equiv 4 (\text{mod } 8) \\
a \equiv 3 (\text{mod } 8) &\implies a^2 \equiv 9 \equiv 1 (\text{mod } 8) \\
a \equiv 4 (\text{mod } 8) &\implies a^2 \equiv 16 \equiv 0 (\text{mod } 8) \\
a \equiv 5 (\text{mod } 8) &\implies a^2 \equiv 25 \equiv 1 (\text{mod } 8) \\
a \equiv 6 (\text{mod } 8) &\implies a^2 \equiv 36 \equiv 4 (\text{mod } 8) \\
a \equiv 7 (\text{mod } 8) &\implies a^2 \equiv 49 \equiv 1 (\text{mod } 8)
\end{aligned}$$

So possible values for $a^2 (\text{mod } 8)$ are 0,1, or 4.

Problem 42

Determine the integers n for which the following pair of congruences have a solution

$$2x - y \equiv 1(\text{mod } n)$$
$$4x + 3y \equiv 2(\text{mod } n)$$

Solution

We have

$$(1)\ nk = 2x - y - 1$$
$$(2)\ nd = 4x + 3y - 2$$

So 3*(1)+(2) gives $n(3k+d) = 10x - 5$. We can find integer k, d such that $3k + d = i$ for any $i \in \mathbb{Z}$ because $\gcd(3,1) = 1$ which divides any integer (by Bezout). Then we can also write the equation as:

$$10x - ni = 5$$

If the equation of x, i have solution, $\gcd(10, n) \mid 5$. So $\gcd(10, n) = 1$ or 5.
(2)-2*(1) gives $n(d - 2k) = 5y$. Similarly, we can find that $d - 2k$ can be any integer j by Bezout. So we want the following equation has solution:

$$nj - 5y = 0$$

This equation of j, y has at least a trivial pair of solution $(0, 0)$ regardless of n.
So we want $\gcd(10, n) \mid 5$. So n should be either co-prime to 10 or have the form of $10k + 5$.

5 Homework 5

Problem 43

Let $G = \langle x \rangle$ be a cyclic group of order 12, Let $G' = \langle y \rangle$ be a cyclic group of order 6, and let $\phi : G \to G'$ be the function defined by $\phi(x^k) = y^k$. Exhibit the correspondence for this homomorphism arising from the Correspondence Theorem.

Solution

First, find the kernel of ϕ. Let $g \in G'$ such that $g = x^k$ where $0 \leqslant k < 12$, so $\phi(g) = y^k$. If $\phi(g) = y^k = 1$, then $6 \mid k \implies k = 0$ or 6. Therefore, $\ker(\phi) = \{e, x^6\}$. Since G is cyclic, the subgroups of G are

$\langle x^0 \rangle, \langle x^1 \rangle, \langle x^2 \rangle, ..., \langle x^{11} \rangle$:

$$
\begin{aligned}
\langle e \rangle &= \{e\}; \\
\langle x \rangle &= G \\
\langle x^2 \rangle &= \{e, x^2, x^4, x^6, x^8, x^{10}\} \\
\langle x^3 \rangle &= \{e, x^3, x^6, x^9\} \\
\langle x^4 \rangle &= \{e, x^4, x^8\} \\
\langle x^5 \rangle &= G \\
\langle x^6 \rangle &= \{e, x^6\} \\
\langle x^7 \rangle &= G \\
\langle x^8 \rangle &= \langle x^4 \rangle \\
\langle x^9 \rangle &= \langle x^3 \rangle \\
\langle x^{10} \rangle &= \langle x^2 \rangle \\
\langle x^{11} \rangle &= G
\end{aligned}
$$

So the subgroups containing $K = \ker(\phi)$ are $K, G, \langle x^2 \rangle, \langle x^3 \rangle$.

$$
\begin{aligned}
\phi(K) &= \{e, e\} = \{e\} \\
\phi(G) &= G' \\
\phi(\langle x^2 \rangle) &= \{e, y^2, y^4\} = \langle y^2 \rangle \\
\phi(\langle x^3 \rangle) &= \{e, y^3\} = \langle y^3 \rangle
\end{aligned}
$$

Problem 44

Let $\phi : G \to G'$ be a surjective homomorphism, and let $H \leqslant G$ and $H' \leqslant G'$ be corresponding subgroups arising from the Correspondence Theorem. Prove that $[G : H] = [G' : H']$

Solution

We want to prove $f : \{\text{Left cosets of } H\} \to \{\text{Left cosets of } H'\}$ is a bijection. More precisely, the function is defined by $f(gH) = \phi(g)\phi(H)$.

