Problem 1. The commutator subgroup $C$ of a group $G$ is the subgroup generated by all commutators $ghg^{-1}h^{-1}$. Show that $C$ is normal, that $G/C$ is abelian, and that any homomorphism $G \to A$ of $G$ to an abelian group $A$ has kernel containing $C$.

Proof. First we will show that $C$ is normal. Let $k \in G$ and $ghg^{-1}h^{-1} \in C$. Then,

\[
k^{-1}ghg^{-1}h^{-1}k = k^{-1}ghg^{-1}kk^{-1}h^{-1}k
= (k^{-1}g)h(k^{-1}g)^{-1}h^{-1}hk^{-1}h^{-1}k
= (k^{-1}g)h(k^{-1}g)^{-1}h^{-1} \cdot hk^{-1}h^{-1}k
\]

where $(k^{-1}g)h(k^{-1}g)^{-1}h^{-1} \in C$ and $hk^{-1}h^{-1}k \in C$. Thus, $k^{-1}ghg^{-1}h^{-1}k \in C$ and $C$ is normal in $G$.

Now we want to show that $G/C$ is abelian. Let $g, h \in G$. We examine the cosets $gC$ and $hC$. We want to show that $gChC = hCgC$. Note that $ghg^{-1}h^{-1} \in C$ implies that $ghg^{-1}h^{-1}C = C$. Also, since $C$ is normal, we know that $(gh)C = gChC$. So,

\[
ghg^{-1}h^{-1}C = C \\
(gh)(g^{-1}h^{-1})C = C \\
(gh)(h)C = C \\
(g)C = (h)C \\
gChC = hCgC.
\]

Thus, $G/C$ is abelian.

Lastly, we want to show that any homomorphism $G \to A$ of $G$ to an abelian group $A$ has a kernel containing $C$. Let $\varphi : G \to A$ be a homomorphism (we will use multiplicative notation for $A$). In particular, we have that $\varphi(1) = 1 \in A$ and $\varphi(ab) = \varphi(a)\varphi(b)$. So consider $ghg^{-1}h^{-1} \in C$, then

\[
\varphi(ghg^{-1}h^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1})\varphi(h^{-1})
= \varphi(g)\varphi(g^{-1})\varphi(h)\varphi(h^{-1})
= \varphi(gg^{-1})\varphi(hh^{-1})
= \varphi(1)\varphi(1) = 1 \in A
\]

Thus, $ghg^{-1}h^{-1} \in \ker(\varphi)$. Since $ghg^{-1}h^{-1}$ was an arbitrary element of $C$, we have that $C$ is contained in the kernel of $\varphi$, an arbitrary homomorphism from $G \to A$. $\square$
Problem 2. Show that a group $G$ of order $pq^2$, with $p$ and $q$ distinct primes, has a proper normal subgroup.

Proof. By the Sylow Theorems, there exists a $p$-Sylow subgroup, $H_p$, such that $|H_p| = p$, and a $q$-Sylow subgroup, $H_q$, such that $|H_q| = q^2$.

Case 1: $p < q$
If $p < q$, then we see that $[G : H_q] = p$, where $p$ is the smallest prime dividing the order of $G$. Thus $H_q$ is normal in $G$.

Case 2: $p > q$
By the Sylow Theorems, the number of $p$-Sylow subgroups, $n_p$, and the number of $q$-Sylow subgroups, $n_q$, have the following properties:

\[
\begin{align*}
    n_p &\equiv 1 \pmod{p}, \quad n_p \mid q^2 &\implies n_p = 1, q, q^2 \\
    n_q &\equiv 1 \pmod{q}, \quad n_q \mid p &\implies n_q = 1, p
\end{align*}
\]

If $n_q = 1$, then we’d be done as $H_q$ would be self-congruent and hence normal in $G$ by the Sylow Theorems. So let us suppose then that $n_q = p$. Then there are $p(q^2 - 1)$ elements of order $q$ or $q^2$ in $G$. If $n_p = q^2$, then $p(q^2 - 1) + q^2(p - 1) + 1 = 2pq^2 - p - q^2 + 1 > pq^2$. So if $n_q = p$, then $n_p \neq q^2$. Similarly, we notice that $n_p \neq q$. Thus, $n_p = 1$ and $H_p$ is normal in $G$.

So $G$ has a proper normal subgroup. $\square$
**Problem 3.** Express $x_1^3 + \cdots + x_n^3$ in terms of the elementary symmetric polynomials in $x_1, \ldots, x_n$.

---

**Proof.** The elementary symmetric polynomials in $n$ variables are

\[
\begin{align*}
e_1 &= x_1 + x_2 + \cdots + x_n \\
e_2 &= \sum_{i \neq j}^{n} x_i x_j \\
e_3 &= \sum_{i \neq j \neq k}^{n} x_i x_j x_k.
\end{align*}
\]

Now we will show by induction that $x_1^3 + x_2^3 + \cdots + x_n^3 = e_1^3 - 3e_1e_2 + 3e_3$.

