## Contents

1. Homework 1 - Solutions  
2. Homework 2 - Solutions  
3. Homework 3 - Solutions  
4. Homework 4 - Solutions  
5. Homework 5 - Solutions  
6. Homework 6 - Solutions  
7. Homework 7 - Solutions  
8. Homework 8 - Solutions  
9. Homework 9 - Solutions
HOMEWORK 1 - SOLUTIONS

Problem 1. Let $a_1, a_2, \ldots, a_n$ be elements of a group $G$. Define the product of the $a_i$’s by induction: $a_1 a_2 \cdots a_n = (a_1 a_2 \cdots a_{n-1}) a_n$.

(a) Prove that 
\[ a_1 a_2 \cdots a_n b_1 b_2 \cdots b_m = (a_1 a_2 \cdots a_n)(b_1 b_2 \cdots b_m). \]
(b) Prove that $a_1 a_2 \cdots a_n$ is equal to the product of the $a_i$’s with parentheses inserted arbitrarily.

Solution. (a) We proceed by induction on $m$. For $m = 0$, the result is obvious.

For $m \geq 1$, we have 
\[ a_1 a_2 \cdots a_n b_1 b_2 \cdots b_m = (a_1 a_2 \cdots a_n b_1 b_2 \cdots b_{m-1}) b_m. \]
Applying the inductive hypothesis, 
\[ (a_1 a_2 \cdots a_n b_1 b_2 \cdots b_{m-1}) b_m = ((a_1 a_2 \cdots a_n)(b_1 b_2 \cdots b_{m-1})) b_m. \]
Then by associativity of the group operation, 
\[ ((a_1 a_2 \cdots a_n)(b_1 b_2 \cdots b_{m-1})) b_m = (a_1 a_2 \cdots a_n)((b_1 b_2 \cdots b_{m-1}) b_m). \]
The last factor is $b_1 b_2 \cdots b_m$, so we are done.

(b) We proceed by induction on the number of pairs of parentheses. If there are no parentheses, then the statement is that $a_1 a_2 \cdots a_n = a_1 a_2 \cdots a_n$, which is true.

Now suppose that there is at least one pair of parentheses, and pick some pair which is not contained in any other. Let $A$ be the expression to the left, $B$ be the expression enclosed, and $C$ be the expression to the right, so the full expression with parentheses inserted is $A(B)C$.
If we can show that $A(B)C = ABC$ as a product of group elements (after substituting the expressions literally), then we will be done by the inductive hypothesis.
Applying part (a), we have 
\[ A(B)C = (A(B))(C), \quad ABC = (AB)(C), \]
so it suffices to show that $A(B) = AB$, as we can then multiply on the right by $(C)$ to obtain the required equality. Using the inductive definition of an arbitrary finite product with last factor $(B)$, and then applying part (a) again, 
\[ A(B) = (A)(B) = AB. \]
Problem 2. (a) Prove that for any natural \( n \), the set of all complex \( n \)-th roots of unity forms a group with respect to the complex multiplication. Show that this group is cyclic.

(b) Prove that if \( G \) is a cyclic group of order \( n \) and \( k \) divides \( n \), then \( G \) has exactly one subgroup of order \( k \).

Solution. (a) We have that \( e^{2\pi i/n} \in \mathbb{C}^\times \), so

\[
\left\{ e^{2\pi i/n} \middle| k \in \mathbb{Z} \right\} = \left\{ e^{2\pi ik/n} \middle| k = 0, 1, \ldots, n-1 \right\}
\]

is a cyclic subgroup of \( \mathbb{C}^\times \). This is precisely the set of complex \( n \)-th roots of unity.

(b) Let \( G = \langle a \rangle \) with \( |G| = n \), and let \( H \leq G \) with \( |H| = k \). Suppose \( b \in H \). Since \( a \) generates \( G \), there is some \( r \) with \( 0 \leq r < n \) such that \( b = a^r \). By Problem 4(a),

\[
b^k = (a^r)^k = a^{rk} = 1,
\]

so \( n \mid rk \). Thus \( r \) is a multiple of \( n/k \) with \( 0 \leq r < n \). There are precisely \( k \) such values of \( r \), which means that there are at most \( k \) elements of \( G \) which could possibly be in \( H \). As \( |H| = k \), in fact \( H \) must contain all of these elements. That is,

\[
H = \{1, a^{n/k}, \ldots, a^{(k-1)n/k}\} = \langle a^{n/k} \rangle
\]

is the unique subgroup of \( G \) of order \( k \).

\[\square\]

Problem 3. (a) Show that if \( K \) and \( N \) are two finite subgroups in \( G \) of relatively prime orders, then \( K \cap N = 1 \).

(b) Show that if a group \( G \) has only a finite number of subgroups, then \( G \) is finite.

Solution. (a) By Lagrange’s theorem, \( |K \cap N| \) divides both \( |K| \) and \( |N| \). As these are coprime, \( |K \cap N| = 1 \), so \( K \cap N = 1 \).

(b) We prove the contrapositive, that if \( G \) is infinite, then \( G \) has infinitely many subgroups.

First suppose that \( G \) contains an element \( a \) of infinite order. Then the cyclic subgroups \( \langle a^n \rangle \) for \( n \in \mathbb{N} \) are distinct subgroups of \( G \), so \( G \) has infinitely many subgroups.

Now suppose that every element of \( G \) has finite order. Let \( a_1 \in G \) and \( H_1 = \langle a_1 \rangle \). Then \( H_1 \) is finite, so \( G \setminus H_1 \) is an infinite set. Choose \( a_2 \in G \setminus H_2 \) and let \( H_2 = \langle a_2 \rangle \). Then \( H_2 \) is finite, so \( G \setminus (H_1 \cup H_2) \) is still an infinite set, and we can continue in this manner to find an infinite collection of distinct subgroups \( H_n \).

\[\square\]
Problem 4.  (a) Let $G$ be a group of order $n$. Show that $a^n = 1$ for all $a \in G$.
(b) Prove that a group $G$ is cyclic if and only if there is an element $a \in G$ with $\text{ord } a = |G|$.
(c) Show that every group of prime order is cyclic.

Solution.  (a) Applying Lagrange’s theorem to the subgroup $\langle a \rangle$ generated by $a$, we have that $\text{ord } a | n$. If $k \cdot \text{ord } a = n$, then $a^n = (a^\text{ord } a)^k = 1$.
(b) First suppose there is an element $a \in G$ with $\text{ord } a = |G|$. Then $H = \langle a \rangle$ is a subgroup of $G$ which contains $|G|$ elements, so $H = G$ is cyclic.
Conversely, if $G$ is cyclic, then there exists $a \in G$ such that $G = \langle a \rangle$, and then $\text{ord } a = |G|$.
(c) Let $|G| = p$ and $a \neq 1$ be an element of $G$. Then $\text{ord } a | p$, so $\text{ord } a = 1$ or $\text{ord } a = p$. The only element of order 1 is 1, so $\text{ord } a = p = |G|$, hence $G$ is cyclic by part (b).

Problem 5.  (a) Show that if $a^2 = 1$ for all elements $a$ of a group $G$, then $G$ is abelian.
(b) Prove that if $G$ is a finite group of even order, then $G$ contains an element $a$ such that $a^2 = 1$ and $a \neq 1$.
(c) Show that every subgroup of index 2 is normal.

Solution.  (a) Let $a, b \in G$. We have $a^2 = 1$, $b^2 = 1$, and $abab = (ab)^2 = 1$, so
$$ba = (abab)ba = aba(bb)a = ab(aa) = ab.$$ (b) Partition $G$ into “pairs” $\{a, a^{-1}\}$. Since $(a^{-1})^{-1} = a$, this forms a genuine partition of $G$. If $a = a^{-1}$, so that $\{a, a^{-1}\}$ is actually a singleton set, then $a^2 = 1$. Now, each set in the partition has size 1 or 2 and their total size is $|G|$, which is even, so the number of singleton sets in the partition is even. There is at least one singleton set, corresponding to $a = 1$, so there must be another singleton set $\{a\}$. This $a$ satisfies $a^2 = 1$ but $a \neq 1$.
(c) Let $N \triangleleft G$ with $[G : N] = 2$. We must show that for any $a \in G$, $aN = Na$. This is clear if $a \in N$, since both cosets are equal to $N$.
Let $a \in G \setminus N$. Since $[G : N] = 2$, the left cosets are $N$ and $aN$, while the right cosets are $N$ and $Na$. Thus $aN = G \setminus N = Na$, as left cosets partition $G$ and right cosets partition $G$.

Problem 6. Find all groups (up to isomorphism) of order $\leq 5$. What is the smallest order of a non-cyclic group?

Solution. In this problem, we repeatedly use the fact that all cyclic groups of order $n$ are isomorphic.
1. We noted in class that the trivial group is unique up to isomorphism.
2. Since 2 is prime, if $G$ has order 2, then by Problem 4c, it must be cyclic. Hence there is one isomorphism class $C_2$ of groups of order 2.
3. Since 3 is prime, we can use the same argument as for 2, so there is one isomorphism class $C_3$ of groups of order 3.

4. Let $G$ be a group of order 4 and let $a \in G$ with $a \neq 1$. By Problem 4a, ord $a \mid 4$, so ord $a = 2$ or ord $a = 4$ (it cannot be 1 since $a \neq 1$).

If there exists $a \in G$ with ord $a = 4$, then by Problem 4b, $G$ is a cyclic group of order 4 generated by $a$, and there is one isomorphism class $C_4$ of such groups.

Otherwise, every non-identity element of $G$ has order 2. Let $G = \{1, a, b, c\}$. The property that $a^2 = b^2 = c^2 = 1$ completely determines the multiplication table of $G$, as the table must be a Latin square, so there is only one other isomorphism class $V_4$ of groups of order 4. This class contains the smallest non-cyclic groups.

$$
\begin{array}{c|cccc}
 & 1 & a & b & c \\
\hline
1 & 1 & a & b & c \\
a & a & 1 & c & b \\
b & b & c & 1 & a \\
c & c & b & a & 1 \\
\end{array}
$$

We can note that $C_2 \times C_2$ is a group (isomorphism class) of order 4 in which every element has order 2, so $V_4 \cong C_2 \times C_2$.

5. Since 5 is prime, we can use the same argument as for 2 and 3, so there is one isomorphism class $C_5$ of groups of order 5.

**Problem 7.** Find a non-normal subgroup in the symmetric group $S_3$.

**Solution.** Let $H = \langle (12) \rangle = \{1, (12)\} \leq G$. This is not normal, because $(123)H = \{(123), (13)\}$ and $H(123) = \{(123), (23)\}$ are not equal to each other.

**Problem 8.** Let $n$ be a natural number. Show that the map

$$f : \mathbb{Q}/\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}, \quad f(a + \mathbb{Z}) = na + \mathbb{Z}$$

is a well-defined homomorphism. Find ker $f$ and im $f$.

**Solution.** First we show that $f$ is well-defined. Let $a + \mathbb{Z} = b + \mathbb{Z}$ for $a, b \in \mathbb{Q}$. Then $a - b \in \mathbb{N}$, so $n(a - b) = na - nb \in \mathbb{Z}$. Thus

$$f(a + \mathbb{Z}) = na + \mathbb{Z} = nb + \mathbb{Z} = f(b + \mathbb{Z}),$$

so $f$ is well-defined.

Now we check that $f$ is a homomorphism. We have

$$f((a + \mathbb{Z}) + (b + \mathbb{Z})) = f((a + b) + \mathbb{Z}) = n(a + b) + \mathbb{Z} = (na + \mathbb{Z}) + (nb + \mathbb{Z}) = f(a + \mathbb{Z}) + f(b + \mathbb{Z}),$$

6
as required.
The kernel of \( f \) consists of all cosets \( a + \mathbb{Z} \) such that \( na + \mathbb{Z} = \mathbb{Z} \), i.e. \( na \in \mathbb{Z} \). Then \( a \in \frac{1}{n} \mathbb{Z} \), and conversely, whenever \( a \in \frac{1}{n} \mathbb{Z} \), \( na \in \mathbb{Z} \), so \( f(a + \mathbb{Z}) = \mathbb{Z} \). Thus we have
\[
\ker f = \left\{ a + \mathbb{Z} \mid a \in \frac{1}{n} \mathbb{Z} \right\} = \left( \frac{1}{n} \mathbb{Z} \right) / \mathbb{Z}.
\]
For the image, given any \( a + \mathbb{Z} \in \mathbb{Q} / \mathbb{Z} \), we have \( f(a/n + \mathbb{Z}) = a + \mathbb{Z} \), so \( \text{im} f = \mathbb{Q} / \mathbb{Z} \).

**Problem 9.**

(a) Show that \( \mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \).

(b) Prove that \( n\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \).

**Solution.**

(a) Define \( f : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \) by
\[
f(a + 6\mathbb{Z}) = (a + 2\mathbb{Z}, a + 3\mathbb{Z}).
\]
We claim that \( f \) is well-defined, that \( f \) is a bijection, and that \( f \) is a homomorphism; then \( f \) is an isomorphism of the two groups.

First, we need to show that if \( a + 6\mathbb{Z} = b + 6\mathbb{Z} \), then \( f(a + 6\mathbb{Z}) = f(b + 6\mathbb{Z}) \). That is, we must have
\[
a + 2\mathbb{Z} = b + 2\mathbb{Z} \quad \text{and} \quad a + 3\mathbb{Z} = b + 3\mathbb{Z}.
\]
By assumption, we have \( 6 \mid a - b \). Therefore, \( 2 \mid a - b \), so \( a + 2\mathbb{Z} = b + 2\mathbb{Z} \). Similarly, \( 3 \mid a - b \), so \( a + 3\mathbb{Z} = b + 3\mathbb{Z} \). This completes the proof that \( f \) is well-defined.

To see that \( f \) is a bijection, we show that it is injective. If \( f(a + 6\mathbb{Z}) = f(b + 6\mathbb{Z}) \), then we require \( a + 2\mathbb{Z} = b + 2\mathbb{Z} \) and \( a + 3\mathbb{Z} = b + 3\mathbb{Z} \). Then \( 2 \mid a - b \) and \( 3 \mid a - b \), so \( 6 \mid a - b \) and \( a + 6\mathbb{Z} = b + 6\mathbb{Z} \). Hence we have injectivity of a function \( f \) from a set of size 6 to another set of size 6, so \( f \) is a bijection.

Finally, \( f \) is a homomorphism, as
\[
f((a + 6\mathbb{Z}) + (b + 6\mathbb{Z})) = f((a + b) + 6\mathbb{Z}) = ((a + b) + 2\mathbb{Z}, (a + b) + 3\mathbb{Z})
\]
\[
= (a + 2\mathbb{Z}, a + 3\mathbb{Z}) + (b + 2\mathbb{Z}, b + 3\mathbb{Z}) = f(a + 6\mathbb{Z}) + f(b + 6\mathbb{Z}).
\]
This completes the proof.

(b) Consider the homomorphism \( f : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/mn\mathbb{Z} \) defined by
\[
f(a + mn\mathbb{Z}) = an + mn\mathbb{Z}.
\]
This is a well-defined homomorphism, by the same argument as Problem 8. Its kernel is
\[
\ker f = \left\{ a + mn\mathbb{Z} \mid an \in mn\mathbb{Z} \right\} = \left\{ a + mn\mathbb{Z} \mid a \in m\mathbb{Z} \right\} = m\mathbb{Z}/mn\mathbb{Z},
\]
while its image is
\[
\text{im} f = \left\{ an + mn\mathbb{Z} \mid a + mn\mathbb{Z} \in \mathbb{Z}/mn\mathbb{Z} \right\} = n\mathbb{Z}/mn\mathbb{Z}.
\]
By the first and third isomorphism theorems,
\[
n\mathbb{Z}/mn\mathbb{Z} \cong (\mathbb{Z}/mn\mathbb{Z})/(m\mathbb{Z}/mn\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z}.
\]
Problem 10. Let $f : G \to H$ be a surjective group homomorphism and let $H'$ be a normal subgroup in $H$. Show that $G' = f^{-1}(H')$ is a normal subgroup in $G$ and $G/G' \simeq H/H'$.

Solution. First, as noted in class, since $H' \leq H$, $G' = f^{-1}(H') \leq G$. Now let $k \in G'$ and $g \in G$. Then $f(gkg^{-1}) = f(g)f(k)f(g)^{-1} \in H'$ since $f(k) \in H'$ and $H' \lhd H$, so $gkg^{-1} \in f^{-1}(H') = G'$. Thus $G'$ is normal.