Well-defined: If $g = k$, prove $f(gH) = f(kH)$. We know by homomorphism that $\phi(gg^{-1}) = \phi(g)\phi(g^{-1}) = e$, so the inverse of $\phi(g)$ is $\phi(g^{-1})$.

$$
\begin{aligned}
f(gH) = f(kH) &\Leftrightarrow \phi(g)\phi(H) = \phi(k)\phi(H) \\
&\Leftrightarrow \phi(k^{-1})\phi(g)\phi(H) = \phi(H) \\
&\Leftrightarrow \phi(k^{-1}g)\phi(H) = \phi(H) \\
&\Leftrightarrow \phi(H) = \phi(H)
\end{aligned}
$$

Surjective: Given an arbitrary left coset $g'H', g' \in G'$. Since ϕ is surjective, we can find $g \in G$ s.t. $\phi(g) = g'$. And by Correspondence Theorem, there is a corresponding $H \leqslant G$ such that $\phi(H) = H'$. So $g'H' = \phi(g)\phi(H) = f(gH)$. So it's surjective.
Injective: If $f(gH) = f(kH)$, which is $\phi(g)\phi(H) = \phi(k)\phi(H)$, we have

$$\phi(H) = \phi(g^{-1})\phi(k)\phi(H) = \phi(g^{-1}k)\phi(H)$$

So $\phi(g^{-1}k) \in H'$. Let $\phi(g^{-1}k) = \phi(h)$. Then

$$\begin{aligned} \phi(g^{-1}kh^{-1}) &= e \\ g^{-1}kh^{-1} &\in \ker(\phi) \in H \end{aligned}$$

Suppose $g^{-1}kh^{-1} = h' \in H$. Then $g^{-1}k = h'h \in H$. So $g^{-1}kH = H \implies kH = gH$. So injective.
Then f is a bijective function, which means the number of left cosets of H equals the number of left cosets of $H' \implies [G : H] = [G' : H']$

Problem 45

Consider the homomorphism $\phi : S_4 \to S_3$. Recalled that the indices $\{1, 2, 3, 4\}$ can be partitioned in three ways:

$$\begin{aligned} \Pi_1 &= \{1, 2\} \cup \{3, 4\} \\ \Pi_2 &= \{1, 3, \} \cup \{2, 4\} \\ \Pi_3 &= \{1, 4\} \cup \{2, 3\} \end{aligned}$$

An element $\sigma \in S_4$ applied to the indices also permutes the partitions $\{\Pi_1, \Pi_2, \Pi_3\}$,and we let $\phi(\sigma)$ be the corresponding element of S_3. This homomorphism is surjective with kernel:

$$K = \ker(\phi) = \{e, (12)(34), (13)(24), (14)(23)\}$$

Find the six subgroups of S_4 containing K arising from the Correspondence Theorem.

Solution

Since $K \leqslant S$ and K contains itself, K is one of the six subgroups. From Correspondence Theorem, $|H| = |H'||K|$. We know $|K| = 4$. Then by Lagrange, we can infer that $|H| = 4, 8, 12, 24$. And it's easy to find that S_4 is also one of the subgroups since $K \leqslant S_4$.
S_3 has six subgroups, the four non-trivial ones are: $\{\{(), (12)\}, \{()(13)\}, \{(), (23)\}, \{(), (123), (132)\}\}$. The subgroups of S_4 corresponding to the four subgroups of S_3 above are: $(23)K, (13)K, (12)K, A_4$. So the six subgroups includes the four mentioned this paragraph and two trivial ones mentioned above.

Problem 46

Let $x \in G$ have $\text{ord}(x) = r$, and let $y \in G'$ have $\text{ord}(y) = s$. What is the order of (x, y) in $G \times G'$?

Solution

We want to solve for k such that $(x,y)^k = e \implies (x^k, y^k) = (1,1) \implies x^k = 1, y^k = 1$. So $r \mid k, s \mid k \implies k = \text{lcm}(r,s) = \frac{rs}{\gcd(r,s)}$.

Problem 47

In each of the following cases, determine whether or not G is isomorphic to the product group $H \times K$.

(a) $G = \mathbb{R}^\times, H = \{\pm 1\}, K = (0, \infty)$.

(b) $G = \left\{A \in GL_2(\mathbb{R}) \mid A = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix}\right\}$

$H = \left\{A \in GL_2(\mathbb{R}) \mid A = \begin{bmatrix} a & 0 \\ 0 & c \end{bmatrix}\right\}$

$K = \left\{A \in GL_2(\mathbb{R}) \mid A = \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}\right\}$

(c) $G = \mathbb{C}^\times, H = S^1 = \{z \in \mathbb{C}^\times \mid |z| = 1\}, K = (0, \infty)$

Solution

(a) $H \cap K = \{1\}, HK = (0, \infty) \cup (-\infty, 0) = \mathbb{R}^\times$. For any $g \in \mathbb{R}^\times$, $gHg^{-1} = \left\{g1g^{-1}, g(-1)g^{-1}\right\} = \{\pm 1\} = H$. If $g \in K, gKg^{-1} \in K$. If $g \notin K$, which means $g \in \{x \mid x \in \mathbb{R}, x < 0\}$, so $g^{-1} < 0 \implies gKg^{-1} > 0 \implies gKg^{-1} \in K$. By proposition 2.11.4, $f(h,k) = hk$ is a isomorphism from $H \times K$ to G. So G is isomorphic.

