Problem 1. Classify all abelian groups of order 32.

Solution. Let $G$ be a group such that $|G| = 32 = 2^5$. Consider the exponent of 2. There are 7 ways to add natural numbers less than or equal to 5 to get 5: $0 + 5, 1 + 1 + 1 + 1 + 1, 2 + 1 + 1 + 1, 2 + 2 + 1, 3 + 1 + 1, 1 + 4$, and $3 + 2$.

By the Fundamental Theorem of Finite Abelian Groups, $G$ is uniquely isomorphic to one of the following 7 groups:

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

$$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

$$\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

$$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

$$\mathbb{Z}/16\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

$$\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$$

$$\mathbb{Z}/32\mathbb{Z}$$
Problem 2. For arbitrary prime $p$, construct a non-abelian group of order $p^3$.

Solution. Consider the Heisenberg Group

$$H(p) = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{Z}/p\mathbb{Z} \right\}.$$ 

First since there are $p$ options for $a$, $b$, and $c$, we see that $|H(p)| = p^3$. We can see that

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in H(p)$$

is the identity element. Inverses are given by

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

Now to show that $H(p)$ is closed, take $a_1, b_1, c_1, a_2, c_2, b_2 \in \mathbb{Z}/p\mathbb{Z}$. Then,

$$\begin{pmatrix} 1 & a_1 & c_1 \\ 0 & 1 & b_1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a_2 & c_2 \\ 0 & 1 & b_2 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a_1 + a_2 & c_2 + a_1b_2 + c_1 \\ 0 & 1 & b_1 + b_2 \\ 0 & 0 & 1 \end{pmatrix} \in H(p).$$

Thus $H(p)$ is a group of order $p^3$. We now want to show that it is not abelian. Define

$$X := \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \quad \quad Y := \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$ 

Then,

$$XY = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

$$YX = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$ 

Thus $XY \neq YX$ and $H(p)$ is not abelian.
Problem 3. Let \( k \) be a field, \( x \) an indeterminate. For distinct \( a_1, \ldots, a_n \) in \( k \), prove that there are unique \( A_1, \ldots, A_n \in k \) such that

\[
\frac{1}{(x-a_1)(x-a_2) \cdots (x-a_n)} = \frac{A_1}{x-a_1} + \frac{A_2}{x-a_2} + \cdots + \frac{A_n}{x-a_n} \quad \text{(in } k(x)\text{)}.
\]

Proof. We will prove this by induction.

base case: as \( n = 1 \) is trivial, consider \( n = 2 \). We attempt to solve

\[
\frac{1}{(x-a_1)(x-a_2)} = \frac{A_1}{x-a_1} + \frac{A_2}{x-a_2}.
\]

If that were to be true then

\[
A_1 + A_2 = 0
\]

\[-A_1 a_2 - A_2 a_1 = 1
\]

must hold (matching coefficients). If \( A_1 + A_2 = 0 \), then \(-A_1 = A_2\) and \(-A_1 a_2 - A_2 a_1 = 1\) becomes \(A_2(a_2 - a_1) = 1\). So we have that

\[
A_1 = \frac{1}{a_1 - a_2} \quad A_2 = \frac{1}{a_2 - a_1}.
\]

Since \( a_1 \neq a_2 \), we have found \( A_1 \) and \( A_2 \) such that

\[
\frac{1}{(x-a_1)(x-a_2)} = \frac{A_1}{x-a_1} + \frac{A_2}{x-a_2}
\]

holds.

inductive step: Assume that if \( a_1, \ldots, a_i \) are distinct in \( k \), then there exists \( A_1, \ldots, A_i \) such that

\[
\frac{1}{(x-a_1) \cdots (x-a_i)} = \frac{A_1}{x-a_1} + \cdots + \frac{A_i}{x-a_i}.
\]

We want to show it holds for \( n = i + 1 \).