Now we need to show that $G/G' \simeq H/H'$. Since $1 \in H'$, ker $f \triangleleft G'$. By the first isomorphism theorem applied to $f$ and $f|_{G'}$, we have

$$G/\ker f \simeq H, \quad G'/\ker f \simeq H'.$$

Then by the third isomorphism theorem,

$$H/H' \simeq (G/\ker f)/(G'/\ker f) \simeq G/G'.$$

\qed
HOMEWORK 2 - SOLUTIONS

Problem 1. Let $G$ be a group and $a, b \in G$.

(a) Prove that $a^n \cdot a^m = a^{n+m}$ and $(a^n)^m = a^{nm}$.

(b) Prove that $\text{ord}(a^n) = \text{ord} a / \gcd(n, \text{ord} a)$ if $\text{ord} a < \infty$.

(c) Prove that $\text{ord}(ab) = \text{ord} a \cdot \text{ord} b$ if $a$ and $b$ commute and $\gcd(\text{ord} a, \text{ord} b) = 1$.

Solution. (a) We do this in three steps.

$a^n \cdot a = a^{n+1}$. For $n \geq 0$, this is immediate from the definition of $a^n$.

If $n < 0$, then write $n = -m$ for $m > 0$. We have

$$a^n \cdot a = a^{-m} \cdot a = a^{-1} \cdots a^{-1} a = a^{-m+1} = a^{n+1}.$$

$a^n \cdot a^m = a^{n+m}$. We fix $n$ and prove the result for all $m \in \mathbb{Z}$ by forwards and backwards induction. The previous step establishes it for $m = 1$, so we take this as our base case. Suppose $a^n \cdot a^m = a^{n+m}$. Then

$$a^n \cdot a^{m+1} = a^n \cdot a^m \cdot a = a^{n+m} \cdot a = a^{n+(m+1)}.$$

In the other direction,

$$a^n \cdot a^{m-1} \cdot a = a^n \cdot a^m = a^{n+m} = a^{n+(m-1)} \cdot a,$$

so by the cancellation law, $a^n \cdot a^{m-1} = a^{n+(m-1)}$. This completes the inductive steps.

$(a^n)^m = a^{nm}$. As before, we fix $n$ and induct on $m$ in both directions. For $m = 0$, we have $(a^n)^0 = 1 = a^0 = a^{n \cdot 0}$, so we have our base case.

If $(a^n)^m = a^{nm}$, then going forwards,

$$ (a^n)^{m+1} = (a^n)^m \cdot a^n = a^{nm} \cdot a^n = a^{nm+n} = a^{n(m+1)}, $$

and going backwards,

$$ (a^n)^{m-1} \cdot a^n = (a^n)^m = a^{nm} = a^{nm-n} \cdot a^n = (a^n)^{m-1} = a^{nm-n} = a^{n(m-1)}, $$

by the cancellation law.

(b) Let $m = \text{ord} a$, $d = \gcd(n, m)$, $n = kd$, and $m = ld$, with $\gcd(k, l) = 1$. We must show that

$$ \frac{\text{ord}(a^n)}{\gcd(n, \text{ord} a)} = \frac{m}{d} = l. $$

First, we have

$$ (a^n)^l = a^{nld} = a^{kd} = a^{km} = (a^m)^k = 1, $$
so \( \text{ord}(a^n) \mid l \). Conversely, we must have \( m \mid n \text{ord}(a^n) \) since \((a^n)^{\text{ord}(a^n)} = a^{n \text{ord}(a^n)} = 1 \), so

\[
\frac{n \text{ord}(a^n)}{m} = \frac{kd \text{ord}(a^n)}{ld} = \frac{k \text{ord}(a^n)}{l} \in \mathbb{N}.
\]

Since \( \gcd(k, l) = 1 \), we have \( l \mid \text{ord}(a^n) \). Thus \( l = \text{ord}(a^n) \), as required.

(c) Let \( m = \text{ord} a \) and \( n = \text{ord} b \). By assumption, \( \gcd(m, n) = 1 \).

First, we have

\[(ab)^{mn} = a^{mn} b^{mn} = (a^m)^n (b^n)^m = 1,
\]

so \( \text{ord}(ab) \mid mn \). Conversely, \( 1 = (ab)^{\text{ord}(ab)} = a^{\text{ord}(ab)} b^{\text{ord}(ab)} \), so \( b^{\text{ord}(ab)} = (a^{\text{ord}(ab)})^{-1} \). Thus \( a^{\text{ord}(ab)} \) and \( b^{\text{ord}(ab)} \) have the same order, and using part b, we get

\[
\frac{m}{\gcd(m, \text{ord}(ab))} = \text{ord}(a^{\text{ord}(ab)}) = \text{ord}(b^{\text{ord}(ab)}) = \frac{n}{\gcd(n, \text{ord}(ab))}.
\]

Since \( m \) and \( n \) are relatively prime, we need \( m \mid \gcd(m, \text{ord}(ab)) \) and \( n \mid \gcd(n, \text{ord}(ab)) \), so \( m \mid \text{ord}(ab) \) and \( n \mid \text{ord}(ab) \). Thus \( mn \mid \text{ord}(ab) \), so \( \text{ord}(ab) = mn \).

\[
\square
\]

**Problem 2.** Let \( H \leq G \) be a subgroup. Show that the correspondence \( Ha \mapsto (Ha)^{-1} = a^{-1}H \) is a bijection between the sets of right and left cosets.

**Solution.** This is well-defined, since if \( Ha = Hb \), then

\[
a^{-1}H = (Ha)^{-1} = (Hb)^{-1} = b^{-1}H.
\]

It is also invertible, with inverse \( aH \mapsto (aH)^{-1} = Ha^{-1} \), as

\[
aH \mapsto Ha^{-1} \mapsto (a^{-1})^{-1}H = aH; \quad Ha \mapsto a^{-1}H \mapsto H(a^{-1})^{-1} = Ha.
\]

Thus the claimed correspondence is a bijection between the sets of left and right cosets. \( \square \)

**Problem 3.** Let \( H \leq G \) be a subgroup. Suppose that for any \( a \in G \), there exists \( b \in G \) such that \( aH = Hb \). Show that \( H \) is normal in \( G \).

**Solution.** Let \( a \in G \) be arbitrary, and choose \( b \) so that \( aH = Hb \). Then for some \( h \in H \), we have \( a = hb \), so \( b = h^{-1}a \). This gives \( aH = Hb = Hh^{-1}a = Ha \). Thus \( H \triangleleft G \) is normal. \( \square \)

**Problem 4.** Let \( f : G \to H \) be a surjective group homomorphism.

(a) Let \( H' \) be a subgroup of \( H \). Show that \( G' = f^{-1}(H') \) is a subgroup of \( G \). Prove that the correspondence \( H' \mapsto G' \) is a bijection between the set of all subgroups of \( H \) and the set of all subgroups of \( G \) containing \( \ker f \).

(b) Let \( H' \) be a normal subgroup of \( H \). Show that \( G' = f^{-1}(H') \) is a normal subgroup of \( G \). Prove that \( G/G' \cong H/H' \) and the correspondence \( H' \mapsto G' \) is a bijection between the set of all normal subgroups of \( H \) and the set of all normal subgroups of \( G \) containing \( \ker f \).
Problem 5. (a) Let $N$ be a subgroup in the center $Z(G)$ of $G$. Show that $N$ is normal in $G$. Prove that if the factor group $G/N$ is cyclic, then $G$ is abelian.

(b) Prove that every group of order $p^2$ (for a prime $p$) is abelian.

Solution. (a) For any $g \in G$, $gNg^{-1} = gg^{-1}N = N$ as $N \leq Z$, so $N$ is normal.

If $G/N = (gN)$ is cyclic, then every element of $G$ can be written as $g^n$ for some $n \in N \leq Z$. Then $g(g'n) = ggn = (g^n)g$, so $g$ commutes with every element of $G$, i.e. $g \in N$. Thus $G/N = \langle N \rangle = \{N\}$ is trivial, i.e. $G = N \leq Z \leq G$, so $Z = G$.

(b) If $|G| = p^2$, then $Z$ is non-trivial, so $|Z| = p$ or $|Z| = p^2$. In the first case, $|G/Z| = p$, so $G/Z$ is cyclic, and by part a, $G$ is abelian. (Also, we get a contradiction to $|Z| = p$.) In the second case, $Z = G$, so $G$ is abelian.

Problem 6. Prove that if a group $G$ contains a subgroup $H$ of finite index, then $G$ contains a normal subgroup $N$ of finite index such that $N \leq H$.

Solution. Consider the action of $G$ on $G/H$ by left multiplication, and let $f : G \to S(G/H)$ be the induced homomorphism. If $g \in N = \ker f$, then $gH = H$, so $g \in H$ and $N \leq H$. Then $N \leq G$ and $G/N \simeq \ker f \leq S(G/H)$. Since $H$ has finite index in $G$, $S(G/H)$ is a finite group, so $N$ has finite index in $G$.

Problem 7. (a) Show that the group $\text{Inn } G$ of all inner automorphisms of a group $G$ (given by $a \mapsto gag^{-1}$ for some $g \in G$) is a normal subgroup in $\text{Aut } G$. 

\[\square\]
(b) Find all automorphisms of all (finite and infinite) cyclic groups.

**Solution.** (a) Let $\varphi \in \text{Aut } G$ and $f_g \in \text{Inn } G$ with $f_g : a \mapsto gag^{-1}$. Then

$$\varphi \circ f_g \circ \varphi^{-1} : a \mapsto \varphi(g\varphi^{-1}(a)g^{-1}) = \varphi(g)a\varphi(g)^{-1},$$

so $\varphi \circ f_g \circ \varphi^{-1} = f_{\varphi(g)} \in \text{Inn } G$, hence $\text{Inn } G \triangleleft \text{Aut } G$.

(b) Let $G = \langle a \rangle$ be cyclic and let $f \in \text{Aut } G$. Then $G = f(G) = \langle f(a) \rangle$, so $f(a)$ is a generator of $G$. Conversely, given any generator $b$ of $G$, defining $f(a^k) = b^k$ for all $k$ gives a well-defined automorphism of $G$.

If $G$ is infinite, then $G \cong \mathbb{Z}$, which has generators $\pm 1$. If $f(1) = 1$, then $f(n) = n$, so $f = \text{id}_\mathbb{Z}$. If $f(1) = -1$, then $f(n) = -n$, so $f = -\text{id}_\mathbb{Z}$.

If $G = \langle a \rangle$ is finite with $|G| = n$, then the generators are $a^k$ for $k$ such that $\text{gcd}(k, n) = 1$. The automorphisms are defined by $a \mapsto a^k$, and $\text{Aut } G \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

\[ \Box \]

**Problem 8.** Prove that if $G$ has no non-trivial automorphisms, then $G$ is abelian and $g^2 = 1$ for all $g \in G$.

**Solution.** If $G$ has no non-trivial automorphisms, then it has no non-trivial inner automorphisms, so $gag^{-1} = a$ for all $a, g \in G$, hence $G$ is abelian.

Since $G$ is abelian, $g \mapsto g^{-1}$ is an automorphism of $G$. This must be trivial, so $g = g^{-1} \iff g^2 = 1$ for all $g \in G$.

**Problem 9.** Let $x$ and $x'$ be two elements in the same orbit under some action of a group $G$ on a set. Show that the stabilizers $G_x$ and $G_{x'}$ are conjugate in $G$.

**Solution.** Since $x$ and $x'$ are in the same orbit, we can find $g \in G$ such that $x' = gx$. We claim that $G_{x'} = gG_xg^{-1}$. Given $h \in G_x$ we have

$$ (ghg^{-1})x' = (ghg^{-1})(gx) = ghx = gx = x', $$

so $gG_xg^{-1} \leq G_{x'}$. Conversely, the same reasoning applied to $x = g^{-1}x'$ gives $g^{-1}G_{x'}g \leq G_x$, so $G_{x'} \leq gG_xg^{-1}$. Thus $G_{x'} = gG_xg^{-1}$.

\[ \Box \]

**Problem 10.** Let a group $G$ act on two sets $X$ and $Y$. We say that $X$ and $Y$ are $G$-isomorphic if there is a bijection $f : X \to Y$ such that $f(gx) = g(f(x))$ for every $x \in X$ and $g \in G$. Prove that if $G$ acts on $X$ transitively, then $X$ is $G$-isomorphic to the set of left cosets $G/H$ for some subgroup $H \leq G$ (with the action of $G$ on $G/H$ by left translations).

**Solution.** Pick some $x_0 \in X$ and let $H = G_{x_0}$. To define a map $\varphi : X \to G/H$, since the action of $G$ on $X$ is transitive, for any $x \in X$, there exists $g \in G$ such that $x = gx_0$. We set $\varphi(x) = gG_{x_0}$.

\[ \varphi \text{ is well-defined.} \] Suppose $x = gx_0 = hx_0$. Then $h^{-1}g \in G_{x_0}$, so $hG_{x_0} = gG_{x_0}$.
φ is a bijection. Define ψ : G/H → X by gGx₀ → gx₀. This is well-defined, as if hGx₀ = gGx₀, then h⁻¹g ∈ Gx₀, so h⁻¹gx₀ = x₀ =⇒ gx₀ = hx₀. Then if x = gx₀, we have

$$(\psi \circ \varphi)(x) = \psi(gGx₀) = gx₀ = x; \quad (\varphi \circ \psi)(gGx₀) = \varphi(gx₀) = gGx₀.$$ 

Thus φ is a bijection, with inverse ψ.

φ is a G-isomorphism. Let x = gx₀ and h ∈ G be arbitrary. Then

$$\varphi(hx) = \varphi(hgx₀) = hgGx₀ = h(gGx₀) = h\varphi(x).$$

□
HOMEWORK 3 - SOLUTIONS

Problem 1. Let $H$ be a $p$-subgroup of a finite group $G$. Show that if $H$ is not a Sylow $p$-subgroup, then $N_G(H) \neq H$.

Solution. We showed in class that under these hypotheses, there exists a subgroup $K$ with $|K| = p \cdot |H|$ and $H \triangleleft K$. Thus $N_G(H) \supset K$ cannot be $H$. \hfill $\Box$

Problem 2. Let $G$ be a $p$-group and let $k$ be a divisor of $|G|$. Prove that $G$ contains a normal subgroup of order $k$.

Solution. Let $|G| = p^n$. We proceed by induction on $n$. For the base case $n = 1$, the result is clear since the only divisors of $p$ are 1 and $p$, corresponding to normal subgroups 1 and $G$.

In general, let $k = p^m$ for $m \leq n$. We showed in class that the center $Z$ of $G$ is non-trivial. Then its order is divisible by $p$, so by Cauchy’s theorem, it contains an element $x$ of order $p$. If $N = \langle x \rangle \leq Z$, then $N$ is a normal subgroup of $G$ of order $p$, so $G/N$ is a $p$-group of order $p^{n-1}$. By the inductive hypothesis, it contains a subgroup of order $p^{m-1}$, and the correspondence theorem tells us that $G$ has a subgroup of order $p^m$ containing $N$. \hfill $\Box$

Problem 3. Prove that if a group $G$ contains a subgroup $H$ of finite index, then $G$ contains a normal subgroup $N$ of finite index such that $N \subset H$.

Solution. This was Homework 2 Problem 6. \hfill $\Box$

Problem 4. Let $G$ be a $p$-group and $H$ a normal subgroup in $G$ of order $p$. Show that $H \subset Z(G)$.

Solution. Since $H$ is a normal subgroup of $G$, the latter acts on $H$ by conjugation, and the orbits are conjugacy classes in $G$. By orbit stabilizer and the fact that $G$ is a $p$-group, each of these conjugacy classes has size 1 or has size divisible by $p$. Since the total size of all of these classes must be $|H| = p$, either there is a single class of size $p$ or every class has size 1. As the conjugacy class of $1 \in H$ is of size 1, the latter is the case, so $H \subset Z$. \hfill $\Box$

Problem 5. (a) A subgroup $H$ of $G$ is called characteristic if $f(H) = H$ for every automorphism $f$ of $G$. Show that a characteristic subgroup $H$ is normal in $G$.

(b) Prove that if $K$ is a characteristic subgroup of $H$ and $H$ is a characteristic subgroup of $G$, then $K$ is characteristic in $G$.

Solution. (a) If $H$ is characteristic in $G$, then in particular it is fixed by every inner automorphism, i.e. $gHg^{-1} = H$ for each $g \in G$. Thus $H$ is normal in $G$.