(b) It's easy to find that H and K are abelian.

$$h_1 h_2 = \begin{bmatrix} a_1 & 0 \\ 0 & d_1 \end{bmatrix}\begin{bmatrix} a_2 & 0 \\ 0 & d_2 \end{bmatrix} = \begin{bmatrix} a_1 a_2 & 0 \\ 0 & d_1 d_2 \end{bmatrix} = \begin{bmatrix} a_2 & 0 \\ 0 & d_2 \end{bmatrix}\begin{bmatrix} a_1 & 0 \\ 0 & d_1 \end{bmatrix} = h_2 h_1$$

$$k_1 k_2 = \begin{bmatrix} 1 & b_1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & b_2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & b_1 + b_2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & b_2 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & b_1 \\ 0 & 1 \end{bmatrix} = k_2 k_1$$

So $(h_1, k_1)(h_2, k_2) = (h_1 h_2, k_1 k_2) = (h_2 h_1, k_2 k_1) = (h_2, k_2)(h_1, k_1) \implies H \times K$ is abelian. But G is obviously not abelian. If there exists an isomorphism f such that $f(h_1, k_1) = g_1, f(h_2, k_2) = g_2$. Then

$$\begin{aligned} g_1 g_2 &= f(h_1, k_1) f(h_2, k_2) \\ &= f((h_1, k_1)(h_2, k_2)) \\ &= f(h_2, k_2) f(h_1, k_1) \\ &= g_2 g_1 \end{aligned}$$

Contradict to G is not abelian. So G is not isomorphic to $H \times K$.

(c) $H \cap K = \{1\}$. Since $H \subseteq G, K \subseteq G$, $HK \subseteq G$. Let $g \in G$, we can write $g = |g|e^{i\theta}$. Then $h = e^{i\theta} \in H, k = |g| \in K, g = h * k$. So $G \subseteq H \times K$. Therefore, $H \times K = G$. We know that $\mathbb{C}^{\times}$ is abelian. So for any $h \in H \in G, g \in G$,

$$ghg^{-1} = gg^{-1}h = h$$

So $gHg^{-1} \in H$, H is a normal subgroup of G. Similarly, K is a normal subgroup of G. So, according to the proposition, G is isomorphic to $H \times K$.

Problem 48

Let G be a group containing normal subgroups of orders 3 and 5. Prove that G contains an element of order 15.

Solution

Let H be the group of order 3 and K be the group of order 5. Since 3 and 5 are prime numbers, H, K are cyclic groups, say $H = \langle h \rangle, K = \langle k \rangle$. Let $g = hk \in G$, $g^{15} = h^{15}k^{15} = e$. If g has order smaller than 15, it can only be $1, 3, 5$. If $g = hk = e$, then $h = k = e$, impossible. If $g^3 = h^3k^3 = k^3 = e$, $k = e$, impossible. If $g^5 = h^5k^5 = h^5 = h^2 = e$, $h = e$, impossible. So g has order 15.

Problem 49

Let $H \leqslant G$, let $\phi : G \to H$ be a homomorphism whose restriction to H is the identity map, and let $N = \ker(\phi)$. What can you say about the product function $f : H \times N \to G, f(h, n) = hn$?

Solution

$\boldsymbol{H \cap N = \{e\}}$**:** If $g \in H \cap K$, $\phi(g) = g$ because of the identity map of H, and $\phi(g) = e$ since $g \in \ker(\phi)$. So $g = e \implies H \cap K = \{e\}$.

$\boldsymbol{HN = G}$**:** Since $N, H \subseteq G$, $HN \subseteq G$. We want to prove that $G \subseteq HN$. Let $g \in G$, we have $\phi(Hg) = \phi(H)\phi(g) = H\phi(g)$. Since $\phi(g) \in H$, $\phi(Hg) = H\phi(g) = H$. So there exists some $h \in H$, such that ϕ maps hg to $e \in H$. That is, $\phi(hg) = e \implies hg \in N$. Then we can write g as $g = h^{-1}hg \in HN$. So $G \subseteq HN \implies HN = G$

H and N are normal: Since ϕ is homomorphism, $\ker(\phi) = N$ is a normal subgroup. (H normal left...)

Problem 50

$$H = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \right\} \text{ and } K = \left\{ \begin{bmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right\}$$

Show that H is a subgroup of $GL_3(\mathbb{R})$ and that K is a normal subgroup of H. Identify the quotient group H/K, and determine the center of H.

