1. Show that a subgroup $H$ of a finite group $G$ of index $[G : H] = 2$ is necessarily normal.

Proof. It suffices to show that $\forall g \in G, gH = Hg$ or equivalently $gHg^{-1} = H$. Consider separately $g \in H$ and $g \in G - H$. If $g \in H$ then $g^{-1} \in H$ and $gHg^{-1} = Hg^{-1} = H$ since $H$ is a subgroup. Else, $g \in G - H$. Since $[G : H] = 2$ by assumption, exactly 2 cosets of $H$ partition $G$:

$$G = gH \sqcup H = (G - H) \sqcup H = Hg \sqcup H$$

Thus, $gH = Hg$, and $H$ is normal in $G$. \qed

2. Exhibit (and prove non-isomorphism of) two not-mutually-isomorphic non-abelian groups of order $3^2$.

Proof. First, construct a non-abelian group of order $3^3$. Let $N = \mathbb{Z}/3 \oplus \mathbb{Z}/3 = \langle a, b \rangle$ and $K = \mathbb{Z}/3 = \langle y \rangle$. If $\varphi : K \to \text{Aut}(N)$ is non-trivial, then $H = N \rtimes_\varphi K$ is a non-abelian group of order $3^3$. Since the automorphisms of $N$ are exactly the $2$-by-$2$ invertible linear transformations over $\mathbb{F}_3$,

$$|\text{Aut}(N)| = |\text{GL}_2(\mathbb{F}_3)| = (3^2 - 1) \cdot (3^2 - 3) = 48$$

By Cauchy’s Theorem, $\text{Aut}(N)$ has an element of order $3$ such as $\sigma(a, b) = (a, ab)$. Let $\varphi : K \to \text{Aut}(N)$ be the homomorphism given by $\varphi(y) = \sigma$. Since $\sigma$ is not the identity, $\varphi$ is non-trivial; thus $H = N \rtimes_\varphi K = \langle a, b, y \mid a^3 = b^3 = y^3 = 1, yab^{-1} = a, yby^{-1} = ab \rangle$ is non-abelian of order $3^3$. Now consider $G_1 = H \times (\mathbb{Z}/3 \oplus \mathbb{Z}/3)$ and $G_2 = H \times \mathbb{Z}/9$. Since $H$ is non-abelian, both groups are non-abelian of order $3^3 \cdot 3^2 = 3^5$. Further, $G_1 \nsim G_2$ since all non-identity elements in $G_1$ have order $3$, but $(a, b, y, 1) \in G_2$ has order $9$. \qed

3. Count the conjugacy classes in the group $\text{GL}_2(\mathbb{F}_4)$ of multiplicatively invertible $2$-by-$2$ matrices over the field with $4$ elements.

Proof. $\text{GL}_2(\mathbb{F}_4)$ is the group of invertible $k$-linear endomorphisms of the $\mathbb{F}_4$-vector space $\mathbb{F}_4^2$, and conjugacy classes of endomorphisms are in bijection with the $\mathbb{F}_4[x]$-module structures on $\mathbb{F}_4^2$. By the Structure Theorem, each module structure is isomorphic to

$$\frac{\mathbb{F}_4[x]}{(d_1)} \oplus \frac{\mathbb{F}_4[x]}{(d_2)} \oplus \cdots \oplus \frac{\mathbb{F}_4[x]}{(d_n)}$$

where $d_1 | d_2 | \ldots | d_n$ are monic polynomials whose degrees sum to the dimension of the vector space $\mathbb{F}_4^2$, namely $2$. To count the conjugacy classes, it suffices to count polynomials in the following list of irredundant representatives:

$$\frac{\mathbb{F}_4[x]}{(x^2 + ax + b)} \quad a \in \mathbb{F}_4, b \in \mathbb{F}_4^2$$

$$\frac{\mathbb{F}_4[x]}{(x - c)} \oplus \frac{\mathbb{F}_4[x]}{(x - c)} \quad c \in \mathbb{F}_4^2$$

Thus, there are $4 \cdot 3 + 3 = 15$ conjugacy classes in $\text{GL}_2(\mathbb{F}_4)$. \qed
4. Prove that the nilpotent elements in a commutative ring is an ideal.