(b) Let $f : G \to G$ be an automorphism of $G$. Then, since $f$ is injective and $H$ is characteristic in $G$, we have $f(H) = H$, so we can restrict $f$ to an automorphism of $H$. This restriction then fixes $K$ since $K$ is characteristic in $H$, i.e. $f(K) = K$. Thus $K$ is characteristic in $G$. \hfill $\Box$

Problem 6. For a group $G$, set $G^{(0)} = G$ and $G^{(i+1)} = [G^{(i)}, G^{(i)}]$ for $i \geq 0$. Show that $G^{(i)}$ is a characteristic subgroup of $G$. 

15
Solution. By induction on $i$ and applying Problem 5b, it is sufficient to show that for any group $G$, $[G, G]$ is a characteristic subgroup of $G$. Let $f : G \to G$ be an automorphism of $G$. Since $[G, G]$ is generated by the commutators $[g, h] = ghg^{-1}h^{-1}$, it is sufficient to show that the image of each commutator lies in $[G, G]$. For this, we have
\[ f([g, h]) = f(ghg^{-1}h^{-1}) = f(g)f(h)f(g)^{-1}f(h)^{-1} = [f(g), f(h)] \in [G, G]. \]

\[ \square \]

Problem 7. (a) For any two subgroups $K$ and $H$ of a group $G$, denote by $[K, H]$ the subgroup in $G$ generated by the commutators $[k, h] = khk^{-1}h^{-1}$ for all $k \in K$ and $h \in H$. Show that if $K$ and $H$ are normal in $G$, then so is $[K, H]$.

Solution. In each case, to show that a subgroup is normal, it is sufficient to show that the conjugates of generators lie in the subgroup.

(a) Let $k \in K$, $h \in H$, and $g \in G$. Then
\[ g[k, h]g^{-1} = gkhk^{-1}h^{-1}g^{-1} = (kg^{-1})(ghg^{-1})(gh^{-1}g^{-1}) = [kg^{-1}, ghg^{-1}]. \]
This is in $[K, H]$ by normality of $K$ and $H$ in $G$.

(b) Let $g, k \in G$ and $h \in H$. Then
\[ k[g, h]k^{-1} = kghg^{-1}h^{-1} = (kg)(kg)^{-1}h^{-1} \cdot hkhk^{-1} = [kg, h] \cdot [k, h]^{-1} \in [G, H]. \]

\[ \square \]

Problem 8. Let $G$ be a group and $Z(G)$ the center of group. Show that if $G/Z(G)$ is nilpotent, then so is $G$.

Solution. Let $G/Z = G_0/Z \geq G_1/Z \geq \cdots \geq G_n/Z = Z/Z$ with $G_i/Z \triangleleft G/Z$ and $(G_i/Z)/(G_{i+1}/Z) \subset Z((G/Z)/(G_{i+1}/Z))$, where the $G_i$ are subgroups of $G$ containing $Z$. Then we have a corresponding descending chain
\[ G = G_0 \geq G_1 \geq \cdots \geq G_n = Z \geq 1. \]
Since $G_i/Z \triangleleft G/Z$, we have $G_i \triangleleft G$ by the correspondence theorem. For $i < n$, the third isomorphism theorem gives
\[ G_i/G_{i+1} \xrightarrow{\sim} (G_i/Z)/(G_{i+1}/Z) \xrightarrow{\subset} Z((G/Z)/(G_{i+1}/Z)) \xrightarrow{\sim \pi^{-1}} Z(G/G_{i+1}), \]
so $G_i/G_{i+1} \subset Z(G/G_{i+1})$. For $i = n$, we have $Z/1 \subset Z(G/1)$. Thus we have obtained a descending chain for $G$ which has the required properties for $G$ to be nilpotent. \[ \square \]
**Problem 9.** Assume that a subset $S \subset G$ of a group satisfies $gSg^{-1} \subset S$ for all $g \in G$. Prove that the subgroup generated by $S$ is normal in $G$.

*Solution.* The subgroup $H$ generated by $S$ is the smallest subgroup of $G$ containing $S$, which is equal to the intersection of all subgroups of $G$ containing $S$, since this is a non-empty family ($G \supset S$) and the intersection of subgroups is a subgroup. For any $g \in G$, $gHg^{-1}$ is a subgroup of $G$, and since $gSg^{-1} \subset S$, we have $S \subset gHg^{-1}$. Thus $H \subset gHg^{-1}$ for all $g \in G$, so $H$ is normal. \hfill \square

**Problem 10.** Let $N$ be an abelian normal subgroup in a finite group $G$. Assume that the orders $|G/N|$ and $|	ext{Aut } N|$ are relatively prime. Prove that $N$ is contained in the center of $G$.

*Solution.* Since $N$ is normal in $G$, there is a homomorphism

\[ \varphi : G \rightarrow \text{Aut } N \]

\[ g \mapsto (n \mapsto gng^{-1}). \]

Since $N$ is abelian, $N \subset \ker \varphi$. By the first and third isomorphism theorems,

\[ \text{Aut } N \supset \text{im } \varphi \simeq G/\ker \varphi \simeq (G/N)/((\ker \varphi)/N), \]

so in particular since all groups involved are finite, $|\text{im } \varphi|$ divides both $|\text{Aut } N|$ and $|G/N|$. The latter two are relatively prime, so $|\text{im } \varphi| = 1$. Thus the map $n \mapsto gng^{-1}$ is trivial for all $g \in G$, i.e. $gng^{-1} = n$ for all $n \in N$ and $g \in G$. Hence $N \subset Z$. \hfill \square
HOMEWORK 4 - SOLUTIONS

Problem 1. Determine all conjugacy classes in $S_n$ for $n \leq 4$.

Solution. The conjugacy classes are determined by cycle types, which correspond to partitions.

$n = 1$. Here $S_1$ is a trivial group, so the only conjugacy class is the one containing the identity.

$n = 2$. The partition $2 = 2$ corresponds to the conjugacy class of the only transposition $\{(1, 2)\}$, while the partition $2 = 1 + 1$ corresponds to the conjugacy class of the identity permutation.

$n = 3$. We list the conjugacy classes according to partition.

$3 = 3$. The conjugacy class of 3-cycles has two elements, $(1, 2, 3)$ and $(1, 3, 2)$.

$3 = 2 + 1$. The conjugacy class of transpositions has three elements, $(1, 2)$, $(2, 3)$, and $(3, 1)$.

$3 = 1 + 1 + 1$. The conjugacy class of the identity element contains just the identity.

$n = 4$. We list the conjugacy classes according to partition.

$4 = 4$. The conjugacy class of 4-cycles has six elements.

$4 = 3 + 1$. The conjugacy class of 3-cycles has eight elements.

$4 = 2 + 2$. The conjugacy class of double transpositions has three elements.

$4 = 2 + 1 + 1$. The conjugacy class of transpositions has six elements.

$4 = 1 + 1 + 1 + 1$. The conjugacy class of the identity element has one element.

Problem 2. Determine all subgroups in $A_4$. Show that $A_4$ has no subgroups of order 6.

Solution. The order of a subgroup $H$ must divide $|A_4| = 12$, so we proceed by order. Let $id \in A_4$ be the identity permutation on four elements.

$|H| = 1$. There is only the trivial subgroup $\{id\}$.

$|H| = 2$. This must be a cyclic subgroup generated by an element of order 2. There are three such elements in $A_4$, namely the double transpositions, so the subgroups of order 2 are

$$\{id, (1, 2)(3, 4)\}, \quad \{id, (1, 3)(2, 4)\}, \quad \{id, (1, 4)(2, 3)\}.$$

$|H| = 3$. This must be a cyclic subgroup generated by an element of order 3. There are eight such elements in $A_4$, namely the 3-cycles, and two of them are in each subgroup of order 3, so the four subgroups of order 3 are

$$\{id, (1, 2, 3), (1, 3, 2)\} \quad \{id, (1, 2, 4), (1, 4, 2)\} \quad \{id, (1, 3, 4), (1, 4, 3)\} \quad \{id, (2, 3, 4), (2, 4, 3)\}.$$
Problem 4. Show that $|H| = 4$. Here $H$ cannot contain any element of order 3, which leaves only four elements which could be in $H$, namely id and the three double transpositions. By direct computation, it can be seen that $H = \{\text{id}, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$ is a subgroup of $A_4$.

Problem 3. (a) Prove that $S_n$ is generated by $(1, 2), (1, 3), \ldots, (1, n)$.

(b) Prove that $S_n$ is generated by two cycles $(1, 2)$ and $(1, 2, \ldots, n)$.

Solution. (a) Every element of $S_n$ can be written as a product of transpositions, so it suffices to show that we can obtain every transposition. This follows from $(i, j) = (1, i)(1, j)(1, i)$.

(b) We can generate
\[
(2, 3) = (1, 2, \ldots, n)(1, 2)(1, 2, \ldots, n)^{-1},
\]
\[
(3, 4) = (1, 2, \ldots, n)(2, 3)(1, 2, \ldots, n)^{-1},
\]
and so on, up to $(n - 1, n)$. From there, we have
\[
(1, 3) = (2, 3)(1, 2)(2, 3),
\]
\[
(1, 4) = (3, 4)(1, 3)(3, 4),
\]
and so on, until we get all of the transpositions listed in part a. Since those are enough to generate $S_n$, the two cycles we started with are enough to generate $S_n$.

Problem 4. Show that $A_n\ (n \geq 4)$ and $S_n\ (n \geq 3)$ have trivial center.

Solution. Let $\sigma \in A_n$ with $\sigma$ not the identity. If $\sigma$ in its disjoint cycle representation contains a $k$-cycle with $k \geq 4$, say $\sigma = (a, b, c, \ldots, d)\tau$, then $(a, b, c)\sigma(a, b, c)^{-1} = (b, c, a, \ldots, d)\tau \neq \sigma$, so $\sigma \notin Z(A_n)$. Otherwise, $\sigma = (a, b)\tau$ or $\sigma = (a, b, c)\tau$ for some $\tau \in A_n$. Since $n \geq 4$, there is an index $d$ which is not $a$, $b$, or $c$. Then $(a, b, d)\sigma(a, b, d)^{-1} = (b, d)(a, b, d)\tau(a, b, d)^{-1}$ (in the first case) or $(a, b, d)\sigma(a, b, d)^{-1} = (b, d, c)(a, b, d)\tau(a, b, d)^{-1}$ (in the second case). In either case this is distinct from $\sigma$, so $\sigma \notin Z(A_n)$. Thus $Z(A_n)$ must be trivial.

The same argument shows that $S_n$ has trivial center for $n \geq 3$. If $\sigma$ contains a $k$-cycle with $k \geq 3$, say $\sigma = (a, b, \ldots, c)\tau$ for $\tau \in S_n$, then $(a, b)\sigma(a, b)^{-1} = (b, a, c, \ldots, c)\tau \neq \sigma$. Otherwise, $\sigma = (a, b)\tau$ for some $\tau \in S_n$, and since $n \geq 3$ there is an index $c$ which is not $a$ or $b$. From this we obtain $(a, c)\sigma(a, c)^{-1} = (c, b)(a, c)\tau(a, c)^{-1} \neq \sigma$, so in either case $\sigma \notin Z(S_n)$. □
Problem 5. (a) Show that the centralizer of $A_n$ in $S_n$ (the subgroup in $S_n$ consisting of all elements which commute with all elements of $A_n$) is trivial if $n \geq 4$.

(b) Let $g \in S_n$ be an odd transformation. Show that the map $f : A_n \rightarrow A_n$ given by $f(x) = gxg^{-1}$ is an automorphism. Prove that $f$ is not an inner automorphism if $n \geq 3$.

Solution. (a) Let $H$ be the centralizer of $A_n$ in $S_n$. Then $H \cap A_n = Z(A_n)$ is trivial for $n \geq 4$ by Problem 4, so the second isomorphism theorem gives $|H| \leq |S_n : A_n| = 2$. Suppose $|H| = 2$, so the non-identity element of $H$ is of the form $\sigma = (a, b)\tau$ for some $\tau$ which is a product of disjoint transpositions. Picking $c$ which is not $a$ or $b$, we have

$$(a, b, c)\sigma(a, b, c)^{-1} = (b, c)[(a, b, c)(a, b, c)^{-1}] \neq \sigma,$$

so $\sigma$ fails to commute with all of $A_n$, contradiction. Hence $|H| = 1$, and $H$ is trivial.

(b) The map $f$ is an automorphism since conjugation by a group element always induces an automorphism of a normal subgroup. To see that it is not an inner automorphism if $g$ is odd and $n \geq 3$, suppose that for some $h \in A_n$ we have $gxg^{-1} = hxh^{-1}$ for all $x \in A_n$. Then $h^{-1}g$ is in the centralizer of $A_n$ in $S_n$, so for $n \geq 4$, we have $h = g$, a contradiction since $g$ is odd. In the case $n = 3$, the inner automorphism group of $A_3$ is trivial since $A_3$ is abelian, while conjugation by an odd element of $S_3$ is not trivial.

Problem 6. Prove that every automorphism of $S_3$ is inner and that $\text{Aut} S_3$ is isomorphic to $S_3$.

Solution. Let $f \in \text{Aut} S_3$. By Problem 3b, $(1, 2)$ and $(1, 2, 3)$ generate $S_3$, so an automorphism is determined by their images. We must send $(1, 2)$ to an element of order 2, of which there are 3, and we must send $(1, 2, 3)$ to an element of order 3, of which there are 2. Thus $|\text{Aut} S_3| \leq 3 \cdot 2 = 6$. On the other hand, $Z(S_3) = 1$ by Problem 4, so $\text{Aut} S_3 \geq \text{Inn} S_3 \simeq S_3/Z(S_3) \simeq S_3$, and hence $|\text{Aut} S_3| \geq |\text{Inn} S_3| = |S_3| = 6$. Thus $|\text{Aut} S_3| = 6$ and $\text{Aut} S_3 = \text{Inn} S_3 \simeq S_3$.

Problem 7. Describe all Sylow subgroups of $S_5$.

Solution. As $|S_5| = 120 = 2^3 \cdot 3 \cdot 5$, we consider the primes $p = 2, 3, 5$.

$p = 2$. The Sylow 2-subgroups have order 8 and are all conjugate, hence isomorphic. There is an embedding of the dihedral group $D_8 \hookrightarrow S_4 \hookrightarrow S_5$ which produces the subgroup generated by $(1, 2, 3, 4)$ and $(1, 3)$, so the Sylow 2-subgroups are isomorphic to $D_8$. In general we can generate a Sylow 2-subgroup with $(a, b, c, d)$ and $(a, c)$. There are 15 subgroups of this form, noting that there are 30 4-cycles and $(d, c, b, a)$ gives the same subgroup as $(a, b, c, d)$. Since the number of Sylow 2-subgroups must divide 15, we have identified all of them.

$p = 3$. The Sylow 3-subgroups have order 3, so are cyclic, generated by a 3-cycle. There are 20 3-cycles, and each Sylow 2-subgroup contains 2 of them, so we have 10 Sylow 3-subgroups.

$p = 5$. The Sylow 5-subgroups have order 5, so are cyclic, generated by a 5-cycle. There are 24 5-cycles, and each Sylow 5-subgroup contains 4 of them, so we have 6 Sylow 5-subgroups.

□
Problem 8. Show that every subgroup in $S_n$ of index $n$ is isomorphic to $S_{n-1}$.

Solution. Let $H \leq S_n$ be a subgroup of index $n$ and consider the action of $S_n$ on $S_n/H$ by left multiplication. Let $f : S_n \to S(S_n/H)$ be the associated homomorphism; note that $\ker f \leq H$ since an element of $\ker f$ must stabilize $H$. Then $[S_n : \ker f] \geq [S_n : H] = n$. For $n \neq 4$, the only normal subgroups of $S_n$ are $1$, $A_n$, and $S_n$, so putting our observations together, it follows that $\ker f$ must be trivial. For $n = 4$, we also have the possibility that $\ker f$ is the normal subgroup of order 4 containing the identity and the double transpositions. However, in this case, $|H| = 6$ and $\ker f \leq H$ has order 4, which is a contradiction. Hence $\ker f$ is always trivial.

Consider the image of $H$ in $S(S_n/H)$. Left multiplication by $h \in H$ fixes $H$ and permutes the other cosets of $H$, so we can regard it as a permutation in $S_{n-1}$, i.e. $f$ induces a homomorphism $H \to S_{n-1}$. This is injective since $\ker f$ is trivial and $H \leq S_n$, and $|H| = n!/n = (n-1)! = |S_{n-1}|$. Thus the induced homomorphism is actually an isomorphism.

Problem 9. (a) Show that for $n \neq 4$, every proper subgroup in $A_n$ has index at least $n$.

(b) Prove that there are no injective homomorphisms $S_n \to A_{n+1}$ for $n \geq 2$.