Solution

It's obvious that $H \subseteq GL_3(\mathbb{R})$. **Closure:**

$$h_1 = \begin{bmatrix} 1 & a_1 & b_1 \\ 0 & 1 & c_1 \\ 0 & 0 & 1 \end{bmatrix}, h_2 = \begin{bmatrix} 1 & a_2 & b_2 \\ 0 & 1 & c_2 \\ 0 & 0 & 1 \end{bmatrix}, h_1 h_2 = \begin{bmatrix} 1 & a_1 + a_2 & b_2 + a_1 c_2 + b_1 \\ 0 & 1 & c_1 + c_2 \\ 0 & 0 & 1 \end{bmatrix} \in H$$

Identity: $I_3 \in H$. **Inverse:**

$$h = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}, h^{-1} = \begin{bmatrix} 1 & -a & ac - b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{bmatrix}$$

So H is a subgroup.

Now check K. **Closure:**

$$k_1 = \begin{bmatrix} 1 & 0 & b_1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, k_2 = \begin{bmatrix} 1 & 0 & b_2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, k_1 k_2 = \begin{bmatrix} 1 & 0 & b_1 + b_2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \in K$$

Identity: $I_3 \in K$. **Inverse:**

$$k = \begin{bmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, k^{-1} = \begin{bmatrix} 1 & 0 & -b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Normal subgroup of H:

$$h = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}, k = \begin{bmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \implies h^{-1} = \begin{bmatrix} 1 & -a & ac - b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{bmatrix}$$

Then

$$hkh^{-1} = \begin{bmatrix} 1 & 0 & d \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \in K$$

So K is a normal subgroup.

Quotient group: If $hK = h'k$, $h'^{-1}hK = K \implies h'^{-1}h \in K$, Let

$$h = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}, h' = \begin{bmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{bmatrix}$$

Then

$$h'^{-1}h = \begin{bmatrix} 1 & a - d & b - cd - e + df \\ 0 & 1 & c - f \\ 0 & 0 & 1 \end{bmatrix} \in K$$

Then $a = d, c = f$. So

$$H/K = \left\{ hK \mid h = \begin{bmatrix} 1 & a & 0 \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \right\}$$

Center of H: $g \in Z(H) \implies gh = hg$. So let

$$g = \begin{bmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{bmatrix}$$

Then

$$\begin{bmatrix} 1 & a + db + e + af & \\ 0 & 1 & c + f \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a + db + e + cd & \\ 0 & 1 & c + f \\ 0 & 0 & 1 \end{bmatrix}$$

So $af = cd$. If the equation holds for all $a, c \in \mathbb{R}$, $d, f = 0$. Therefore, $Z(H) = K$.

Problem 51

Let $H = \{\pm 1, \pm i\}$ be the subgroup of $G = \mathbb{C}^\times$ of fourth roots of unity. Describe the cosets of H in G explicitly, and determine whether or not G/H is isomorphic to G.

Solution

$zH = \{\pm z, \pm iz\} = \{a + bi, -a - bi, ai - b, b - ai\}$.
Let $\phi : G \to G$ be defined as $\phi(z) = z^4$. ϕ is **homomorphism:** $\phi(xy) = (xy)^4 = x^4y^4$. ϕ is **surjective:** for every $x \in G$, $\phi(x^{\frac{1}{f}}) = x$. And $\ker(\phi) : \phi(z) = 1 \implies z = \pm 1$ or $\pm i \implies \ker(\phi) = H$. By First Isomorphism Theorem, $G/H \cong G$.

Problem 52

$$G = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \in GL_2(\mathbb{R}) \mid a, d \neq 0 \right\}$$

For each of the following subset, determine whether or not S is a subgroup and whether or not S is a normal subgroup. If S is a normal subgroup, identify the quotient group G/S.

(1) S is the subset with $b = 0$.

(2) S is the subset with $d = 1$.

(3) S is the subset with $a = d$.

Solution

(1) **Closure:**

$$\begin{bmatrix} a_1 & 0 \\ 0 & d_1 \end{bmatrix}\begin{bmatrix} a_2 & 0 \\ 0 & d_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 & 0 \\ 0 & d_1d_2 \end{bmatrix} \in S$$

Identity:

$$e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in S$$

Inverse:

$$\begin{bmatrix} a_1 & 0 \\ 0 & d_1 \end{bmatrix}\begin{bmatrix} \frac{1}{a_1} & 0 \\ 0 & \frac{1}{d_1} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} \frac{1}{a_1} & 0 \\ 0 & \frac{1}{d_1} \end{bmatrix}\begin{bmatrix} a_1 & 0 \\ 0 & d_1 \end{bmatrix}$$

Not normal:

$$gxg^{-1} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix} \notin S$$

(2) **Closure:**

$$\begin{bmatrix} a_1 & b_1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} a_2 & b_2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a_1a_2 & b_1 + a_1b_2 \\ 0 & 1 \end{bmatrix} \in S$$

Identity:

$$e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in S$$

Inverse:

$$\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}\begin{bmatrix} \frac{1}{a} & -\frac{b}{a} \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} \frac{1}{a} & -\frac{b}{a} \\ 0 & 1 \end{bmatrix}\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$$