**base case:** $n = 2$

Notice that when $n = 2$, $e_3 = 0$.
\[
e_1^3 - 3e_1e_2 + 3e_3 &= (x_1 + x_2)^3 - 3(x_1 + x_2)(x_1x_2) + 3 \cdot 0 \\
&= x_1^3 + 3x_1^2x_2 + 3x_1x_2^2 + x_2^3 - 3(x_1^2x_2 + x_1x_2^2) \\
&= x_1^3 + 3x_1^2x_2 + 3x_1x_2^2 + x_2^3 - 3x_1^2x_2 - 3x_1x_2^2 \\
&= x_1^3 + x_2^3.
\]

**inductive step:** Assume that
\[
x_1^3 + x_2^3 + \cdots + x_k^3 = e_1^3 - 3e_1e_2 + 3e_3
\]
holds when $e_1, e_2,$ and $e_3$ are the elementary symmetric polynomials in $k$ variables. We want to show it holds for when $n = k + 1$.

\[
(x_1 + \cdots + x_k + x_{k+1})^3 - 3(x_1 + \cdots + x_k + x_{k+1})(x_1x_2 + \cdots + x_kx_{k+1}) + 3(x_1x_2x_3 + \cdots + x_{k-1}x_kx_{k+1}) \\
= (e_1 + x_{k+1})^3 - 3(e_1 + x_{k+1})(e_2 + e_1x_{k+1}) - 3(e_3 + e_2x_{k+1}) \\
= e_1^3 + 3e_1^2x_{k+1} + 3e_1x_{k+1}^2 + x_{k+1}^3 - 3e_1e_2 - 3e_1^2x_{k+1} - 3e_2x_{k+1} - 3e_1x_{k+1}^2 + 3e_3 + 3e_2x_{k+1} \\
= (e_1^3 - 3e_1e_2 + 3e_3) + 3e_1^2x_{k+1} - 3e_1^2x_{k+1} + 3e_1x_{k+1}^2 - 3e_1x_{k+1}^2 + x_{k+1}^3 + 3e_2x_{k+1} - 3e_2x_{k+1} + 3e_2x_{k+1} \\
= x_1^3 + \cdots + x_k^3 + x_{k+1}^3.
\]
Since \( x_1 + \cdots x_k + x_{k+1} \), \( x_1x_2 + \cdots + x_kx_{k+1} \), and \( x_1x_2x_3 + \cdots x_{k-1}x_kx_{k+1} \) are just the elementary symmetric polynomials in \( k + 1 \) variables, we have shown that

\[
x_1^3 + \cdots + x_k^3 + x_{k+1}^3 = e_1^3 - 3e_1e_2 + 3e_3
\]

where \( e_1, e_2, \) and \( e_3 \) are the first three elementary symmetric polynomials in \( k + 1 \) variables.

Thus, by the Principle of Mathematical Induction, \( x_1^3 + \cdots + x_n^3 \) can be expressed in terms of elementary symmetric polynomials.
Problem 4. Show that a finite abelian group of linear operators on a finite-dimensional complex vector space has simultaneous eigenvectors forming a basis.

Proof. Let $A = \{A_i\}_{i=1}^n$ be a finite abelian group of linear operators on a finite-dimensional complex vector space, $V$. $A$ is a group, therefore, for any $i$,

$$A_i^n = I \implies A_i^n - I = 0.$$ 

Let $f_i(x)$ denote the minimum polynomial of $A_i$. $f_i(x)$ must divide $x^n - 1$. Because $V$ is a complex vector space, and $\mathbb{C}$ is algebraically closed, $x^n - 1$ splits completely into distinct roots in $\mathbb{C}$. Therefore, $f_i(x)$ splits completely into distinct linear factors for every $i$. Thus, for every $i$, $A_i$ is diagonalizable on $V$.

We will prove the statement by induction.

**base case:** As $n = 1$ is trivial, consider $n = 2$. Let $A = \{A_1, A_2\}$, where $A_1$ and $A_2$ are diagonalizable on $V$ and $A$ is abelian. $A_1$ is diagonalizable on $V$ and so there exists a basis for $V$ made up of eigenvectors of $A_1$. That is, $V$ can be decomposed as

$$V = \sum_{\text{eigenvalues } \lambda \text{ of } A_1} V_\lambda,$$

where $V_\lambda = \{v \in V \mid A_1v = \lambda v\}$, the $\lambda$-eigenspace. For every $\lambda$, an eigenvalue of $A_1$, and any $v \in V_\lambda$, since $A$ is abelian,

$$A_1(A_2v) = A_1A_2v = A_2A_1v = A_2\lambda v = \lambda A_2v = \lambda(A_2v).$$

So $A_2$ stabilizes $V_\lambda$, for every $\lambda$. That is, $A_2$ maps vectors from $V_\lambda$ to vectors in $V_\lambda$. So, $A_2$ is a linear operator on each $V_\lambda$.