Solution. (a) For $n = 1, 2$, this is clear, so suppose $n \geq 3$. Let $H < A_n$ be a proper subgroup and consider the action of $A_n$ on $A_n/H$ by left multiplication. Let $f : A_n \to S(A_n/H)$ be the associated homomorphism. Then $\ker f \leq A_n$ and $\ker f \leq H$, so the fact that $A_n$ is simple for $n \neq 4$ means that $\ker f$ is trivial. Thus $f$ is injective, so $|A_n| = n!/2$ is at most $|S(A_n/H)| = ([A_n : H])$. For $n \geq 3$, this means that $|A_n : H| \geq n$, as required.

(b) The image of $S_n$ in $A_{n+1}$ would be a subgroup of $A_{n+1}$ of index $(n+1)!/2n! < n$ for $n \geq 2$. This rules out every case except for $n = 3$. In this case, the image of $S_3$ would be a subgroup of $A_4$ of order 6, but no such subgroup exists by Problem 2.

Problem 10. (a) Show that for any $n \geq 1$, there is an injective homomorphism $S_n \to A_{n+2}$.

(b) Prove that every finite group is isomorphic to a subgroup of a finite simple group.

Solution. (a) Let $H = ((n+1, n+2)) \leq S_{n+2}$. This has order 2, so there is an isomorphism $\phi : \{\pm 1\} \to H$. Furthermore, $S_n \cap H$ is trivial and $H$ commutes with $S_n$, so $S_n \times H \leq S_{n+2}$ as an internal product. Define $f : S_n \to S_{n+2}$ by $f = \text{id}_{S_n} \times (\phi \circ \text{sgn}_n)$, where $\text{sgn}_n : S_n \to \{\pm 1\}$ is the sign homomorphism. This is evidently an injective homomorphism, so it remains to check that $\text{im } f$ lies in $A_{n+2}$. For this, note that $\text{sgn}_{n+2}((\phi \circ \text{sgn}_n)(\sigma)) = \text{sgn}_n(\sigma)$ for $\sigma \in S_n$, so we have

$$\text{sgn}_{n+2}(f(\sigma)) = \text{sgn}_{n+2}(\sigma) \text{sgn}_{n+2}((\phi \circ \text{sgn}_n)(\sigma)) = \text{sgn}_n(\sigma) \text{sgn}_n(\sigma) = 1,$$

as required for $f(\sigma)$ to be in $A_{n+2}$.

(b) Let $|G| = n$. Then we have injective homomorphisms $G \hookrightarrow S_n \hookrightarrow A_{n+2} \hookrightarrow A_{\max(5, n+2)}$, the last of which is simple.
HOMEWORK 5 - SOLUTIONS

Problem 1. Prove that two elements $\sigma$ and $\tau$ in $S_n$ are conjugate if and only if type($\sigma$) = type($\tau$).

Solution. ($\implies$) Suppose $\tau = \pi \sigma \pi^{-1}$ and write $\sigma = \rho_1 \cdots \rho_k$ in disjoint cycle notation. Then

$$\tau = \pi \sigma \pi^{-1} = (\pi \rho_1 \pi^{-1}) \cdots (\pi \rho_k \pi^{-1}),$$

so it suffices to show that the conjugates of the $\rho_i$ by $\pi$ are disjoint cycles of the same lengths. Observe that if $\rho = (a_1, \ldots, a_r)$ is a cycle, then

$$\pi \rho \pi^{-1} = (\pi(a_1), \ldots, \pi(a_r)).$$

Since $\pi$ is bijective, disjointness is preserved. (This part was done in class.)

($\impliedby$) Suppose type($\sigma$) = type($\tau$) and write

$$\sigma = (a_1, \ldots, a_{n_1})(a_{n_1+1}, \ldots, a_{n_1+n_2}) \cdots (a_{\sum k}, \ldots, a_{\sum k+n_k}),$$

$$\tau = (b_1, \ldots, b_{n_1})(b_{n_1+1}, \ldots, b_{n_1+n_2}) \cdots (b_{\sum k}, \ldots, b_{\sum k+n_k}),$$

$$n_1 + \cdots + n_k = n.$$

(There may be 1-cycles.) Defining $\pi : a_{i,j} \mapsto b_{i,j}$, we have $\tau = \pi \sigma \pi^{-1}$. \hfill $\square$

Problem 2. Prove that $S_4$ acts by conjugation on the set of all non-trivial elements of the normal subgroup $N = \{\text{id}, (12)(34), (13)(24), (14)(23)\}$. Using this action, prove that $S_4/N$ is isomorphic to $S_3$.

Solution. The non-trivial elements of $N$ are the elements of cycle type $(2,2)$; that $S_4$ acts on them transitively by conjugation then follows from Problem 1. Let $f : S_4 \to S_3$ be the induced homomorphism. Since the action is transitive, $|\text{im } f|$ is divisible by 3. The element $(12) \in S_4$ fixes $(12)(34)$ but swaps $(13)(24)$ and $(14)(23)$, so $\text{im } f$ contains an element of order 2. Thus we must have $\text{im } f = S_3$, so $S_4/\ker f \simeq S_3$. This tells us that $|\ker f| = 4$, and since $N$ is abelian, $N \leq \ker f$, so in fact $\ker f = N$. Hence $S_4/N \simeq S_3$. \hfill $\square$

Problem 3. Let $\sigma = (12 \cdots n) \in S_n$. Show that the conjugacy class of $\sigma$ has $(n - 1)!$ elements. Show that the centralizer of $\sigma$ is the cyclic subgroup generated by $\sigma$.

Solution. By Problem 1, the conjugacy class of $\sigma$ is the set of $n$-cycles in $S_n$. There are $n!$ ways to arrange the $n$ indices to obtain an $n$-cycle, but for each $n$-cycle, there are $n$ ways to represent it in cycle notation, since cycling the indices in a cycle doesn’t change the cycle itself. Thus we have $n!/n = (n - 1)!$ distinct $n$-cycles.

The centralizer of $\sigma$ contains $\langle \sigma \rangle$, which has $n$ elements since $\sigma$ has order $n$. By orbit-stabilizer, the centralizer of $\sigma$ has $n!/(n - 1)! = n$ elements, so it must be just $\langle \sigma \rangle$. \hfill $\square$

Problem 4. Prove the following useful counting result: Let $H$ be a subgroup of a finite group $G$ with $H \neq G$. Suppose that $|G|$ does not divide $[G : H]!$. Then $G$ contains a proper normal subgroup $N$ such that $N$ is a subgroup of $H$. In particular, $G$ is not simple.
Solution. Let $G$ act on $G/H$ by left multiplication and let $[G : H] = n$. Let $f : G \to S_n$ be the induced homomorphism and $N = \ker f$, so $G/N \simeq \im f \leq S_n$. Then $|G/N|$ divides $n!$, but $|G|$ does not, so $|N| > 1$, i.e. $N$ is a non-trivial normal subgroup. Furthermore, $N \leq H$ since the only elements of $G$ which fix $H$ are elements of $H$, so $N$ has all of the required properties. \hfill \Box

**Problem 5.** Prove that all groups of order $2p^n$ and $4p^n$ are not simple (where $p$ is a prime number).

*Solution.* First we consider $p = 2$, in which case we must show that if $|G| = 2^n$ for some $n \geq 2$, then $G$ is not simple. Here we use the lemma (proved in class) that if $H \leq G$ is a $p$-subgroup but not a Sylow $p$-subgroup, then there is a subgroup $K \leq G$ with $H \leq K$ and $[K : H] = p$. In this case $G$ is itself the Sylow $2$-subgroup of $G$, so by iterating the lemma, there exists a subgroup $H \leq G$ of index 2. Since $n \geq 2$, $H$ is not simple.

Now suppose $p \geq 3$ is odd. If $|G| = 2^p$, then Sylow’s third theorem shows that there is a unique Sylow $p$-subgroup, which is then normal, so $G$ is not simple. If $|G| = 4p^n$, then the same argument works for $p \geq 5$, so the only remaining case is that $|G| = 4\cdot3^n$ and $G$ has four Sylow $3$-subgroups. Let $G$ act on the set of Sylow $3$-subgroups by conjugation and let $f : G \to S_4$ be the induced homomorphism. Since the action is transitive, $\ker f \neq G$. If $\ker f = 1$, then $G \simeq \im f \leq S_4$, which is only possible if $n = 1$ and $G \simeq A_4$, which is not simple. In all other cases, $\ker f$ is a non-trivial proper normal subgroup of $G$, so $G$ is not simple.

Having exhausted all cases, the proof is complete. \hfill \Box

**Problem 6.** (a) Let $H \leq G$ be a subgroup. Prove that if $H$ is contained in the center of $G$ and the factor group $G/H$ is cyclic, then $G$ is abelian.

(b) Prove that any group of order $p^2$ is abelian (where $p$ is a prime integer).

*Solution.* This was Homework 2 Problem 5. \hfill \Box

**Problem 7.** Let $G$ be a non-abelian group of order $p^3$ (where $p$ is a prime integer). Prove that the center $Z(G)$ of $G$ coincides with the commutator subgroup $[G, G]$.

*Solution.* Since $G$ is a $p$-group, $Z = Z(G)$ is non-trivial, and since $G$ is non-abelian, either $|Z| = p$ or $|Z| = p^2$. In the latter case, $|G/Z| = p$, so $G/Z$ must be cyclic, which implies $G$ is abelian by Problem 5a, contradiction. Hence $|Z| = p$, and $G/Z$ is a group of order $p^2$, hence abelian by Problem 5b. If $G' = [G, G]$ is the commutator subgroup, then equivalently $G'$ is the smallest normal subgroup of $G$ for which $G/G'$ is abelian. We have found that $G/Z$ is abelian, so $G' \leq Z$. Since $Z$ has order $p$, this means $G' = 1$ or $G' = Z$. As $G$ is non-abelian, $G' \neq 1$, so $G' = Z$, as required. \hfill \Box

**Problem 8.** Let $G$ be a semidirect product of a cyclic normal subgroup $N$ of order $n$ and an abelian group $K$. Show that if $|K|$ is relatively prime to $\varphi(n)$ (where $\varphi$ is the Euler function), then $G$ is abelian.

*Solution.* Let $G = N \rtimes_f K$ with respect to the homomorphism $f : K \to \text{Aut } N$. Since $N$ is cyclic of order $n$, the group $\text{Aut } N$ is of order $\varphi(n)$, which is relatively prime to $|K|$, so the only possible $f$ is the trivial homomorphism. In this case, $G$ is the direct product $N \times K$, which is abelian since both $N$ and $K$ are. \hfill \Box

**Problem 9.** Determine the center of the dihedral group $D_n$. 
Solution. First, note that $D_1 \cong \mathbb{Z}/2\mathbb{Z}$ and $D_2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ are abelian, so the centers are the full groups. From now on, suppose $n \geq 3$.

Write $D_n = \langle r, s \mid r^n, s^2, rsr \rangle$. For any reflection $r^k s$, we have
\[
r(r^k s)r^{-1} = r^k(srs^{-1}) = r^{k+2}s \neq r^k s,
\]
where we have used $n \geq 3$ to deduce that $r^k \neq r^{k+2}$. Thus $r^k s \notin Z(D_n)$ for any $k$. For any rotation $r^k$ with $0 \leq k < n$, we have $r(r^k)r^{-1} = r^k$ and
\[
s(r^k)s^{-1} = (srs)^k = r^{-k}.
\]
If $n$ is odd, then $r^k \neq r^{-k}$ for any $k \neq 0$, so $Z(D_n) = 1$ for $n$ odd. If $n$ is even, then we also have equality for the rotation $r^{n/2}$ by $\pi$. Commuting with the generators is enough to commute with the whole group, so $Z(D_n) = \{1, r^{n/2}\}$ when $n$ is even. \(\square\)

**Problem 10.** Show that the exact sequence
\[
0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0
\]
is not split.

Solution. Let $f : \mathbb{Z} \rightarrow \mathbb{Q}$ be the injective map in this diagram, and suppose $f(1) = q$. To show that the exact sequence is not split, it is enough to show that there is no $g : \mathbb{Q} \rightarrow \mathbb{Z}$ such that $g \circ f = \text{id}_\mathbb{Z}$. Indeed, such a $g$ must satisfy $2g(q/2) = g(q) = 1$ with $g(q/2) \in \mathbb{Z}$, a contradiction. \(\square\)
MATH 210A (17F)  Algebra  Alan Zhou

HOMEWORK 6 - SOLUTIONS

Problem 1. For every two non-zero integers $n$ and $m$, construct an exact sequence

$$0 \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/nm\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \longrightarrow 0.$$ 

For which $n$ and $m$ is the sequence split?

Solution. The two non-trivial maps are

$$f : [a]_n \longmapsto [am]_{nm}, \quad g : [b]_{nm} \longmapsto [b]_m.$$ 

It is clear that $f$ is injective and $g$ is surjective. For $[a]_n \in \mathbb{Z}/n\mathbb{Z}$, we have

$$[a]_n \xrightarrow{f} [am]_{nm} \xrightarrow{g} [am]_m = [0]_m,$$

so $\text{im } f \leq \ker g$, and conversely if $[b]_{nm} \in \ker g$, then $b = am$ for some integer $a$, so $[b]_{nm} = f([a]_n)$, giving the other inclusion. Thus the sequence is exact.

For the sequence to split, it is necessary that $\mathbb{Z}/nm\mathbb{Z} \cong (\mathbb{Z}/n\mathbb{Z}) \oplus (\mathbb{Z}/m\mathbb{Z})$, which can only happen when $n$ and $m$ are coprime. Conversely, when $n$ and $m$ are coprime, there exist integers $r$ and $s$ such that $rn + sm = 1$, and then we can define a left inverse $p$ for $f$ and a right inverse $q$ for $g$ by

$$p : [a]_{nm} \longmapsto [as]_n, \quad q : [b]_m \longmapsto [brn]_{nm},$$

so the sequence indeed splits.

Problem 2. Let $N$ be the normal subgroup in $G*H$ generated by $G \subset G*H$. Prove that $(G*H)/N \cong H$.

Solution. Let $f_G : G \rightarrow H$ be trivial and $f_H : H \rightarrow H$ be the identity. By the universal property of free products, there is a unique $f_G * f_H : G*H \rightarrow H$ such that the diagram below commutes.

$$\begin{array}{ccc}
G & \xrightarrow{i_G} & G*H & \xrightarrow{i_H} & H \\
\downarrow{f_G} & & & & \downarrow{f_G*f_H} \\
H & & & & \downarrow{f_H}
\end{array}$$

Then $G \leq \ker(f_G * f_H)$, so $N \leq \ker(f_G * f_H)$. For the reverse inclusion, consider expressions $k = g_0h_1g_1 \cdots h_ng_n \in \ker(f_G * f_H)$ and induct on $n$. (Here $h_i \in H$ and $g_i \in G$ for each $i$, and $h_1, g_1, \ldots, h_n \neq 1$, but it is possible that $g_0 = 1$ or $g_n = 1$.) For $n = 0$, we just have $k = g_0 \in N$. In general, note that $(f_G * f_H)(k) = h_1 \cdots h_n = 1$ since $f_G * f_H$ extends $f_G$ and $f_H$. 

27
so \( h_n = h_{n-1}^{-1} \cdots h_1^{-1} = hh_1^{-1} \), with \( h = h_{n-1}^{-1} \cdots h_2^{-1} \). Since \( g_0 \) and \( g_n \) are in \( \ker(f_G \ast f_H) \), being elements of \( G \), this means that

\[
h_1g_1 \cdots h_ng_n = h_1(g_1h_2 \cdots g_nh_1^{-1}) \in \ker(f_G \ast f_H) \implies g_1h_2 \cdots g_nh \in \ker(f_G \ast f_H).
\]

By the inductive hypothesis, \( g_1h_2 \cdots g_nh \in N \) (this is fine even if \( h = 1 \)). Since \( N \) is closed under conjugates and contains \( G \), this means that \( k \in N \). Hence \( N = \ker(f_G \ast f_H) \), and the result follows by the first isomorphism theorem. \( \square \)

**Problem 3.** Let \( D_\infty = \mathbb{Z} \rtimes (\mathbb{Z}/2\mathbb{Z}) \) with respect to the (unique) isomorphism \( \mathbb{Z}/2\mathbb{Z} \to \text{Aut} \mathbb{Z} \). Prove that \( D_\infty \cong (\mathbb{Z}/2\mathbb{Z}) \rtimes (\mathbb{Z}/2\mathbb{Z}) \).