Normal:

$$gxg^{-1} = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}\begin{bmatrix} m & n \\ 0 & 1 \end{bmatrix}\begin{bmatrix} \frac{1}{a} & -\frac{b}{ad} \\ 0 & \frac{1}{d} \end{bmatrix} = \begin{bmatrix} m & \frac{b+an-bm}{d} \\ 0 & 1 \end{bmatrix} \in S$$

Quotient Group: Let $gS, hS \in G/S$ such that $gS = hS \implies h^{-1}g \in S$. Let

$$g = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix}, h = \begin{bmatrix} d & e \\ 0 & f \end{bmatrix}, h^{-1} = \begin{bmatrix} \frac{1}{d} & -\frac{e}{df} \\ 0 & \frac{1}{f} \end{bmatrix}$$

Then

$$h^{-1}g = \begin{bmatrix} \frac{a}{d} & \frac{b}{d} - \frac{ce}{df} \\ 0 & \frac{c}{f} \end{bmatrix} \in S$$

So $\frac{c}{f} = 1 \implies c = f$. That is $gS \neq hS \Leftrightarrow c \neq f$. So

$$G/S = \left\{ gS \mid g = \begin{bmatrix} 1 & 0 \\ 0 & d \end{bmatrix}, d \neq 0 \right\}$$

(3) **Closure:**

$$\begin{bmatrix} a_1 & b_1 \\ 0 & a_1 \end{bmatrix}\begin{bmatrix} a_2 & b_2 \\ 0 & a_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 & b_1 + a_1b_2 \\ 0 & a_1a_2 \end{bmatrix} \in S$$

Identity:

$$e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in S$$

Inverse:

$$\begin{bmatrix} a & b \\ 0 & a \end{bmatrix}\begin{bmatrix} \frac{1}{a} & -\frac{b}{a^2} \\ 0 & \frac{1}{a} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} \frac{1}{a} & -\frac{b}{a^2} \\ 0 & \frac{1}{a} \end{bmatrix}\begin{bmatrix} a & b \\ 0 & a \end{bmatrix}$$

Normal:

$$gxg^{-1} = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}\begin{bmatrix} m & n \\ 0 & m \end{bmatrix}\begin{bmatrix} \frac{1}{a} & -\frac{b}{ad} \\ 0 & \frac{1}{d} \end{bmatrix} = \begin{bmatrix} m & \frac{b+an-bm}{d} \\ 0 & m \end{bmatrix} \in S$$

Quotient Group: Let $gS, hS \in G/S$ such that $gS = hS \implies h^{-1}g \in S$. Let

$$g = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix}, h = \begin{bmatrix} d & e \\ 0 & f \end{bmatrix}, h^{-1} = \begin{bmatrix} \frac{1}{d} & -\frac{e}{df} \\ 0 & \frac{1}{f} \end{bmatrix}$$

Then

$$h^{-1}g = \begin{bmatrix} \frac{a}{d} & \frac{b}{d} - \frac{ce}{df} \\ 0 & \frac{c}{f} \end{bmatrix} \in S$$

So $\frac{c}{f} = \frac{a}{d}$. That is $gS \neq hS \Leftrightarrow \frac{a}{c} \neq \frac{d}{f}$.

6 Homework 6

Problem 53

Let G be the group of matrices of the form $\begin{bmatrix} x & y \\ & 1 \end{bmatrix}$ where $x, y \in \mathbb{R}$ and $x > 0$. Determine the conjugacy classes in G and sketch them in the (x,y)-plane.

Solution

Let

$$A = \begin{bmatrix} a & b \\ & 1 \end{bmatrix}$$

For any $g \in G$, we have

$$g = \begin{bmatrix} x & y \\ & 1 \end{bmatrix}; g^{-1} = \begin{bmatrix} \frac{1}{x} & -\frac{y}{x} \\ & 1 \end{bmatrix}$$

So

$$Cl(A) = \{B \in G \mid B = gAg^{-1} = \begin{bmatrix} a & -ay + bx + y \\ 0 & 1 \end{bmatrix}\}$$

Since B is in G, $-ay + bx + y$ can be any real number, say c. So

$$-ay + bx + y = c$$
$$y = \frac{c - bx}{1 - a}$$

When $a \neq 1$, the graph is defined and would be linear depending on what a, b, and c is.

Problem 54

Rule out as many of the following as you can, as class equations for a group of order 10:

- 1+1+1+2+5=10
- 1+2+2+5=10
- 1+2+3+4=10
- 1+1+2+2+2+2=10

Solution

- 1+1+1+2+5=10. There are three elements whose conjugacy class has order 1. Therefore, there are three elements in $Z(G)$. But $|Z(G)|$, which equals to 3, should divide $|G|$. This class equation is wrong.
- 1+2+3+4=10. Since $|Cl(G)| \mid |G|$ and $3, 4 \nmid 10$, this class equation is wrong
- 1+1+2+2+2+2=10. Similarly, we know $|Z(G)| = 2$. Since $Z(G)$ is a normal subgroup, $G/Z(G)$ is a group which has order $\frac{10}{2} = 5$. Since 5 is prime, $G/Z(G)$ is cyclic $\implies$ G is abelian. In this case, all conjugacy classes should have order 1. So, the class equation is wrong.