\[
\frac{1}{(x-a_1) \cdots (x-a_i)(x-a_{i+1})} = \frac{1}{(x-a_1) \cdots (x-a_i)} \cdot \frac{1}{(x-a_{i+1})} = \left( \frac{A_1}{x-a_1} + \cdots + \frac{A_i}{x-a_i} \right) \cdot \frac{1}{(x-a_{i+1})}, \text{ by the inductive hypothesis}
\]

\[
= \frac{A_1}{(x-a_1)(x-a_{i+1})} + \cdots + \frac{A_i}{(x-a_i)(x-a_{i+1})}
\]

\[
= \sum_{m=1}^{i} A_m \cdot \frac{1}{(x-a_m)(x-a_{i+1})}
\]

\[
= \sum_{m=1}^{i} A_m \left( \frac{\alpha_m}{x-a_m} + \frac{\beta_m}{x-a_{i+1}} \right), \text{ by the base case}
\]

\[
= \frac{A_1 \alpha_1}{x-a_1} + \cdots + \frac{A_i \alpha_i}{x-a_i} + \sum_{m=1}^{i} A_m \beta_m
\]

\[
= \frac{A_1}{x-a_1} + \cdots + \frac{A_i}{x-a_i} + \sum_{m=1}^{i} A_m \beta_m
\]
Thus we have found new $A'_1, \ldots, A'_{i+1} \in k$ such that
\[
\frac{1}{(x - a_1) \cdots (x - a_i)(x - a_{i+1})} = \frac{A'_1}{x - a_1} + \cdots + \frac{A'_i}{x - a_i} + \frac{A'_{i+1}}{x - a_{i+1}}
\]
holds. Thus by the Principle of Mathematical Induction, for distinct elements $a_1, \ldots, a_n$ of a field $k$, there exists $A_1, \ldots, A_n$ such that
\[
\frac{1}{(x - a_1) \cdots (x - a_n)} = \frac{A_1}{x - a_1} + \cdots + \frac{A_n}{x - a_n}.
\]
Problem 4. Let $S, T$ be linear operators on a finite dimensional complex vector space, with $ST = TS$. Show that $S$ and $T$ have a common eigenvector.

Proof. Let $V$ be the finite-dimensional complex vector space on which $S$ and $T$ are linear operators. Since $\mathbb{C}$ is algebraically closed, there exists a root of the minimum polynomial of $T$, $\lambda \in \mathbb{C}$, which is an eigenvalue of $T$, with a corresponding non-zero eigenvector.

Let $V_\lambda$ denote the $\lambda$-eigenspace. That is,

$$V_\lambda = \{v \in V \mid Tv = \lambda v\}.$$ 

So, $\forall v \in V_\lambda$, since $S$ and $T$ commute,

$$T(Sv) = TSv = STv = S\lambda v = \lambda Sv = \lambda (Sv).$$

Thus $S$ stabilizes $V_\lambda$. In other words, $S$ maps vectors in $V_\lambda$ to vectors in $V_\lambda$. So $S$ is a linear operator on $V_\lambda$. Let $f(x)$ represent the minimum polynomial of $S$ on $V_\lambda$. Since $\mathbb{C}$ is algebraically closed, $f(x)$ had a root, $\gamma \in \mathbb{C}$, which is an eigenvalue of $S$ on $V_\lambda$ with corresponding non-trivial eigenvector $u \in V_\lambda$. Since $f(x)$ must divide the minimum polynomial of $S$ on all of $V$, we know that $\gamma$ is an eigenvalue of $S$ on all of $V$ and hence $u \in V_\lambda$ is an eigenvector of $S$ on all of $V$.

Thus, since $u \in V_\lambda$, we have that $Tu = \lambda u$, and by definition, $Su = \gamma u$. So $S$ and $T$ have a common eigenvector. \qed
Problem 5. Show that the ideal generated by 13 and \( x^3 - 2 \) in \( \mathbb{Z}[x] \) is maximal.

Proof. We can show that \( \langle 13, x^3 - 2 \rangle \) is maximal if we can show that

\[
\mathbb{Z}[x]/\langle 13, x^3 - 2 \rangle \cong (\mathbb{Z}/13\mathbb{Z})[x]/\langle x^3 - 2 \rangle
\]

is a field.

Since \( \mathbb{Z}/13\mathbb{Z} \) is a field, \( \mathbb{Z}/13\mathbb{Z} \) is a PID and hence a UFD. Thus, all irreducible elements are prime in \( (\mathbb{Z}/13\mathbb{Z})[x] \). Since any prime ideal is maximal in a PID, it remains to be shown that \( x^3 - 2 \) is irreducible in \( (\mathbb{Z}/13\mathbb{Z})[x] \).