**Solution.** Write the free product as \( \langle a,b \mid a^2,b^2 \rangle \), and let \( D_\infty = \langle r \rangle \rtimes \langle s \mid s^2 \rangle \). Then

\[
(rs)^2 = rsrc = rr^{-1}ss = 1,
\]

so we have a pair of homomorphisms

\[
f : \langle a \mid a^2 \rangle \longrightarrow D_\infty \quad g : \langle b \mid b^2 \rangle \longrightarrow D_\infty
\]

\[
a \mapsto s \quad b \mapsto rs.
\]

By the universal property of free products, there is a unique homomorphism \( f \ast g \) extending them to \( \langle a,b \mid a^2,b^2 \rangle \). We claim that in fact \( f \ast g \) is an isomorphism. For surjectivity, we have that \( (f \ast g)(ba) = rss = r \) and \( (f \ast g)(a) = s \), so both generators of \( D_\infty \) are in the image of \( f \ast g \). For injectivity, every reduced expression in \( \langle a,b \mid a^2,b^2 \rangle \) has the form \( c(ba)^n \) with \( n \geq 0 \), \( c \in \{1,a\} \), and \( d \in \{1,b\} \). Then by brute forcing, \( (f \ast g)(c(ba)^n) = (f \ast g)(c)r^na(f \ast g)(d) \) is never 1 unless \( n = 0 \) and \( c = d = 1 \), which means the kernel is trivial. \( \square \)

**Problem 4.** Show that there exists a surjective homomorphism \( (\mathbb{Z}/n\mathbb{Z}) \rtimes (\mathbb{Z}/2\mathbb{Z}) \to S_n \).

**Solution.** Define a set map \( f : \{a,b\} \to S_n \) by \( f(a) = (1,2,\ldots,n) \) and \( f(b) = (1,2) \). By the universal property of free groups, this extends uniquely to a homomorphism \( \varphi : F(a,b) \to S_n \). It is surjective, as \( (1,2,\ldots,n) \) and \( (1,2) \) generate \( S_n \). Then \( a^n \) and \( b^2 \) are in \( \ker \varphi \), so \( \varphi \) descends to a surjective homomorphism \( F(a,b)/\langle \langle a^n,b^2 \rangle \rangle \to S_n \). This completes the proof, as

\[
F(a,b)/\langle \langle a^n,b^2 \rangle \rangle = \langle a,b \mid a^n, b^2 \rangle \cong \langle a \mid a^n \rangle * \langle b \mid b^2 \rangle \cong (\mathbb{Z}/n\mathbb{Z}) * (\mathbb{Z}/2\mathbb{Z}).
\]

\( \square \)

**Problem 5.** Prove that the group \( SL_2(\mathbb{Z}) \) is generated by the two matrices

\[
\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}.
\]

**Solution.** First note that we can get the matrix

\[
\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1} \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},
\]

so the group \( SL_2(\mathbb{Z}) \) is generated by these elementary matrices.
so it suffices to use the first of the two given matrices and this one to generate all of $SL_2(\mathbb{Z})$.

For any matrix in $SL_2(\mathbb{Z})$, we can compute

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a + c & b + d \\ c & d \end{pmatrix}.$$

Focusing on the first column, these two matrix products allow us to run the Euclidean algorithm on $a$ and $c$. Since the matrix has determinant 1, $a$ and $c$ must be coprime, so in particular we can obtain, after finitely many steps, a matrix of the form $\begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix}$. Having determinant 1 forces $d = 1$.

Then the matrix we are left with is precisely $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$, so we are done. \hfill $\Box$

**Problem 6.** Let $H$ and $K$ be two subgroups in $G$. Assume that $G$ acts on a set $X$ and that there are two subsets $A, B \subseteq X$ and an element $x \in X \setminus (A \cup B)$ such that $h(A \cup \{x\}) \subseteq B$ for every $h \in H$, $h \neq 1$, and $k(B \cup \{x\}) \subseteq A$ for every $k \in K$, $k \neq 1$. Prove that the natural homomorphism $H \ast K \to G$ is injective.

**Solution.** Suppose not, so there is some $h_0k_1h_2 \cdots h_nk_n \in H \ast K$ with $n \geq 1$ and $h_i, k_i \neq 1$ for all $i$, except for possibly $h_0$ and $k_n$, such that $h_0k_1h_2 \cdots h_nk_n = 1$ in $G$. If $h_0, k_n \neq 1$, then we have that $k_nx \in A$, so $h_nk_nx \in B$, and so on, until we get to $h_0k_1 \cdots k_nx = x \in B$, a contradiction to how $x$ was chosen. A similar contradiction arises in the other possible cases. \hfill $\Box$

**Problem 7.** Let $G$ and $H$ be two non-trivial groups. Show that $G \ast H$ is an infinite group with trivial center.

**Solution.** If $g \in G$ and $h \in H$ are non-identity elements, then the words $(gh)^n$ are all reduced in $G \ast H$, so $G \ast H$ must be infinite.

Consider an arbitrary non-identity word, without loss of generality of the form $g_1h_1 \cdots g_nh_n$, with $g_i, h_i \neq 1$ except possibly for $h_n$. Pick some $h \neq 1$ in $H$. Then $hg_1h_2 \cdots g_nh_n$ and $g_1h_1 \cdots g_nh'$ are distinct reduced words, where $h' = h_nh$, so $h$ and $g_1h_1 \cdots g_nh_n$ do not commute. Hence the center of $G \ast H$ must be trivial. \hfill $\Box$

**Problem 8.** Let $X$ be a subset in a group $G$. Prove that $\langle \langle X \rangle \rangle = \langle Y \rangle$, where $Y = \bigcup_{g \in G} gXg^{-1}$.

**Solution.** Since normal subgroups are closed under conjugates, we must have $Y \subseteq \langle \langle X \rangle \rangle$, and hence $\langle Y \rangle \subseteq \langle \langle X \rangle \rangle$. In the other direction, $Y$ is clearly self-conjugate, so $\langle Y \rangle$ is normal and contains $X$ (Homework 3 Problem 9). Since $\langle \langle X \rangle \rangle$ is the smallest such subgroup of $G$, $\langle \langle X \rangle \rangle \subseteq \langle Y \rangle$. \hfill $\Box$

**Problem 9.** Let $G$ be the group defined by the generators $a$ and $b$ and relations $w^3 = 1$ for all words $w$ in $a$ and $b$. Show that $G$ is finite, and find $|G|$. 

**Solution.** Introduce an additional generator $c = aba^{-1}b^{-1}$. Then we have

\[ aca^{-1}c^{-1} = a^2ba^2b^2a^2bab^2a^2 = (a^2b)^2ba(ab)^2ba^2 = b(ba)^2b(ba)^2 = ba^2b^2bab^2 = 1, \]

29
so $ac = ca$, and similarly $bc = cb$. Also, we have $cba = ab$, so $ba = c^{-1}ab = abc^2$. Therefore, any word in $G$ can be written in the form $a^ib^jc^k$ with $i, j, k \in \{0, 1, 2\}$, which means that $G$ is finite with $|G| \leq 27$. To get equality, note that the Heisenberg group $H$ on $\mathbb{F}_3$ is generated by two elements and every non-identity element has order 3. This means that $H$ is some quotient of $G$, hence $|G| \geq |H| = 27$. (From this we deduce that $G$ is isomorphic to the Heisenberg group.)

**Problem 10.** Prove that if the free groups $F(X)$ and $F(Y)$ for the finite sets $X$ and $Y$ are isomorphic, then $|X| = |Y|$.

**Solution.** There are $2^{|X|}$ homomorphisms from $F(X)$ to $\mathbb{Z}/2\mathbb{Z}$, as there are this many set functions from $X$ to $\mathbb{Z}/2\mathbb{Z}$. If $F(X)$ and $F(Y)$ are isomorphic, then $2^{|X|} = 2^{|Y|}$, so $|X| = |Y|$.
HOMEWORK 7 - SOLUTIONS

Problem 1. Show that $Q_8 = \langle x, y, c \mid c^2, x^2c, y^2c, xyzc \rangle$.

Solution. Let $G$ be the group with this presentation. First note that $Q_8$ is generated by $x = i$, $y = j$, and $c = -1$, and they satisfy these relations (and possibly more), so $Q_8$ is a quotient of $G$. In $G$, we have $x^2 = y^2 = c$, so $c \in Z(G)$ as it commutes with the generators. Then

$$G/\langle c \rangle = \langle x, y, c \mid c^2, x^2c, y^2c, xyzc \rangle = \langle x, y \mid x^2, y^2, xyz \rangle.$$ 

This is a presentation of $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, so $|G| = 8$. Hence $G \cong Q_8$.

Problem 2. Prove that if $X_1$ and $X_2$ are disjoint sets, then

$$\langle X_1 \mid R_1 \rangle \ast \langle X_2 \mid R_2 \rangle \cong \langle X_1 \cup X_2 \mid R_1 \cup R_2 \rangle.$$ 

Solution. Let $G = \langle X_1 \mid R_1 \rangle$, $H = \langle X_2 \mid R_2 \rangle$, and $K = \langle X_1 \cup X_2 \mid R_1 \cup R_2 \rangle$. The natural maps

$$i : G \rightarrow K \quad j : H \rightarrow K$$

$$[x]_{R_1} \rightarrow [x]_{R_1 \cup R_2} \quad [y]_{R_2} \rightarrow [y]_{R_1 \cup R_2}$$

are well-defined, as if $x$ and $x'$ are equivalent with reductions in $R_1$ allowed, then they are also equivalent with reductions in $R_1 \cup R_2$ allowed, by only using reductions in $R_1$. (The same argument applies for $y$ and $y'$ equivalent with reductions in $R_2$ allowed.) We claim that $K$, with the maps $i$ and $j$, satisfies the universal property of free products.

Let $L$ be some group and $g, h : G, H \rightarrow L$ be homomorphisms. Let $\pi_1, \pi_2 : F(X_1), F(X_2) \rightarrow G, H$ be the canonical projections and $i, j : F(X_1), F(X_2) \rightarrow F(X_1 \cup X_2)$ be the natural inclusions. Then define $\tilde{g} = g \circ \pi_1$ and $\tilde{h} = h \circ \pi_2$. We may define a set function $\tilde{f} : X_1 \cup X_2 \rightarrow L$ by

$$\tilde{f}(x) = \begin{cases} \tilde{g}(x) & x \in X_1, \\ \tilde{h}(x) & x \in X_2. \end{cases}$$

By repeatedly using the universal property of free groups, this is well-defined and extends uniquely to a homomorphism $\tilde{f} : F(X_1 \cup X_2) \rightarrow L$. Furthermore, by construction, we have that $\tilde{g} = \tilde{f} \circ i$ and $\tilde{h} = \tilde{f} \circ j$. If $x \in R_1 \subset F(X_1)$, then we have

$$\tilde{f}(x) = \tilde{f}(i(x)) = \tilde{g}(x) = g(\pi_1(x)) = g(1) = 1,$$

so $x \in \ker \tilde{f}$. Similarly, if $y \in R_2$, then $y \in \ker \tilde{f}$. Thus $R_1 \cup R_2 \subset \ker \tilde{f}$, so $\tilde{f}$ descends to a homomorphism $f : K \rightarrow L$ through the projection $\pi : F(X_1 \cup X_2) \rightarrow K$. We must show that $g = f \circ i$ and $h = f \circ j$; given this, such an $f$ must be unique, since it is fixed on the generators of $K$ by the values of $i$ and $g$ on the generators of $G$ and $H$. Observe that for $x \in F(X_1)$, we have

$$(\pi \circ \tilde{i})(x) = [x]_{R_1 \cup R_2}, \quad (i \circ \pi_1)(x) = i([x]_{R_1}) = [x]_{R_1 \cup R_2},$$

so $\pi \circ \tilde{i} = i \circ \pi_1$. This gives

$$g \circ \pi_1 = \tilde{g} = \tilde{f} \circ \tilde{i} = f \circ \pi \circ \tilde{i} = f \circ i \circ \pi_1.$$
Problem 3. Prove that if $X$ is a set of $n$ elements, then $F(X) \cong \mathbb{Z} \ast \cdots \ast \mathbb{Z}$ ($n$ times).

Solution. This follows from Problem 2 by induction and the fact that $F(\{x\}) \cong \mathbb{Z}$. 

Problem 4. Prove that the natural homomorphisms $G \rightarrow G \ast H$ and $H \rightarrow G \ast H$ are injective.

Solution. Let $i : G \rightarrow G \ast H$ be the natural homomorphism, $g : G \rightarrow G$ be the identity, and $h : H \rightarrow G$ be the trivial homomorphism. By the universal property of free products, there exists $f : G \ast H \rightarrow G$ such that $f \circ i = g$. Since $g$ is the identity, $f$ is a left inverse for $i$, i.e. $i$ is injective. (More directly, if $i(x) = i(y)$, then $x = g(x) = f(i(x)) = f(i(y)) = g(y) = y$.)

Problem 5. Let $f$ be a homomorphism from the free group on $x$ and $y$ to the cyclic group $\{\pm 1\}$ taking $x$ and $y$ to $-1$. Prove that the kernel of $f$ is a free group freely generated by $x^2$, $y^2$, and $xy$.

Solution. The kernel of $f$ consists of words of even length with letters from $\{x, x^{-1}, y, y^{-1}\}$. (Note that elementary reductions remove two letters, so parity of length is a well-defined quantity associated to elements of $F(x, y)$.) First we claim that $x^2 = xx$, $y^2 = yy$, and $xy$ generate this subgroup. It suffices to generate every word of length 2. For this, we compute

$$yx = y^2(xy)^{-1}x^2, \quad x^{-1}y = (x^2)^{-1}(xy), \quad yx^{-1} = y^2(xy)^{-1},$$

and every other word of length 2 is an inverse of one of the six words of length 2 mentioned thus far. To see that $a = x^2$, $b = y^2$, and $c = xy$ freely generate $\ker f$, consider a non-empty irreducible word $w$ in $F(a, b, c)$ which, when expanded fully as a word $v$ in $F(x, y)$, reduces to the empty word. Then there exist substrings of $v$ which only use one of the letters (and its inverse) that reduce to the empty word; let $u$ be a maximal such substring. Without loss of generality, suppose $u$ consists of some number of $y$’s and an equal number of $y^{-1}$’s in some order. To obtain such a substring in $v$, we must have a (non-empty) substring $t$ in $w$ of the form $rb_1 \cdots b_n s$, where each $b_i$ is either $b$ or $b^{-1}$, so that $b$ and $b^{-1}$ appear the same number of times, $r$ is either empty or $c$, and $s$ is either empty or $c^{-1}$. By parity, $n$ is even, and if $r$ is empty, then $s$ is empty, while if $r = c$, then $s = c^{-1}$. If $n \geq 2$, then we can cancel all of the $b_i$’s, contradicting the assumption that $w$ is irreducible. If $n = 0$, then we are left with $rs$, which is either empty if both are empty, contradicting the assumption that $t$ is non-empty, or equal to $cc^{-1}$, which reduces, contradicting irreducibility of $w$. Having exhausted all possible cases, we conclude that no non-empty irreducible words in $F(a, b, c)$ reduce to the empty word in $F(x, y)$, so $a, b, c$ freely generate $\ker f$. 

\[\square\]
Problem 6. Give an example of a category $\mathcal{C}$ and a full subcategory $\mathcal{C}'$ such that the initial objects of $\mathcal{C}$ and $\mathcal{C}'$ are different.

Solution. Let $\mathcal{C} = \text{Ring}$, which has initial object $\mathbb{Z}$, and $\mathcal{C}'$ be the full subcategory of fields of characteristic zero, which has initial object $\mathbb{Q}$.

Problem 7. (a) A morphism $f : A \to B$ in a category $\mathcal{C}$ is called a monomorphism if for any two morphisms $g, h : C \to A$, the equality $fg = fh$ implies $g = h$. Show that the composition of two monomorphisms is a monomorphism. Determine monomorphisms in $\text{Set}$ and $\text{Grp}$.

(b) Define the dual notion of epimorphism and solve the dual problems in $\text{Set}$ and $\text{Grp}$.

Solution. (a) Let $f : A \to B, g : B \to C$ be monomorphisms and let $k, l : D \to A$ be morphisms with $gf = gfl$. Since $g$ is a monomorphism, $fk = fl$. Since $f$ is a monomorphism, $k = l$.

In $\text{Set}$, the monomorphisms are injective functions. If $f : A \to B$ is injective and $g, h : C \to A$ are functions with $fg = fh$, then for any $x \in C$, we have $f(g(x)) = f(h(x))$, so $g(x) = h(x)$, hence $g = h$. Conversely, if $f : A \to B$ is a monomorphism, then let $C = A/\sim$, where $x \sim y$ if $f(x) = f(y)$. Let $g, h : C \to A$ be two functions which pick, for each equivalence class of $\sim$, an element of $A$ in that class. Then $fg = fh$ by construction, so $g = h$ as $f$ is a monomorphism. This means that each equivalence class of $\sim$ contains exactly one element, i.e. $f(x) = f(y)$ implies $x = y$, so $f$ is injective.