Problem 55

Determine the possible class equations for the non-abelian groups of:

(a) order 8;

(b) order 21;

Solution

(a) $|G| = 8$. First consider the order of the center. If $|Z(G)| = 1$, then $8 = 1 + |O_1| + |O_2| + \dots \implies$ at least one orbit has even order. Since the order of orbit should also divide 8, the even order orbit must have order 1. Then $|Z(G)| \neq 1$. Contradiction. If $|Z(G)| = 2$, then for $x \in G \notin Z$, $Z(G) \subset Z(x) \implies |Z(x)| = 4$ or 8. Since G is not abelian, $|Z(x)| = 4$. By orbit-stabilizer theorem, $|\mathrm{Orb}(x)| = 2$. So $8 = 2 + 2 + 2 + 2$. If $|Z(G)| = 4$, $|G/Z| = 2$, a prime. So G/Z is cyclic $\implies$ G is abelian. Contradiction.So class equation of non-abelian group of order 8 is $8 = 2 + 2 + 2 + 2$

(b) $|G| = 21$. $Z(G)$ cannot have order 3 or 7. Otherwise, $|G/Z| = 7$ or 3 and G should be abelian. So $|Z(G)|$ $= 1$. Then the only possible combination that sums up to 21 is $21 = 1 + 3 + 3 + 7 + 7$.

Problem 56

Determine the class equation for the following groups:

(a) the quaternion group

(b) D_8

(c) D_{10}

Solution

(a) The quaternion group is a non-abelian group with order 8. According to problem 3, its class equation is $8 = 1 + 1 + 2 + 2 + 2$

(b) Similarly, D_8 is a non-abelian group with order 8, so its class equation is $8 = 1 + 1 + 2 + 2 + 2$

(c) D_{10} is a non-abelian group with order 10. To avoid letting D_{10}/Z has prime order, $|Z(G)| = 1$. To sums up to 10, one of the conjugacy classes must have odd order, so one conjugacy class has order 5. Then the class equation can only be $10 = 1 + 2 + 2 + 5$.

Problem 57

Determine the centralizer in $GL_3(\mathbb{R})$ for each of the following matrices:

$$(a)\begin{bmatrix}1&&\\&2&\\&&3\end{bmatrix};(b)\begin{bmatrix}1&&\\&1&\\&&2\end{bmatrix};(c)\begin{bmatrix}1&1&\\&1&\\&&1\end{bmatrix};(d)\begin{bmatrix}1&1&\\&1&1\\&&1\end{bmatrix};(e)\begin{bmatrix}&1&\\&&1\\1&&\end{bmatrix}$$

Solution

(a)

$$\begin{bmatrix}a&b&c\\d&e&f\\g&h&i\end{bmatrix}\begin{bmatrix}1&&\\&2&\\&&3\end{bmatrix}=\begin{bmatrix}1&&\\&2&\\&&3\end{bmatrix}\begin{bmatrix}a&b&c\\d&e&f\\g&h&i\end{bmatrix}$$

$$\begin{bmatrix}a&2b&3c\\d&2e&3f\\g&2h&3i\end{bmatrix}=\begin{bmatrix}a&b&c\\2d&2e&2f\\3g&3h&3i\end{bmatrix}$$

$\implies b = c = d = f = g = h = 0$. So the centralizer is $\left\{\begin{bmatrix} a & & \\ & e & \\ & & i \end{bmatrix} : a, e, i \neq 0\right\}$

(b)

$$\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}\begin{bmatrix} 1 & & \\ & 1 & \\ & & 2 \end{bmatrix} = \begin{bmatrix} 1 & & \\ & 1 & \\ & & 2 \end{bmatrix}\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$$

$$\begin{bmatrix} a & b & 2c \\ d & e & 2f \\ g & h & 2i \end{bmatrix} = \begin{bmatrix} a & b & c \\ d & e & f \\ 2g & 2h & 2i \end{bmatrix}$$

$\implies c = f = g = h = 0$. So the centralizer is $\left\{\begin{bmatrix} a & b & 0 \\ d & e & 0 \\ 0 & 0 & i \end{bmatrix} \in GL_3(\mathbb{R})\right\}$

(c)

$$\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}\begin{bmatrix} 1 & 1 & \\ & 1 & \\ & & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & \\ & 1 & \\ & & 1 \end{bmatrix}\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$$

$$\begin{bmatrix} a & a+b & c \\ d & d+e & f \\ g & g+h & i \end{bmatrix} = \begin{bmatrix} a+d & b+e & c+f \\ d & e & f \\ g & h & i \end{bmatrix}$$