**Proof.** Let \((R, +, \cdot)\) be a commutative ring and \(I \subseteq R\) the nilpotent elements. It suffices to show \((I, +)\) is an additive subgroup and \(\forall r \in R\) and \(\forall x \in I\), we have \(r \cdot x \in I\) and \(x \cdot r \in I\). Clearly \(0 \in I\), and \(\forall x \in I\) with \(x^n = 0\),
\[
(-x)^m = (-1)^m \cdot x^m = (-1)^m \cdot 0 = 0
\]
Thus, \(-x \in I\). Consider arbitrary \(x, y \in I\). Since \(x, y\) are nilpotent, there are positive integers \(m, n\) such that \(x^n = y^m = 0\). By the Binomial Theorem,
\[
(x + y)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} x^k \cdot y^{n+m-k}
\]
Continuing our equality,
\[
= \sum_{k=0}^{n-1} \binom{n+m}{k} x^k \cdot y^{n+m-k} + \sum_{k=n}^{n+m} \binom{n+m}{k} x^k \cdot y^{n+m-k}
\]
For the first sum \(n + m - k > m\), so for each term,
\[
y^{n+m-k} = y^m \cdot y^{n-k} = 0 \cdot y^{n-k} = 0
\]
Similarly for the second sum \(k \geq n\), so for each term,
\[
x^k = x^n \cdot x^{k-n} = 0 \cdot x^{k-n} = 0
\]
Continuing our equality,
\[
(x + y)^{n+m} = \sum_{k=0}^{n-1} \binom{n+m}{k} x^k \cdot y^{n+m-k} + \sum_{k=n}^{n+m} \binom{n+m}{k} x^k \cdot y^{n+m-k}
\]
Thus, \((I, +)\) is an additive subgroup. Finally, consider any \(x \in I\) (with \(x^n = 0\)) and \(r \in R\). Since \(R\) is commutative, we have
\[
(rx)^m = rx \cdot rx \cdot ... \cdot rx = r^m \cdot x^m = r^m \cdot 0 = 0
\]
Thus, \(r \cdot x = x \cdot r \in I\), so \(I\) is an ideal. \(\square\)

5. Let \(A\) be an abelian group of linear operators on a finite-dimensional complex vector space. Show that there is a (non-zero) simultaneous eigenvector for all \(T \in A\).

**Proof.** Let \(V\) be a finite-dimensional complex vector space. First treat two commuting operators \(A_1, A_2\). Since \(A_1 \in \text{End}_C(V)\), it has a minimum polynomial \(f_1 \in \mathbb{C}[x]\) whose roots are eigenvalues of \(A_1\). By algebraic closedness of \(\mathbb{C}\), \(f_1\) has such a root \(\lambda \in \mathbb{C}\). Let \(V_\lambda = \{v \in V \mid A_1 v = \lambda v\}\) be the \(\lambda\)-eigenspace of \(A_1\). Since \(A\) is abelian, for \(v \in V_\lambda\)
\[
A_1(A_2v) = (A_1A_2)v = (A_2A_1)v = A_2(A_1v) = A_2(\lambda v) = \lambda(A_2v)
\]
Thus, \(V_\lambda\) is \(A_2\)-stable, and \(A_2\) is a linear operator on \(V_\lambda\). Let \(f_2 \in \mathbb{C}[x]\) be the minimum polynomial of \(A_2\) on \(V\) and \(f_{2,\lambda} \in \mathbb{C}[x]\) its minimum polynomial on \(V_\lambda\). By algebraic closedness of \(\mathbb{C}\), \(f_{2,\lambda}\) has a root \(\gamma \in \mathbb{C}\) which is an eigenvalue of \(A_2\) with non-zero eigenvector \(w \in V_\lambda\). Since \(w\) is also an eigenvector of \(A_1\), it is a simultaneous eigenvector of \(A_1, A_2\).

Next consider finitely many operators \(A_1, ..., A_n, A_{n+1}\), and let \(V_\lambda\) be the (non-zero) common eigenspace for \(A_1, ..., A_n\). For all \(v \in V_\lambda\) and \(i \in \{1, ..., n\}\), we have
\[
A_i(A_{n+1}v) = (A_iA_{n+1})v = (A_{n+1}A_i)v = A_{n+1}(A_i v) = A_{n+1}(\lambda v) = \lambda(A_{n+1}v)
\]
Thus, \(V_\lambda\) is \(A_{n+1}\)-stable, and \(A_{n+1}\) is a linear operator on \(V_\lambda\). Let \(g_\lambda \in \mathbb{C}[x]\) be the minimum polynomial of \(A_{n+1}\) on \(V\) and \(g_{\lambda\lambda} \in \mathbb{C}[x]\) its minimum polynomial on \(V_\lambda\). By algebraic closedness of \(\mathbb{C}\), \(g_{\lambda\lambda}\) has a
7. Give a prescription for a formula for an isomorphism.