In $\text{Grp}$, the monomorphisms are injective homomorphisms. The same work as in $\text{Set}$ shows that if $f$ is injective, then $f$ is a monomorphism. Conversely, if $f : A \to B$ is a monomorphism, then let $C = \ker f$. If $i : C \to A$ is inclusion and $g : C \to A$ is trivial, then $fi = fg$ since both are the trivial map $C \to B$. Then $i = g$, so $\ker f = 1$, i.e. $f$ is injective.

(b) A morphism $f : B \to A$ in a category $\mathcal{C}$ is an epimorphism if for any morphisms $g, h : A \to C$, the equality $gf = hf$ implies $g = h$. A similar argument to above shows that compositions of epimorphisms are epimorphisms.

In $\text{Set}$, the epimorphisms are surjective functions. If $f : B \to A$ is surjective and $g, h : A \to C$ are functions with $gf = hf$, then for each $x \in A$, we can find $y \in B$ such that $f(y) = x$, and then $g(x) = g(f(y)) = h(f(y)) = h(x)$, hence $g = h$. Conversely, if $f : B \to A$ is an epimorphism, then let $C = \{0, 1\}$. If $g : A \to C$ is the constant function 1 and $\chi : A \to \{0, 1\}$ is the indicator function of $\text{im} f \subset A$, then $gf = hf$ since both are the constant function 1 on $B$. Thus $g = h$, so $\text{im} f = B$, i.e. $f$ is surjective.

In $\text{Grp}$, the epimorphisms are surjective homomorphisms. The same work as in $\text{Set}$ shows that if $f$ is surjective, then $f$ is an epimorphism. Conversely, if $f : B \to A$ is an epimorphism, then let $C = A_1 \ast_{\text{im} f} A_2$ with $A_1 = A_2 = A$, the fiber coproduct of $A$ and $A$ under $\text{im} f$. Write $i : \text{im} f \to A$ for the inclusion, $f'$ for the map $f$ from $B$ to $\text{im} f$, and $g : A_1 \to A_1 \ast_{\text{im} f} A_2$ and $h : A_2 \to A_1 \ast_{\text{im} f} A_2$ for the natural maps. Then $gf = gi f' = h i f' = hf$, so $g = h$. This can only happen if $\text{im} f = A$, i.e. $f$ is surjective.
Problem 8. (a) An object $P$ of $\mathcal{C}$ is called projective if for every epimorphism $f : B \to C$ and every morphism $g : P \to C$, there exists a morphism $h : P \to B$ such that $fh = g$. Show that free groups in $\text{Grp}$ are projective objects.

(b) Define the dual notion of injective objects. Show that in the category of finite-dimensional vector spaces over a given field, every object is projective and injective.

Solution. (a) Let $f : B \to C$ be an epimorphism of groups, i.e. a surjective group homomorphism, and let $g : P \to C$ be a morphism, where $P$ is a free group. Let $S \subset P$ be a subset which freely generates $P$, and define a set function $\hat{h} : S \to B$ by picking, for each $s \in S$, some $b \in B$ with $f(b) = g(s)$, and setting $\hat{h}(s) = b$. By the universal property of free groups, $\hat{h}$ extends uniquely to a homomorphism $h : P \to B$. By construction, $(fh)(s) = g(s)$ for all $s \in S$, so $fh = g$ on all of $P$. This shows that $P$ is projective.

(b) An object $Q$ of $\mathcal{C}$ is injective if for every monomorphism $f : C \to B$ and every morphism $g : C \to P$, there exists a morphism $h : B \to P$ such that $hf = g$.

Let $V$ be a finite-dimensional vector space over a field $K$. Suppose we have an epimorphism (surjective linear map) $f : U \to W$ and a linear map $g : V \to W$. Let $v_1, \ldots, v_n$ be a basis of $V$. To define $h$, we take the set function $\hat{h}$ defined on $v_i$ by taking $u_i \in U$ such that $f(u_i) = g(v_i)$, setting $\hat{h}(v_i) = u_i$, and extending it to a linear map $h : V \to U$. This satisfies $fh = g$ on the basis $\{v_i\}$ by construction, hence on all of $V$, so $V$ is projective.

Now suppose we have a monomorphism (injective linear map) $f : W \to U$ and a linear map $g : W \to V$. Then we can regard $W$ as a subspace of $U$ and consider a projection $\pi : U \to W$. If we set $h = g\pi$, then $hf = g$, as required for $V$ to be an injective object.

Problem 9. (a) Let $X$ be an object of a category $\mathcal{C}$. Consider a new category $\mathcal{C}/X$ with objects the morphisms $f : Y \to X$ for $Y$ in $\mathcal{C}$ and morphisms between $f : Y \to X$ and $g : Z \to X$ being morphisms $h : Y \to Z$ such that $gh = f$. The product of two objects $f : Y \to X$ and $g : Z \to X$ in $\mathcal{C}/X$ is called the fiber product of $Y$ and $Z$ over $X$, denoted $Y \times_X Z$. Show that fiber products exist when $\mathcal{C}/X$ is $\text{Set}/X$, $\text{Grp}/X$, or $\text{Ab}/X$ for any object $X$ in $\mathcal{C}$.

(b) Define the dual notion and solve the dual problems.

Solution. (a) The fiber product is given by the following universal property: Let $r : Y \to X$ and $s : Z \to X$ be morphisms. The fiber product is the object $Y \times_X Z$ (unique up to isomorphism), with morphisms $p : Y \times_X Z \to Y$ and $q : Y \times_X Z \to Z$ satisfying $rp = sq$, such that for any pair of morphisms $f : W \to Y$ and $g : W \to Z$ with $rf = sg$, there is a unique morphism $h : W \to Y \times_X Z$ such that the diagram below commutes.

![Diagram](https://via.placeholder.com/150)

34
In all three categories listed, this is satisfied by \( Y \times_X Z = \bigcup_{x \in X} (r^{-1}(x) \times s^{-1}(x)) \) with the natural projections to \( Y \) and \( Z \), via the universal property of (ordinary) products. Indeed, if we have morphisms \( f : W \to Y \) and \( g : W \to Z \) with \( rf = sg \), then \( h : W \to Y \times_X Z \) must be given by \( h(w) = (f(w), g(w)) \). For \( w \in W \), that \( h(w) \in Y \times_X Z \) follows from \( x = rf(w) = sg(w) \) for some \( x \), so \( f(w) \in r^{-1}(x) \) and \( g(w) \in s^{-1}(x) \). Thus we have the required existence and uniqueness in the case of \( \text{Set} \).

In the case of \( \text{Grp} \), we also need to check that \( Y \times_X Z \) is a group and that \( h \) is a group homomorphism. The latter is clear from the corresponding statement for products, while for the former, if \( (y_1, z_1) \in r^{-1}(x_1) \times s^{-1}(x_1) \) and \( (y_2, z_2) \in r^{-1}(x_2) \) are in \( Y \times_X Z \), then \( (y_1 y_2, z_1 z_2) \in r^{-1}(x_1 x_2) \times s^{-1}(x_1 x_2) \subset Y \times_X Z \), as required.

For \( \text{Ab} \), note that \( Y \times_X Z \) is abelian since it is a subgroup of the abelian group \( Y \times Z \), and \( h \) is a homomorphism of abelian groups.

(b) The fiber coproduct is the fiber product in \( \mathbf{C}^\text{op}/X \), i.e. given morphisms \( i : X \to Y \) and \( j : X \to Z \), the fiber coproduct is the object \( Y \ast_X Z \) (unique up to isomorphism), with morphisms \( k : Y \to Y \ast_X Z \) and \( l : Z \to Y \ast_X Z \) satisfying \( ki = lj \), such that for any pair of morphisms \( f : Y \to W \) and \( g : Z \to W \), there is a unique morphism \( h : Y \ast_X Z \to W \) such that the diagram below commutes.

\[
\begin{array}{ccc}
X & \xrightarrow{i} & Y \\
| & & | \\
\downarrow{j} & & \uparrow{k} \\
Z & \xrightarrow{l} & Y \ast_X Z \\
& & \downarrow{h} \\
& & W
\end{array}
\]

In each category listed, this is satisfied by \( Y \ast_X Z = (Y \ast Z)/\sim \), where \( \sim \) is the minimal equivalence relation for which \( \tilde{k}i(x) \sim \tilde{l}j(x) \) for all \( x \in X \) and \( \tilde{k}, \tilde{l} \) are the natural morphisms \( Y, Z \to Y \ast Z \). The morphisms \( k \) and \( l \) are \( \pi \tilde{k} \) and \( \pi \tilde{l} \), where \( \pi : Y \ast Z \to Y \ast_X Z \) is the canonical projection.

In \( \text{Set} \), the coproduct \( Y \ast Z \) is the disjoint union \( Y \sqcup Z \), so \( Y \ast_X Z = (Y \sqcup Z)/\sim \).

In \( \text{Grp} \), the coproduct \( Y \ast Z \) is the free product and \( \tilde{k}, \tilde{l} \) are inclusions, so \( Y \ast_X Z = (Y \ast Z)/\sim \).

In \( \text{Ab} \), the coproduct \( Y \ast Z \) is the direct sum and \( \tilde{k}, \tilde{l} \) are inclusions, so \( Y \ast_X Z = (Y \oplus Z)/\sim \).

In each case, the morphisms \( \tilde{k}, \tilde{l} \) are inclusions, so \( \sim \) is the equivalence relation generated by \( i(x) = j(x) \) for all \( x \in X \).

\[\square\]
Problem 10. (a) The kernel of a pair of morphisms \( f, g : X \to Y \) in \( \mathcal{C} \) is a morphism \( h : Z \to X \) such that \( fh = gh \) and for any morphism \( i : T \to X \) in \( \mathcal{C} \) such that \( fi = gi \), there exists a unique morphism \( j : T \to Z \) such that \( hj = i \). Show that kernels exist in \( \text{Set} \) and \( \text{Ab} \).

(b) Define the dual notion of a cokernel. Show that cokernels exist in \( \text{Set} \) and \( \text{Ab} \).

Solution. (a) In \( \text{Set} \), the kernel is \( Z = \{ x \in X \mid f(x) = g(x) \} \) with the inclusion \( h : Z \to X \). It is clear that \( fh = gh \), and given a morphism \( i : T \to X \) with \( fi = gi \), we must define \( j : T \to Z \), if it exists and satisfies \( hj = i \), by \( j(t) = i(t) \). Such a \( j \) exists as long as \( \text{im } i \subset Z \), which follows from the fact that \( f(i(t)) = g(i(t)) \).

The same construction works in \( \text{Ab} \), but we must also check that \( Z \) is a group and that \( j \) is a homomorphism. The former is true because \( Z = \ker(f - g) \), and the latter is trivial.

(b) The cokernel of a pair of morphisms \( f, g : Y \to X \) in \( \mathcal{C} \) is a morphism \( h : X \to Z \) such that \( hf = hg \) and for any morphism \( i : X \to T \) in \( \mathcal{C} \) such that \( if = ig \), there exists a unique morphism \( j : Z \to T \) such that \( jh = i \).

In both categories listed, we take \( Z = X/\sim \), where \( \sim \) is the minimal equivalence relation with \( f(y) \sim g(y) \) for all \( y \in Y \), with the projection \( h : X \to Z \). It is clear that \( fh = gh \), and given a morphism \( i : X \to T \) with \( if = ig \), then \( j : Z \to T \) must be given by \( j([x]) = i(x) \) for \( x \in X \). To see that such a \( j \) exists, it is enough to note that if \( f(y) = x_1 \sim x_2 = g(y) \), then \( i(x_1) = i(f(y)) = i(g(y)) = i(x_2) \), so using \( j([x]) = i(x) \) gives a well-defined morphism.

In \( \text{Ab} \), we must also show that \( Z \) is an abelian group (then the fact that \( j \) is a homomorphism follows trivially). For this, note that \( \sim \) gives the subgroup \( \text{im}(f - g) \). In abelian groups, all subgroups are normal, so \( Z = X/\text{im}(f - g) \) is an abelian group. 

\[ \square \]
Problem 1. Let $X$ be a final object of a category $C$. Prove that $X \times Y \cong Y$ for every $Y \in \text{Ob}\ C$.

Solution. Let $\pi_X : X \times Y \to X$ and $\pi_Y : X \times Y \to Y$ be the projections. Since $X$ is terminal (final), $\pi_X$ is the unique morphism $X \times Y \to X$ and there is a unique morphism $f : Y \to X$. By the universal property of products, there are unique morphisms $g : Y \to X \times Y$ and $h : X \times Y \to X \times Y$ such that the diagrams below commute.

In particular, $h = \text{id}_{X \times Y}$. From the first diagram, $\pi_Y \circ g = \text{id}_Y$ so $\pi_Y \circ g \circ \pi_Y = \pi_Y$. Since $\pi_X \circ g \circ \pi_Y : X \times Y \to X$ is a morphism and $X$ is terminal, $\pi_X \circ g \circ \pi_Y = \pi_X$. Thus $h = g \circ \pi_Y$ also makes the second diagram commute, so we must have $g \circ \pi_Y = \text{id}_{X \times Y}$. Thus $\pi_Y : X \times Y \to Y$ is an isomorphism with inverse $g$.

Problem 2. Let $F : C^\text{op} \to \text{Grp}$ be a functor such that the composition of $F$ with the forgetful functor $\text{Grp} \to \text{Set}$ is corepresented by an object $X$. Prove that $X$ has the structure of a group object in $C$.

Solution. For this problem, assume $X$ has a terminal object and finite products.

That $F$ is corepresented by $X$ means that for each $Y \in C$, there is a bijection $\alpha_Y$ from $\text{Hom}_C(Y, X)$ to the set $F(Y)$. Furthermore, given a morphism $f : Y \to Z$, the diagram below commutes.

The group operation on $F(Y)$ induces a group operation $\star_Y$ on $\text{Hom}_C(Y, X)$, defined by

$$g \star_Y h = \alpha_Y^{-1}(\alpha_Y(g)\alpha_Y(h)).$$

For $Y = X \times X$, there are two projections $\pi_1, \pi_2 : X \times X \to X$. Define $m = \pi_1 \star \pi_2 : X \times X \to X$, with $\star = \star_{X \times X}$. We claim that $m$ is a valid multiplication morphism for giving $X$ the structure of a group object, i.e. the diagram below commutes.

$$X \times X \times X \xrightarrow{m \times \text{id}_X} X \times X \xrightarrow{\text{id}_X \times m} X \xrightarrow{m} X$$
Both $m \circ (m \times \text{id}_X)$ and $m \circ (\text{id}_X \times m)$ are morphisms $X \times X \times X \to X$, so to show that they are equal, it is enough to show that

$$
\alpha_{X \times X \times X}(m \circ (m \times \text{id}_X)) = \alpha_{X \times X \times X}(m \circ (\text{id}_X \times m)).
$$

Using $Y = X \times X \times X$, $Z = X \times X$, and $f = m \times \text{id}_X$ in (1), we have the diagram below.

\[
\begin{array}{ccc}
\text{Hom}_C(X \times X, X) & \xrightarrow{g \mapsto g(m \times \text{id}_X)} & \text{Hom}_C(X \times X \times X, X) \\
\downarrow \alpha_{X \times X} & & \downarrow \alpha_{X \times X \times X} \\
F(X \times X) & \xrightarrow{F(m \times \text{id}_X)} & F(X \times X \times X)
\end{array}
\]

Following arrows for $m \in \text{Hom}_C(X \times X, X)$, and noting that $F(m \times \text{id}_X)$ is a homomorphism,

$$
\alpha_{X \times X \times X}(m \circ (m \times \text{id}_X)) = F(m \times \text{id}_X)(\alpha_{X \times X}(m)) = F(m \times \text{id}_X)(\alpha_{X \times X}(\pi_1)\alpha_{X \times X}(\pi_2)) = F(m \times \text{id}_X)(\alpha_{X \times X}(\pi_1))F(m \times \text{id}_X)(\alpha_{X \times X}(\pi_2)).
$$

To simplify this further, let $p_1, p_2, p_3 : X \times X \times X \to X$ be the three projections onto the individual factors, and let $q_{12} : X \times X \times X \to X \times X$ be the unique projection onto the first two factors, so that $\pi_1 \circ q_{12} = p_1$ and $\pi_2 \circ q_{12} = p_2$. The product morphism $m \times \text{id}_X$ is defined by the commutative diagram below.

\[
\begin{array}{ccc}
X \times X \times X & \xrightarrow{q_{12}} & X \\
\downarrow m \times \text{id}_X & & \downarrow \pi_2 \\
X \times X & \xleftarrow{\pi_1} & X \times X
\end{array}
\]

Since $F$ is a contravariant functor,

$$
F(q_{12}) \circ F(m) = F(m \times \text{id}_X) \circ F(\pi_1), \quad F(p_3) = F(m \times \text{id}_X) \circ F(\pi_2).
$$

Evaluating the first equation at $\alpha_X(\text{id}_X) \in F(X)$ and using naturality of $\alpha$ (i.e. following arrows in (1) for various choices of $Y, Z, f$), we have

$$
F(m \times \text{id}_X)(F(\pi_1)(\alpha_X(\text{id}_X))) = F(q_{12})(F(m)(\alpha_X(\text{id}_X))) \\
F(m \times \text{id}_X)(\alpha_{X \times X}(\pi_1)) = F(q_{12})(\alpha_{X \times X}(m)) \\
= F(q_{12})(\alpha_{X \times X}(\pi_1))F(q_{12})(\alpha_{X \times X}(\pi_2)) \\
= \alpha_{X \times X \times X}(\pi_1 \circ q_{12})\alpha_{X \times X \times X}(\pi_2 \circ q_{12}) \\
= \alpha_{X \times X \times X}(p_1)\alpha_{X \times X \times X}(p_2).
$$

Evaluating the second equation at $\alpha_X(\text{id}_X)$ gives, by a similar calculation,

$$
F(m \times \text{id}_X)(\alpha_{X \times X}(\pi_2)) = \alpha_{X \times X \times X}(p_3),
$$

so

$$
\alpha_{X \times X \times X}(m \circ (m \times \text{id}_X)) = \alpha_{X \times X \times X}(p_1)\alpha_{X \times X \times X}(p_2)\alpha_{X \times X \times X}(p_3).
$$
We can show by the same argument that

\[ \alpha_{X \times X \times X}(m \circ (\text{id}_X \times m)) = \alpha_{X \times X \times X}(p_1)\alpha_{X \times X \times X}(p_2)\alpha_{X \times X \times X}(p_3), \]

and since \( \alpha_{X \times X \times X} \) is a bijection, \( m \circ (m \times \text{id}_X) = m \circ (\text{id}_X \times m) \), as required.