$\implies a = a+d, a+b = b+e, c = c+f, d+e = e, g+h = h \implies d = 0, a = e, f = 0, g = 0$. So the centralizer is $\left\{\begin{bmatrix} a & b & c \\ 0 & a & 0 \\ 0 & h & i \end{bmatrix} \in GL_3(\mathbb{R})\right\}$

(d)

$$\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}\begin{bmatrix} 1 & 1 & \\ & 1 & 1 \\ & & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & \\ & 1 & 1 \\ & & 1 \end{bmatrix}\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$$

$$\begin{bmatrix} a & a+b & b+c \\ d & d+e & e+f \\ g & g+h & h+i \end{bmatrix} = \begin{bmatrix} a+d & b+e & c+f \\ d+g & e+h & f+i \\ g & h & i \end{bmatrix}$$

$\implies a = a+d, a+b = b+e, b+c = c+f, d = d+g, d+e = e+h, e+f = f+i, g+h = h, h+i = i \implies d = 0, a = e = i, b = f, g = 0, d = h = 0$. So the centralizer is $\left\{\begin{bmatrix} a & b & c \\ 0 & a & b \\ 0 & 0 & a \end{bmatrix} \in GL_3(\mathbb{R})\right\}$

(e)

$$\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}\begin{bmatrix} & 1 & \\ & & 1 \\ 1 & & \end{bmatrix} = \begin{bmatrix} & 1 & \\ & & 1 \\ 1 & & \end{bmatrix}\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$$

$$\begin{bmatrix} c & a & b \\ f & d & e \\ i & g & h \end{bmatrix} = \begin{bmatrix} d & e & f \\ g & h & i \\ a & b & c \end{bmatrix}$$

$\implies a = e = i, b = f = g, c = d = h$. So the centralizer is $\left\{\begin{bmatrix} a & b & c \\ c & a & b \\ b & c & a \end{bmatrix} \in GL_3(\mathbb{R})\right\}$

Problem 58

Let N be a normal subgroup of a group G. Suppose that $|N| = 5$ and $|G|$ is odd. Prove that N is contained in the center of G, i.e. that $N \leqslant Z(G)$.

Solution

Prove by contradiction: suppose N is not contained in $Z(G)$. Since N has a prime order, it's a cyclic group. Suppose $N = \{e, x, x^2, x^3, x^4\} = \langle x \rangle$. We also know N is a normal subgroup, so

$$gxg^{-1} = x^s$$

for some $0 \leqslant s \leqslant 4$. Since N is not contained in the center, there exists at least one $x^r \neq e$ such that

$$\begin{aligned} gx^rg^{-1} &\neq x^r \\ gx^rg^{-1} = (gxg^{-1})^r = x^{sr} &\neq x^r \\ sr &\not\equiv r (\text{mod } 5) \\ 5 &\nmid sr - r \\ 5 &\nmid r(s-1) \\ \text{Since } 5 \nmid r, \quad 5 &\nmid s - 1 \end{aligned}$$

Then for any $r \neq 0$, $5 \nmid r(s-1) \implies gx^rg^{-1} \neq x^r$ for any $r \neq 0$. So the four elements (except e) in N are all outside the center. Therefore, the conjugacy classes of those four elements should have order > 1. Then they would either divide into two conjugacy classes each with order 2, or be in the same conjugacy class with order 4 because any of them cannot have conjugacy class of order 3 (otherwise, one element's conjugacy class will be order 1). However, 2 or 4 doesn't divide the odd order of $G \implies$ contradiction.

Problem 59

The class sum of a group G of order 20 is $1+4+5+5+5$.

(1) Does G have a subgroup of order 5? If so, is it a normal subgroup?

(2) Does G have a subgroup of order 4? If so, is it a normal subgroup?

Solution

(1) From class equation, we know some x has conjugacy class of order 4. So $|Z(x)| = |G|/|Cl(x)| = 5$. Since centralizer is a subgroup, G has a subgroup of order 5. Since 5 is a prime, $Z(x)$ is a cyclic group. Let $Z(x) = \langle x \rangle$. If $Z(x)$ is not normal, there exists $x^r \in Z(x)$ such that for some $g \in G$, $gx^rg^{-1} = a \notin Z(x)$. We also know there can only be one group of order 5. (Quick proof: If a different subgroup H has order 5, then it's cyclic $\implies H \cap Z(x) = \{e\}$. If so, $H \times Z(x)$ would have order 25, which is larger than the order of G. So, only one subgroup of G has order 5.) Then $\langle a \rangle$ has order 2 or 4

$$
\begin{aligned}
&\implies (gx^rg^{-1})^2 = e \\
&gx^{2r}g^{-1} = e \\
&|x^r| = 2 \\
&\implies (gx^xg^{-1})^4 = e \\
&|x^r| = 4
\end{aligned}
$$

Since $x^r \in \langle x \rangle$, $|x^r| \mid |\langle x \rangle| = 5$. The above two cases are both impossible to get, so contradiction $\implies Z(x)$ is normal.