Suppose for contradiction that \( x^3 - 2 \) is reducible in \( (\mathbb{Z}/13\mathbb{Z})[x] \). That is, \( \exists \alpha \in \mathbb{Z}/13\mathbb{Z} \) such that \( \alpha^3 - 2 = 0 \implies \alpha^3 = 2 \). Since \( |(\mathbb{Z}/13\mathbb{Z})^\times| = 12 \), we know that \( \alpha^{12} = 1 \). But,

\[
\alpha^{12} = (\alpha^3)^4 = 2^4 = 16 = 3 \mod 13 \neq 1 \in (\mathbb{Z}/13\mathbb{Z})^\times.
\]

Thus, \( x^3 - 2 \) is irreducible in \( \mathbb{Z}/13\mathbb{Z} \) and \( \langle x^3 - 2 \rangle \) is a prime ideal and hence a maximal ideal of \( (\mathbb{Z}/13\mathbb{Z})[x] \). Thus,

\[
(\mathbb{Z}/13\mathbb{Z})[x]/\langle x^3 - 2 \rangle \cong \mathbb{Z}[x]/\langle 13, x^3 - 2 \rangle
\]

is a field. Therefore, \( \langle 13, x^3 - 2 \rangle \) is a maximal ideal in \( \mathbb{Z}[x] \). \( \square \)
Problem 6. Let $R$ be a commutative ring with unit. Show that the collection of all nilpotent elements of $R$ is an ideal.

Proof. Let $I := \{ x \in R \mid x^n = 0 \text{ for some } n \in \mathbb{N} \}$ (the collection of all nilpotent elements). We want to show that $I$ is in fact an ideal. Thus we need to show that $I$ is an additive subgroup of $R$ and that $\forall x \in I, \forall r \in R, xr \in I$ and $rx \in I$. Let $x^n = y^m = 0$ for some $n, m \in \mathbb{N}$.

First we will show that $I$ is an additive subgroup of $R$. Consider $(x + y)^{n+m}$. By the Binomial Theorem,

$$(x + y)^{n+m} = \sum_{k=1}^{n+m} \binom{n+m}{k} x^k y^{n+m-k}.$$

If $k \geq n$, then

$$x^k = x^{n+k-n} = x^n x^{k-n} = 0.$$

Similarly, if $k < n$, then

$$y^{n+m-k} = y^m y^{n-k} = 0.$$

Thus $(x + y) \in I$. Moreover, $(-x)^n = (-1)^n x^n = 0 \in I$, and thus $(-x) \in I$. Also notice that $0 = 0^1$ so $0 \in I$. Thus, $I$ is an additive subgroup of $R$.

Let $r \in R$. Then since $R$ is commutative,

$$\begin{align*}
(rx)^n &= r x \cdot r x \cdots r x = r \cdot r \cdots r x \cdot x \cdots x = r^n x^n = 0 \\
(xr)^n &= x r \cdot x r \cdots x r = x \cdot x \cdots x r \cdot r \cdots r = x^n r^n = 0
\end{align*}$$

Thus, $\forall x \in I$ and $\forall r \in R$, we have that $xr, rx \in I$.

So the collection of all nilpotent elements of $R$ is an ideal. $\square$
Problem 7. Show that $x^5 - 2$ is irreducible in $\mathbb{F}_{11}[x]$.

Proof. To show that $x^5 - 2$ is irreducible in $\mathbb{F}_{11}[x]$, it suffices to show that $x^5 - 2$ has no linear or quadratic factors.

First we notice that $|\mathbb{F}_{11}^\times| = 10$, so a linear factor $\alpha$ would have the property $\alpha^{10} = 1$. If additionally, $\alpha$ was a root of $x^5 - 2$, then $\alpha^5 = 2$ must hold. Then, we get the contradiction

$$\alpha^{10} = (\alpha^5)^2 = 2^2 = 4 \neq 1.$$ 

Thus, $x^5 - 2$ has no linear factors.

If $x^5 - 2$ has a quadratic factor, it would lie in $\mathbb{F}_{11^2}^\times$. Notice that $|\mathbb{F}_{11^2}^\times| = 120$. So if $\alpha$ is a root of $x^5 - 2$, then $\alpha^{120} = 1$ and $\alpha^5 = 2$. Then we once again come across a contradiction,

$$\alpha^{120} = (\alpha^5)^{24} = 2^{24} = 16777215 = 5 \neq 1.$$ 

Thus, $x^5 - 2$ has no quadratic factors.

Since $x^5 - 2$ has no linear or quadratic factors, it is irreducible in $\mathbb{F}_{11}[x]$. \qed