$f_2(x)$ denotes the minimum polynomial of $A_2$ on $V$. Let $f_{2,\lambda}(x)$ denote the minimum polynomial of $A_2$ on $V_\lambda$. We know that $f_{2,\lambda}(x)$ must divide $f_2(x)$. Since $f_2(x)$ splits into distinct linear factors since $A_2$ is diagonalizable on $V$, $f_{2,\lambda}(x)$ must also split into distinct linear factors. Thus, $A_2$ is diagonalizable on $V_\lambda$ for every $\lambda$. Thus, there is a basis for $V_\lambda$ that is made up of eigenvectors of $A_2$ which are $\lambda$-eigenvectors for $A_1$.

Since

$$V = \sum_{\text{eigenvalues } \lambda \text{ of } A_1} V_\lambda,$$

this implies that $V$ has a basis of simultaneous eigenvectors for $A_1$ and $A_2$. 
inductive step: Assume that $A_1, \ldots, A_k$ have simultaneous eigenvectors forming a basis for $V$. So we can write

$$V = \sum_{\text{eigenvalues } \lambda_1, \ldots, \lambda_k} V_{\lambda_1, \ldots, \lambda_k}$$

where $V_{\lambda_1, \ldots, \lambda_k} = \{ v \in V \mid A_1 v = \lambda_1 v, \ldots, A_k v = \lambda_k v \}$.

Let us examine $A_{k+1}$. Let $v \in V_{\lambda_1, \ldots, \lambda_k}, i \in \{1, \ldots, k\}$. Since $A$ is abelian,

$$A_i(A_{k+1})v = A_iA_{k+1}v = A_{k+1}A_i v = A_{k+1}\lambda_i v = \lambda_i A_{k+1}v = \lambda_i(A_{k+1}v).$$

So $A_{k+1}$ stabilizes $V_{\lambda_1, \ldots, \lambda_k}$ for every vector space $V_{\lambda_1, \ldots, \lambda_k}$. Then, $A_{k+1}$ is a linear operator on each $V_{\lambda_1, \ldots, \lambda_k}$.

$f_{k+1}(x)$ denotes the minimum polynomial of $A_{k+1}$ on $V$. Let $f_{k+1,\lambda_1,\ldots,\lambda_k}(x)$ denote the minimum polynomial of $A_{k+1}$ on $V_{\lambda_1, \ldots, \lambda_k}$. We know that $f_{k+1,\lambda_1,\ldots,\lambda_k}(x)$ must divide $f_{k+1}(x)$, which has distinct roots since $A_{k+1}$ is diagonalizable on $V$. Thus, $f_{k+1,\lambda_1,\ldots,\lambda_k}(x)$ has distinct roots and hence $A_{k+1}$ is diagonalizable on each $V_{\lambda_1, \ldots, \lambda_k}$. Thus there is a basis for $V_{\lambda_1, \ldots, \lambda_k}$ that is made up of eigenvectors of $A_{k+1}$ which are in $V_{\lambda_1, \ldots, \lambda_k}$ and are hence eigenvectors for $A_1, \ldots, A_k$.

Since

$$V = \sum_{\text{eigenvalues } \lambda_1, \ldots, \lambda_k} V_{\lambda_1, \ldots, \lambda_k},$$

$V$ has a basis of simultaneous eigenvectors for $A_1, \ldots, A_k, A_{k+1}$.

Thus, by the Principle of Mathematical Induction, a finite abelian group of linear operators on a finite dimensional complex vector space has simultaneous eigenvectors forming a basis. \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 principal ideal domain and hence a unique factorization domain. Thus, all irreducible elements are prime in \( (\mathbb{Z}/13\mathbb{Z})[x] \). Since any prime ideal is maximal in a principal ideal domain, 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. Prove that the tenth cyclotomic polynomial
\[
\Phi_{10}(x) = \frac{(x^{10} - 1)(x - 1)}{(x^5 - 1)(x^2 - 1)} = x^4 - x^3 + x^2 - x + 1
\]
is irreducible in \(\mathbb{F}_3[x]\), where \(\mathbb{F}_3\) is the finite field with 3 elements.

Proof. To show that \(\Phi_{10}(x)\) is irreducible in \(\mathbb{F}_3[x]\), it suffices to show that \(\Phi_{10}(x)\) has no linear or quadratic factors.

First note that the roots of \(\Phi_{10}(x)\) are the primitive 10\(^{th}\) roots of unity. That is, if \(\Phi_{10}(\alpha) = 0\), then \(\alpha^{10} = 1\) and \(\alpha^n \neq 1\) holds \(\forall n < 10\).

Since \(|\mathbb{F}_3^\times| = 2\), we see that it holds no elements of order 10. Thus \(\Phi_{10}(x)\) has no linear factors.

If \(\Phi_{10}(x)\) were to have a quadratic factor, its root would lie in \(\mathbb{F}_3^\times\)^2. Notice that \(|\mathbb{F}_3^\times|^2 = 8\), and so \(\mathbb{F}_3^\times\)^2 contains no elements of order 10. Thus, \(\Phi_{10}(x)\) has no quadratic factors.

Thus \(\Phi_{10}(x)\) has no linear or quadratic factors and is therefore irreducible in \(\mathbb{F}_3[x]\). \(\square\)