(2) Similarly, there exists y such that $|Cl(y)| = 5, |Z(y)| = 4$. So G has subgroup of order 4. If $Z(y)$ is a normal subgroup, then $G/Z(y)$ has order 5 so it's cyclic. We can write the quotient group as $\langle yZ(y) \rangle$. Similar to the proof of problem 8, we can write any elements $g, h \in G$ as $y^mZ(y), y^nZ(y)$ then prove $gh = hg$, which implies that G is abelian. But then the class equation should consist of 1's. Contradiction. So $Z(y)$ is not normal.

Problem 60

Let $Z = Z(G)$ be the center of a group G. Prove that if G/Z is cyclic, then G is abeliawn, and therefore $G = Z$

Solution

We can write $G/Z(G) = \langle xZ(G) \rangle$ for some $x \in G$. Then for any $g \in G$, we have $gZ(G) = x^mZ(G), m \in \mathbb{N}$. Then according to proposition of cosets, $gZ(G) = x^mZ(G) \implies (x^m)^{-1}g \in Z(G)$. Suppose there's another arbitrary element $h \in G$, let $(x^m)^{-1}g = z_1 \in Z(G), (x^n)^{-1}g = z_2 \in Z(G)$,

$$\begin{aligned} gh &= x^m z_1 x^n z_2 \\ &= x^m x^n z_1 z_2 \\ &= x^n z_1 x^m z_2 \\ &= hg \end{aligned}$$

So G is abelian.

Problem 61

A non-abelian group G has order p^3 for a prime p.

(1) What are the possible orders of the center $Z(G)$?

(2) Let $x \in G$ such that $x \notin Z(G)$. What is the order of its centralizer, i.e. what is $|C_G(x)|$

(3) What are the possible class sums for G?

Solution

(1) $Z(G)$ as a subgroup, may have order $1, p, p^2, p^3$. Since G is non-abelian, $Z(G) \neq G$ and G/Z is not cyclic. Since G is a p-group, its center is non-trivial. So $|Z(G)| = p$.

(2) We know $Z(G) \leqslant C_G(x)$ and $x \notin Z(G)$, so $|C_G(x)| > p$. And $|C_G(x)| \neq p^3$. Otherwise, $|Cl(x)| = \frac{p^3}{p^3} = 1 \implies x \in Z(G)$. And the order of centralizer should divide the order of G since it's a subgroup. Therefore, $|C_G(x)| = p^2$.

(3) From (2), we know for $x \notin Z(G)$, $|Cl(x)| = |G|/|C_G(x)| = p$. So the class equation is

$$p^3 = \underbrace{1 + 1 + .. + 1}_{p} + \underbrace{p + p + ... + p}_{p^2-1}$$

Problem 62

Classify groups of order 8.

Solution

Notice G is a p-group of order $8 = 2^3$.
Abelian: The class equation is $8 = 1+1+1+1+1+1+1+1$. By corollary to Abelian Group Factored by Prime, $G \cong \mathbb{Z}_8$ or $\mathbb{Z}_2 \times \mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.
Non-abelian. By Lagrange, any $x \in G, x \neq e$ may have order 2,4, and 8. We can rule out 8 first, because G would be a cyclic group generate by the order 8 elements which implies abelian otherwise. G also cannot

contain only elements of order 2. If it does, for two arbitrary elements $x, y \in G$, we have

$$\begin{aligned}(xy)^2 &= e \\ xy &= xey \\ xy &= x(xy)(xy)y \\ xy &= yx\end{aligned}$$

Then it's abelian. Therefore, G must contain one element of order 4, name it x. Let $H = \langle x \rangle \leqslant G$. Since $[G : H] = |G|/|H| = 2$, H is a normal subgroup. Let $y \neq e \in G \backslash H$, then $yxy^{-1} \in H$. Since x has order 4, $(yxy^{-1})^4 = e$. If $yxy^{-1} = e$ or $(yxy^{-1})^2 = e$, x should equal to e or have order 2. So yxy^{-1} has order 4 $\implies$ $yxy^{-1} = x$ or x^3. However, if $yxy^{-1} = x$, $yx = xy \implies |C_G(x)| > 4 \implies |C_G(x)| = 8$(same for x^2, x^3) $\implies G$ is abelian, contradiction. So $yxy^{-1} = x^3$.

Case 1: y has order 2. $G \cong D_8$ in the following way: $\phi(x) = r, \phi(y) = s$.

Case 2: y has order 4. Since G has order 8 and the order contains $\langle x \rangle$ and $\langle y \rangle$. So $1 < |\langle x \rangle \cap \langle y \rangle| < 4$ and it divides 4, so the intersection contains 2 elements. Apart from e, the intersection can only contain x^2 or y^2 (Otherwise, they are the same). So $y^2 = x^2$. Then it's easy to find that $G \cong Q_8$ in the following way: $\phi(e) = 1, \phi(x) = i, \phi(y) = j, \phi(xy) = k$