Let \( T \) be a terminal object in \( C \). As \( F(T) \) is a group, it has an identity element 1; let \( e = \alpha^{-1}_T(1) \).

We claim that \( e \) is a valid identity morphism for giving \( X \) the structure of a group object, i.e. the diagrams below commute (\( r_1, s_2 \) are projections onto \( X \)).

\[
\begin{align*}
X \times T & \xrightarrow{\text{id}_X \times e} X \times X \xrightarrow{m} X \\
T & \xrightarrow{\pi_1} X
\end{align*}
\]

The product morphism \( \text{id}_X \times e : X \times T \to X \times X \) is defined by the following commuting diagram.

\[
\begin{align*}
X \times T & \xrightarrow{r_2} T \xrightarrow{e} X \\
X \xleftarrow{\pi_1} X \times X
\end{align*}
\]

From this and naturality of \( \alpha \), we compute

\[
\alpha_{X \times T}(m \circ (\text{id}_X \times e)) = F(\text{id}_X \times e)(\alpha_{X \times X}(m)) \\
= F(\text{id}_X \times e)(\alpha_{X \times X}(\pi_1))F(\text{id}_X \times e)(\alpha_{X \times X}(\pi_2)) \\
= \alpha_{X \times T}(\pi_1 \circ (\text{id}_X \times e))\alpha_{X \times T}(\pi_2 \circ (\text{id}_X \times e)) \\
= \alpha_{X \times T}(r_1)\alpha_{X \times T}(e \circ r_2) \\
= \alpha_{X \times T}(r_1)F(r_2)(\alpha_T(e)) = \alpha_{X \times T}(r_1),
\]

where in the last step, we used the fact that \( \alpha_T(e) = 1 \) and \( F(r_2) \) is a group homomorphism. Since \( \alpha_{X \times T} \) is a bijection, \( m \circ (e \times \text{id}_X) = r_1 \). A similar argument shows that \( m \circ (e \times \text{id}_X) = s_2 \), so we have the required results for \( e \).

Finally, let \( i = \alpha^{-1}_X(\alpha_X(\text{id}_X)^{-1}) : X \to X \). We claim that \( i \) is a valid inverse morphism for giving \( X \) the structure of a group object, i.e. the diagrams below commute, where \( \varphi : X \to T \) is the unique morphism and \( h_1, h_2 : X \to X \times X \) are the unique morphisms such that \( \pi_1 \circ h_1 = \pi_2 \circ h_2 = \text{id}_X \) and \( \pi_2 \circ h_1 = \pi_1 \circ h_2 = i \).

\[
\begin{align*}
X & \xrightarrow{\varphi} X \times X \xrightarrow{m} X \\
T & \xrightarrow{e} X
\end{align*}
\]

\[
\begin{align*}
X & \xrightarrow{h_1} X \times X \xrightarrow{\varphi} X \xrightarrow{m} X \\
X & \xrightarrow{h_2} X \times X \xrightarrow{\varphi} X \xrightarrow{m} X
\end{align*}
\]

39
For this, we compute
\[
\alpha_X(m \circ h_1) = F(h_1)(\alpha_X \times_X (m)) = F(h_1)(\alpha_X \times_X (\pi_1))F(h_1)(\alpha_X \times_X (\pi_2))
\]
\[
= \alpha_X(\pi_1 \circ h_1)\alpha_X(\pi_2 \circ h_1) = \alpha_X(\text{id}_X)\alpha_X(i)
\]
\[
= \alpha_X(\text{id}_X)\alpha_X(\text{id}_X)^{-1} = 1 \in F(X),
\]
\[
\alpha_X(m \circ h_2) = \alpha_X(i)\alpha_X(\text{id}_X)^{-1} = 1 \in F(X),
\]
\[
\alpha_X(e \circ \varphi) = F(\varphi)(\alpha_T(e)) = F(\varphi)(1) = 1 \in F(X).
\]
Thus \(m \circ h_1 = m \circ h_2 = e \circ \varphi\), since \(\alpha_X\) is a bijection, so the proof is complete.

\[\text{Problem 3.}\] Let \(F : \mathcal{C} \to \mathcal{Set}\) be a functor. Consider a new category \(\mathcal{D}\) with objects the pairs \((X, u)\), where \(X\) is an object in \(\mathcal{C}\) and \(u \in F(X)\). A morphism between \((X, u)\) and \((X', u')\) in \(\mathcal{D}\) is a morphism \(f : X \to X'\) in \(\mathcal{C}\) such that \(F(f)(u) = u'\). Prove that if \((X, u)\) is an initial object in \(\mathcal{D}\), then the functor \(F\) is represented by \(X\).

\[\text{Solution.}\] Let \(Y \in \mathcal{C}\). Define a function \(\alpha_Y : \text{Hom}_\mathcal{C}(X, Y) \to F(Y)\) by \(f \mapsto F(f)(u)\). We claim that \(\alpha\) is a natural isomorphism.

- **\(\alpha_Y\) is injective.** If \(v = F(f_1)(u) = F(f_2)(u)\), then \(f_1\) and \(f_2\) both give morphisms \((X, u) \to (Y, v)\).
  Since \((X, u)\) is an initial object of \(\mathcal{D}\), \(f_1 = f_2\).

- **\(\alpha_Y\) is surjective.** Let \(v \in F(Y)\). Since \((X, u)\) is an initial object of \(\mathcal{D}\), there exists \(f : X \to Y\) such that \(F(f)(u) = v\).

- **\(\alpha\) is a natural transformation.** Let \(g : Y \to Z\) be a morphism. We must show that the following diagram commutes.

\[
\begin{array}{ccc}
\text{Hom}_\mathcal{C}(X, Y) & \xrightarrow{f \mapsto \varphi \circ f} & \text{Hom}_\mathcal{C}(X, Z) \\
\downarrow{\alpha_Y} & & \downarrow{\alpha_Z} \\
F(Y) & \xrightarrow{F(g)} & F(Z)
\end{array}
\]

Let \(f \in \text{Hom}_\mathcal{C}(X, Y)\). Then
\[
F(g)(\alpha_Y(f)) = F(g)(F(f)(u)) = (F(g) \circ F(f))(u) = F(g \circ f)(u) = \alpha_Z((g \circ f)(u)).
\]

Having shown that \(\alpha\) is a natural isomorphism, \(F\) is represented by \(X\).

\[\text{Problem 4.}\] Prove that the category \(\mathcal{Set}^{\text{op}}\) is not equivalent to \(\mathcal{Set}\).

\[\text{Solution.}\] Suppose \(F : \mathcal{Set} \to \mathcal{Set}^{\text{op}}\) is an equivalence. Then
\[
F : \text{Hom}_{\mathcal{Set}}(X, Y) \to \text{Hom}_{\mathcal{Set}^{\text{op}}}(F(X), F(Y)) = \text{Hom}_{\mathcal{Set}}(F(Y), F(X))
\]
is a bijection. In particular,
\[
|\text{Hom}_{\mathcal{Set}}(F(\{1, 2\}), F(\{1\})| = |\text{Hom}_{\mathcal{Set}}(\{1\}, \{1, 2\})| = 2,
\]
\[
|\text{Hom}_{\mathcal{Set}}(F(\emptyset), F(\{1, 2\})| = |\text{Hom}_{\mathcal{Set}}(\{1, 2\}, \emptyset)| = 0.
\]
This is a contradiction, as the first equality requires \(F(\{1, 2\}) \neq \emptyset\) while the second equality requires \(F(\{1, 2\}) = \emptyset\). Hence there is no equivalence of \(\mathcal{Set}\) and \(\mathcal{Set}^{\text{op}}\).
Problem 5. Construct a functor $F : \text{Grp} \to \text{Set}$ that assigns to each group the set of its subgroups.

Solution. We are already told how $F$ acts on objects of $\text{Grp}$, so it remains to describe how $F$ acts on morphisms and show that $F$ is a genuine functor.

Let $f : G \to H$ be a group homomorphism. If $L \in F(G)$, i.e. $L$ is a subgroup of $G$, then $f(L)$ is a subgroup of $H$, i.e. $f(L) \in F(H)$. Thus we can define $F(f) : F(G) \to F(H)$ by $L \mapsto f(L)$. Now we check that $F$ respects the identity morphism and composition of morphisms.

(i) For any group $G$ and subgroup $K \leq G$, we have $\text{id}_G(K) = K$, so $F(\text{id}_G) = \text{id}_{F(G)}$.

(ii) Let $G \xrightarrow{f} H \xrightarrow{g} K$ be group homomorphisms and $L \leq G$ be a subgroup. Then

$$F(g \circ f)(L) = (g \circ f)(L) = g(f(L)) = F(g)(F(f)(L)) = (F(g) \circ F(f))(L).$$

Problem 6. Prove that if a functor $F : \mathcal{C} \to \mathcal{D}$ is an equivalence of categories, then $X$ and $Y$ are isomorphic in $\mathcal{C}$ if and only if $F(X)$ and $F(Y)$ are isomorphic in $\mathcal{D}$.

Solution. $(\implies)$ Let $f : X \to Y$ be an isomorphism. Then

$$F(f) \circ F(f^{-1}) = F(f \circ f^{-1}) = F(\text{id}_Y) = \text{id}_{F(Y)},$$

and similarly $F(f^{-1}) \circ F(f) = \text{id}_{F(X)}$. Thus $F(f) : F(X) \to F(Y)$ is an isomorphism.

$(\impliedby)$ Let $h : F(X) \to F(Y)$ be an isomorphism. Since $F$ is full, there exist $f \in \text{Hom}_\mathcal{C}(X, Y)$ and $g \in \text{Hom}_\mathcal{C}(Y, X)$ such that $F(f) = h$ and $F(g) = h^{-1}$. Then

$$F(f \circ g) = F(f) \circ F(g) = \text{id}_{F(Y)} = F(\text{id}_Y).$$

Since $F$ is faithful, $f \circ g = \text{id}_Y$. Similarly, $g \circ f = \text{id}_X$, so $f : X \to Y$ is an isomorphism.

□
Problem 7. Consider a category $\mathcal{C}$ with the set of objects $\{0,1,2,\ldots\}$ and morphisms $\text{Hom}(i,j)$ the set of all $j \times i$ matrices over $\mathbb{R}$ (with composition the matrix multiplication). Construct an equivalence between $\mathcal{C}$ and the category of real finite-dimensional vector spaces.

Solution. Define a functor $F : \mathcal{C} \to \mathbb{R}\text{-FdVect}$ by

$$n \mapsto \mathbb{R}^n \quad \text{and} \quad M \in \text{Hom}(i,j) \mapsto F(M) \in \mathcal{L}(\mathbb{R}^i,\mathbb{R}^j),$$

where $\mathbb{R}^0 = 0$ and $F(M) \in \mathcal{L}(\mathbb{R}^i,\mathbb{R}^j)$ is the linear map induced by $M$ with respect to the standard bases. By standard facts of linear algebra,

- the identity matrix $I_n$ induces the identity map on $\mathbb{R}^n$;
- composition of linear maps is given by multiplication of matrices, so $F$ is a genuine functor;
- every linear map can be given by a matrix with respect to the standard bases, so $F$ is full;
- the matrix of a linear map with respect to the standard bases is unique, so $F$ is faithful;
- every finite-dimensional real vector space is isomorphic to $\mathbb{R}^n$ for some $n$.

Putting these together, $F$ is an equivalence.

Problem 8. Let $F : \mathcal{A} \to \mathcal{B}$ be a functor. Suppose that $F$ has a left adjoint functor. Prove that $F$ takes terminal objects of $\mathcal{A}$ to terminal objects of $\mathcal{B}$.

Solution. Let $G : \mathcal{B} \to \mathcal{A}$ be a left adjoint to $F$ and let $X \in \mathcal{A}$ be a terminal object. For any object $Y \in \mathcal{B}$, we have $\text{Hom}_\mathcal{B}(Y,F(X)) \cong \text{Hom}_\mathcal{A}(G(Y),X)$. Since $X$ is a terminal object, there is exactly one morphism $G(Y) \to X$, so there is exactly one morphism $Y \to F(X)$. Since $Y$ is arbitrary, $F(X)$ is a terminal object in $\mathcal{B}$.

Problem 9. Determine the limit and colimit of the following diagram in $\text{Set}$.

\[
\begin{array}{ccc}
X & \longrightarrow & Y \\
\downarrow & & \downarrow \\
Z & \longrightarrow & T
\end{array}
\]

Solution. Let $Z$ be a limit of the diagram below, i.e. for any other object $T$ with morphisms as shown, there is a unique morphism $k : T \to Z$ such that the diagram commutes.

\[
\begin{array}{ccc}
T & \longrightarrow & Z \\
\downarrow & & \downarrow \\
\downarrow & & \downarrow \\
X & \longrightarrow & Y
\end{array}
\]

This is precisely the equalizer (kernel) of $f$ and $g$, which exists by Homework 7 Problem 10. Similarly, the colimit is the coequalizer (cokernel) of $f$ and $g$.
Problem 10. Prove that limits and colimits exist in \textbf{Set} and \textbf{Grp}.

\textit{Solution.} Let $\mathcal{I}$ be a small category with $\text{Ob}\mathcal{C} = \{X_i\}_{i \in I}$ and $F : \mathcal{I} \to \textbf{Set}$ be a functor. Let $Z = \prod_i F(X_i)$, together with projections $\pi_i : Z \to F(X_i)$. (Products exist in \textbf{Set}.) We claim that the limit of $F : \mathcal{I} \to \textbf{Set}$ is

$$L = \{ z \in Z \mid F(f)(\pi_i(z)) = \pi_j(z) \text{ for all } i,j \text{ and morphisms } f : X_i \to X_j \}.$$  

By construction, we have $F(f) \circ \pi_i = \pi_j$ for all $i,j$ and morphisms $f : X_i \to X_j$. Let $L'$ be another set with morphisms $p_i : L' \to F(X_i)$ such that $F(f) \circ p_i = p_j$ for all $i,j$ and morphisms $f : X_i \to X_j$. By the universal property of products, there is a unique morphism $p : L' \to Z$ such that $\pi_i \circ p = p_i$ for all $i$. If $f : X_i \to X_j$ is a morphism, then

$$F(f) \circ (\pi_i \circ p) = (F(f) \circ \pi_i) \circ p = \pi_j \circ p.$$  

Thus $p(L')$ lies in $L$, so in fact we can regard $p$ as the unique morphism $L' \to L$ we required.

For the colimit, let $W = \bigsqcup_i X_i$, together with the inclusions $i_i : X_i \to W$. (Coproducts, i.e. disjoint unions, exist in \textbf{Set}.) We claim that the colimit of $F$ is

$$K = W/ \sim, \quad F(f)(x) \sim F(g)(x) \text{ for all } i, x \in X_i \text{ and morphisms } f, g : X_i \to X_j.$$  

That this is correct follows by an analogous argument.

For the limit in \textbf{Grp}, we use the same construction, but we must also check that $L$ is a group. This follows from the fact that $F(f)$ is a homomorphism for all morphisms $f \in \text{Hom}\mathcal{C}$, and the projections $\pi_i$ are also homomorphisms.

For the colimit in \textbf{Grp}, the disjoint union is replaced with the coproduct in groups, and we quotient by the normal subgroup generated by the relation $\sim$.  \hfill $\square$
HOMEWORK 9 - SOLUTIONS

Problem 1. Let \((G, m, e, i)\) be a group object in the category of groups. Prove that \(G\) is an abelian group and \(m : G \times G \to G, e : 1 \to G, \) and \(i : G \to G\) are the product map, the unit map, and the inverse map, respectively.

Solution. It is clear that \(e\) is the unit map, since 1 is the initial object in \(\text{Grp}\). Then, from the diagram defining \(e\),
\[
m(a, 1) = m(\text{id}_G(a), e(1)) = \pi_1(a, 1) = a,
\]
and similarly \(m(1, b) = b\). Therefore, since \(m\) is a homomorphism,
\[
m(a, b) = m(a, 1)m(1, b) = ab,
\]
so \(m\) is the product map. From the diagram defining \(i\),
\[
a \cdot i(a) = m(a, i(a)) = 1,
\]
so \(i\) is the inverse map. For \(i\) to be a homomorphism, we require that for all \(a, b \in G\),
\[
ab = i(b^{-1}a^{-1}) = i(b^{-1})i(a^{-1}) = ba,
\]
so \(G\) is abelian.

Problem 2. Let \(F : \mathcal{I} \to \mathcal{C}\) be a functor from a small category \(\mathcal{I}\) with an initial object \(i\). Prove that \(\lim F \cong F(i)\).

Solution. Let \(\text{Ob} \mathcal{I} = \{X_j\}_{j \in J}\) for some index set \(J\), and for each \(j\), let \(f_j : i \to X_j\) be the unique morphism. Let \(g_j : \lim F \to F(X_j)\) be morphisms for which whenever \(f : X_j \to X_k\) is a morphism in \(\mathcal{I}\), we have \(F(f) \circ g_j = g_k\). By the universal property of limits, applied to the object \(F(i)\) with morphisms \(F(f_j) : F(i) \to F(X_j)\), there exists a unique morphism \(h : F(i) \to \lim F\) such that \(g_j \circ h = F(f_j)\) for all \(j \in J\). In particular, choosing \(\gamma \in J\) with \(X_\gamma = i\), we have
\[
g_\gamma \circ h = F(\text{id}_i) = \text{id}_{F(i)}.
\]
To show that \(h \circ g_\gamma = \text{id}_{\lim F}\), note that \(g_\gamma \circ h \circ g_\gamma = g_\gamma\), so for any \(j\),
\[
g_j = F(f_j) \circ g_\gamma = F(f_j) \circ g_\gamma \circ h \circ g_\gamma = g_j \circ h \circ g_\gamma.
\]
By the universal property of limits, applied to the object \(\lim F\) with morphisms \(g_j : \lim F \to F(X_j)\), there exists a unique morphism \(k : \lim F \to \lim F\) such that \(g_j \circ k = g_j\) for all \(j \in J\). Both \(h \circ g_\gamma\) and \(\text{id}_{\lim F}\) satisfy this condition, so \(h \circ g_\gamma = \text{id}_{\lim F}\). Thus \(h : F(i) \to \lim F\) is an isomorphism.
Problem 3. Determine initial and terminal objects in the category of rings.

Solution. We claim that \( \mathbb{Z} \) is an initial object in \( \text{Ring} \). Let \( R \) be a ring and \( f : \mathbb{Z} \to R \) be a homomorphism. Then \( f : (\mathbb{Z}, +) \to (R, +) \) is a group homomorphism, so \( f \) is completely determined by the image of the generator 1 of \( \mathbb{Z} \). For \( f \) to be a ring homomorphism, we must have \( f(1) = 1 \in R \), so if \( f \) exists, then \( f \) is unique. To demonstrate existence of \( f \), we start from \( f(1) = 1 \) and extend it to a group homomorphism \( f : (\mathbb{Z}, +) \to (R, +) \). It remains to show that \( f(ab) = f(a)f(b) \) for all \( a, b \in \mathbb{Z} \). Fix \( a \) and induct forwards and backwards on \( b \). As a base case, we have

\[
 f(a \cdot 0) = f(0) = 0 = f(a)f(0). 
\]

Then, if \( f(ab) = f(a)f(b) \), we have

\[
 f(a(b - 1)) = f(ab - a) = f(ab) - f(a) = f(a)f(b) - f(a) = f(a)(f(b) - 1) = f(a)f(b - 1),
\]

\[
 f(a(b + 1)) = f(ab + a) = f(ab) + f(a) = f(a)f(b) + f(a) = f(a)(f(b) + 1) = f(a)f(b + 1). 
\]

This completes the proof that \( f \) is a ring homomorphism, so \( \mathbb{Z} \) is an initial object. It is clear that 0 is the terminal object in \( \text{Ring} \). \( \square \)

Problem 4. Prove that a finite non-zero ring with no zero divisors is a division ring and a finite integral domain is a field.

Solution. Let \( R \) be a finite non-zero ring with no zero divisors and let \( r \neq 0 \) be an element of \( R \). We claim that \( a \mapsto ar \) is an injective function. Indeed, if \( ar = br \), then \( (a - b)r = 0 \), and since \( R \) has no zero divisors and \( r \neq 0 \), this means \( a - b = 0 \), so \( a = b \). Since \( R \) is finite and \( a \mapsto ar \) is injective, it is also surjective, so there exists \( s \in R \) with \( sr = 1 \). By a similar argument, there exists \( t \in R \) with \( rt = 1 \). Then \( s = s(rt) = (sr)t = t \), so \( r \) is invertible and \( R \) is a division ring. If \( R \) is a finite integral domain, then it is a commutative division ring, i.e. a field. \( \square \)

Problem 5. Let \( R \) be the set of all \( 2 \times 2 \) matrices over \( \mathbb{C} \) of the form

\[
 \begin{pmatrix} u & v \\ -\overline{v} & \overline{u} \end{pmatrix}. 
\]

Show that \( R \) is a subring of \( \text{Mat}_2(\mathbb{C}) \) that is isomorphic to the ring of real quaternions \( \mathbb{H} \).

Solution. Letting \( (u, v) = (1, 0) \) gives \( I \in R \), and we can compute

\[
 \begin{pmatrix} u & v \\ -\overline{v} & \overline{u} \end{pmatrix} + \begin{pmatrix} r & s \\ -\overline{s} & \overline{r} \end{pmatrix} = \begin{pmatrix} u + r & v + s \\ -\overline{v} - \overline{s} & \overline{u} + \overline{r} \end{pmatrix} + \begin{pmatrix} u + r & v + s \\ -(v + s) & u + r \end{pmatrix},
\]

\[
 \begin{pmatrix} u & v \\ -\overline{v} & \overline{u} \end{pmatrix} \begin{pmatrix} r & s \\ -\overline{s} & \overline{r} \end{pmatrix} = \begin{pmatrix} ur - vs & us + vr \\ -\overline{vr} - \overline{us} & -\overline{vs} + \overline{wr} \end{pmatrix} = \begin{pmatrix} ur - vs & us + vr \\ -(us + vr) & ur - vs \end{pmatrix},
\]

so \( R \subset \text{Mat}_2(\mathbb{C}) \) is a subring.

If we write \( u = a + bi \) and \( v = c + di \), then the isomorphism to \( \mathbb{H} \) is

\[
 \begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix} \mapsto a + bi + cj + dk. 
\]

\( \square \)
Problem 6. (a) Prove that a non-zero matrix \( a \in \text{Mat}_n(F) \), where \( F \) is a field, is a zero divisor if and only if \( \det a = 0 \).

(b) Prove that a non-zero matrix \( a \in \text{Mat}_n(R) \), where \( R \) is a commutative ring, is a zero divisor if \( \det a = 0 \).

Solution. (a) \( (\implies) \) We show the contrapositive, so suppose \( \det a \neq 0 \). Then \( a \) is invertible (standard linear algebra), so if \( ab = 0 \) then \( b = a^{-1}(ab) = 0 \), and similarly, if \( ba = 0 \), then \( b = 0 \). Hence \( a \) is not a zero-divisor.

\( (\impliedby) \) This is a special case of part (b).

(b) If \( \det a = 0 \), then \( (\text{adj} \ a)a = a(\text{adj} \ a) = (\det a)I = 0 \), so \( a \) is a zero divisor. Here \( \text{adj} \ a \) is the adjugate matrix of \( a \), defined in terms of minors / cofactors.

Problem 7. Let \( S = \text{Mat}_n(R) \), where \( R \) is a ring with identity. Show that for any ideal \( J \subset S \), there is a unique ideal \( I \subset R \) such that \( J \) is the set of all \( n \times n \) matrices with the elements in \( I \).

Solution. Let \( I \subset R \) be the set of all elements of \( R \) which appear as an entry of a matrix in \( J \). We claim that \( I \) is an ideal and \( J = \text{Mat}_n(I) \).

First, let \( e_{ij} \in S \) be the matrix with 1 in the \( i,j \)-position and 0’s elsewhere. Then for \( A \in J \), \( e_{ij}Ae_{kl} \in J \) is the matrix with \( A_{jk} \) in the \( i,l \)-position and 0’s elsewhere. By applying row and column swaps, we can obtain a matrix with \( A_{jk} \) in the upper left position and 0’s elsewhere. Thus if \( M(r) = \begin{pmatrix} r & 0 \\ 0 & 0 \end{pmatrix} \), we have that \( M(r) \in J \) if and only if \( r \in I \).

Let \( a, b \in I \) and \( r \in R \). Then the matrices

\[
M(a) + M(b) = M(a + b), \quad M(a)M(r) = M(ar), \quad M(r)M(a) = M(ra),
\]

are in \( J \), so \( a + b, ar, ra \in I \), i.e. \( I \) is an ideal.

By construction, \( J \subset \text{Mat}_n(I) \). For the other inclusion, let \( A \in \text{Mat}_n(I) \). By row and column swaps applied to \( M(A_{ij}) \in J \), we can obtain a matrix \( B_{ij} \in J \) with \( A_{ij} \) in the \( i,j \)-position and 0’s elsewhere. Then \( A = \sum_{i,j} B_{ij} \in J \), as required. Uniqueness of \( I \) is trivial.

Problem 8. (a) Let \( f : R \rightarrow S \) be a ring homomorphism, \( I \) be an ideal in \( R \), and \( J \) be an ideal in \( S \). Show that \( f^{-1}(J) \) is an ideal in \( R \) that contains \( \ker f \).

(b) If \( f \) is surjective, then \( f(I) \) is an ideal in \( S \). If \( f \) is not surjective, \( f(I) \) need not be an ideal in \( S \).

Solution. (a) We have \( f(f^{-1}(J) + f^{-1}(J)) = J + J = J \), so \( f^{-1}(J) \) is additively closed, and \( f(Rf^{-1}(J)) = f(R)J = J \), so \( f^{-1}(J) \) is a left ideal, and similarly \( f^{-1}(J) \) is a right ideal. Since \( f(\ker f) = 0 \subset J \), we have \( \ker f \subset f^{-1}(J) \).

(b) If \( f \) is surjective, then \( f(I) + f(I) = f(I + I) = f(I) \), so \( f(I) \) is additively closed, and \( Sf(I) = f(R)f(I) = f(RI) = f(I) \), so \( f(I) \) is a left ideal, and similarly \( f(I) \) is a right ideal.

The inclusion \( i : Z \rightarrow Q \) is not surjective, and the image of the ideal \( Z \) is not an ideal of \( Q \).
Problem 9.  (a) An element $a$ of a ring $R$ is called nilpotent if $a^n = 0$ for some $n$. Show that if $R$ is a commutative ring, then the set $\text{Nil} R$ of all nilpotent elements in $R$ is an ideal, called the nilradical of $R$. Prove that the factor ring $R/\text{Nil} R$ has no non-zero nilpotent elements.

(b) Prove that a polynomial $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$ (where $R$ is a commutative ring) is nilpotent if and only if all $a_i$ are nilpotent in $R$.

Solution.  (a) Let $a, b \in \text{Nil} R$ with $a^n = 0$ and $b^m = 0$. Then

$$(a + b)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} a^k b^{n+m-k} = 0,$$

as either $k \geq n$ or $n+m-k \geq m$ for all $k$. Hence $\text{Nil} R$ is additively closed. Now let $a \in \text{Nil} R$ with $a^n = 0$ and $r \in R$. Then $(ra)^n = r^n a^n = 0$, so $ra \in \text{Nil} R$. Suppose $a + \text{Nil} R$ is nilpotent for some $a \in R$. Then for some $n$, we have

$$\text{Nil} R = (a + \text{Nil} R)^n = a^n + \sum_{k=1}^{n} \binom{n}{k} a^k (\text{Nil} R)^{n-k} = a^n + \text{Nil} R,$$

since $\text{Nil} R$ is an ideal. Thus $a^n \in \text{Nil} R$, so there is some $m$ with $(a^n)^m = a^{nm}$, hence $a$ is nilpotent and $a + \text{Nil} R = \text{Nil} R$ is the zero element of $R/\text{Nil} R$.

(b) First suppose $f \in \text{Nil}(R[x])$. We prove by induction that $f \in (\text{Nil} R)[x]$. If $\deg f = 0$, the result is obvious. Otherwise, let $\deg f = n > 0$. If $f$ is nilpotent, then $f^m = 0$ for some $m$. The coefficient of $x^m$ is $a_m = 0$, so $a_n$ and $a_n x^n$ are nilpotent. Since $\text{Nil}(R[x])$ is an ideal, $f - a_n x^n = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$ is nilpotent and has degree $n - 1$. By the inductive hypothesis, $a_i \in \text{Nil} R$ for $i = 0, 1, \ldots, n - 1$. Hence $f \in (\text{Nil} R)[x]$.

Conversely, if $f \in (\text{Nil} R)[x]$ and $a_i^{m_i} = 0$ for some $m_i$, then $f^{m_0 + \cdots + m_n} = 0$ by the same reasoning as for showing that $\text{Nil} R$ is an ideal. Hence $f \in \text{Nil}(R[x])$.

Problem 10.  (a) Prove that if $a$ is a nilpotent element of a ring $R$, then $1 + a$ is invertible.

(b) Prove that a polynomial $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$ (where $R$ is a commutative ring) is invertible in $R[x]$ if and only if $a_0$ is invertible and $a_i$ is nilpotent in $R$ for $i \geq 1$.

Solution.  (a) If $a^n = 0$, then

$$(1 + a)(1 - a + a^2 - \cdots + (-1)^{n-1} a^{n-1}) = 1 + (-1)^n a^n = 1.$$

(b) Write $f = a_0 + a_1 x + \cdots + a_n x^n = a_0 + xg$ for $g \in R[x]$. If $a_0$ is invertible and $a_i$ is nilpotent for $i \geq 1$, then $g$ is nilpotent by Problem 9(b), so by part (a), $a_0^{-1} f = 1 + a_0^{-1} xg$ is invertible, hence also $f$.

Conversely, let $f$ be invertible with inverse $h = b_0 + b_1 x + \cdots + b_m x^m$. Then $a_0 b_0 = 1$, so $a_0$ is invertible. Without loss of generality, suppose $a_0 = b_0 = 1$. We have $a_n b_n = 0$ and $a_{n-1} b_n + a_n b_{n-1} = 0$. Multiplying through by $a_n$, we have $a_n^2 b_{n-1} = 0$. Continuing in this way, we eventually get $a_n^{n+1} b_0 = a_n^{n+1} = 0$, so $a_n$ is nilpotent. The proof is then complete by induction on $n$, as if $f$ is invertible and $a_n x^n$ is nilpotent, then $f - a_n x^n$ is invertible.