6. Show that \( B \) eigenvectors for a subset \( B \) of a non-zero subspace of simultaneous eigenvectors \( V \). Since \( y \) divides a non-zero subspace of simultaneous eigenvectors \( V \). Thus, \( B_2 = B_1 \cup T \) has a non-zero subspace of simultaneous eigenvectors \( V_2 \subseteq V_1 \). If all operators in \( A - B_2 \) act by scalars on \( V_2 \), we are done; else, we construct a non-zero subspace of simultaneous eigenvectors \( V_3 \subseteq V_2 \) by an identical argument and try again. We claim that after finitely many iterations, all operators in \( A \) act by scalars on the non-zero subspace \( V_k \). Notice that each iteration decreases the dimension of the common non-zero eigenspace:

\[
\phi \subseteq \ldots \subseteq V_2 \subseteq V_1 \subseteq V
\]

It suffices to show that \( y \) is a unique factorization domain. Thus, there is an irreducible, non-unit root \( \gamma \) such that at least one \( v \in V_1 \) is not its eigenvector. Since \( T \) commutes with all operators in \( B_1 \), \( T \) stabilizes \( V_1 \). As argued above, the minimum polynomial of \( T \) on \( V_1 \) has a root, so \( T \) shares an eigenvector with all operators in \( B_1 \).

Proof. Let \( m, n > 1 \) and define

\[
m' = \frac{m}{\gcd(m, n)} \quad n' = \frac{n}{\gcd(m, n)}
\]

Since \( Z \) is a unique factorization domain and \( \gcd(m, n) \in Z \), there are integers \( r, s \) such that \( sn + rm = \gcd(m, n) \). Next let

\[
\varphi : Z/m \oplus Z/n \to Z/\gcd(m, n) \oplus Z/\lcm(m, n)
\]

We will show \( \varphi \) is well-defined. Observe that \( \forall k, \ell \in Z \),

\[
\varphi(a + km, b + \ell n) = (a + km - (b + \ell n), (a + km)sn' + (b + \ell n)rm') = (a - b + (km - \ell n), asn' + brm' + (kmsn' + \ell nr'm'))
\]

\[
= (a - b, asn' + brm' + \frac{kms + \ell nrm}{\gcd(m, n)})
\]

\[
= (a - b, asn' + brm' + \frac{mn(ks + \ell r)}{\gcd(m, n)})
\]

\[
= (a - b, asn' + brm' + \lcm(m, n)(ks + \ell r))
\]

\[
= (a - b, asn' + brm')
\]

Finally, consider \( A \) of infinite order. Let \( V_1 \subseteq V \) be the non-zero subspace of simultaneous eigenvectors for a subset \( B_1 \subseteq A \). If all operators in \( A - B_1 \) act by scalars on \( V_1 \), we are done. Else, let \( T_1 \in A - B_1 \) such that at least one \( v \in V_1 \) is not its eigenvector. Since \( T_1 \) commutes with all operators in \( B_1 \), \( T_1 \) stabilizes \( V_1 \). As argued above, the minimum polynomial of \( T_1 \) on \( V_1 \) has a root, so \( T_1 \) shares an eigenvector with all operators in \( B_1 \). Thus, \( B_2 = B_1 \cup T_1 \) has a non-zero subspace of simultaneous eigenvectors \( V_2 \subseteq V_1 \). If all operators in \( A - B_2 \) act by scalars on \( V_2 \), we are done; else, we construct a non-zero subspace of simultaneous eigenvectors \( V_3 \subseteq V_2 \) by an identical argument and try again. We claim that after finitely many iterations, all operators in \( A \) act by scalars on the non-zero subspace \( V_k \). Notice that each iteration decreases the dimension of the common non-zero eigenspace:

\[
\phi \subseteq \ldots \subseteq V_2 \subseteq V_1 \subseteq V
\]

Since \( V \) is finite-dimensional, only finitely many iterations are possible. Let \( k \) denote the number of iterations. By construction, \( V_k \) is a non-zero common eigenspace for some \( B_k \subseteq A \), and by choice of \( k \), all operators in \( A - B_k \) act by scalars on \( V_k \). Thus, \( V_k \) is a non-zero subspace of simultaneous eigenvectors for all operators in \( A \), and any \( v \in V_k \) is a simultaneous eigenvector. 

7. Give a prescription for a formula for an isomorphism \( \mathbb{Z}/m \oplus \mathbb{Z}/n \to \mathbb{Z}/\gcd(m, n) \oplus \mathbb{Z}/\lcm(m, n) \) for integers \( m, n > 1 \).

Proof. We shall prove irreducibility using Eisenstein’s criterion. First identify

\[
\mathbb{C}[x, y] \cong \mathbb{C}[y][x]
\]

via the natural isomorphism where \( x^7 + y^7 + 2 \) is a degree 7 polynomial in \( x \) with constant term \( y^7 + 2 \). It suffices to show that \( y^7 + 2 \) is divisible by some prime \( p \in \mathbb{C}[y] \) but not by \( p^2 \). Since \( \mathbb{C} \) is a field, \( \mathbb{C}[y] \) is a unique factorization domain. Thus, there is an irreducible, non-unit \( p \in \mathbb{C}[y] \) such that \( p \) divides \( y^7 + 2 \). Assume \( p^2 \) divides \( y^7 + 2 \). Then, \( p \) divides \( \frac{dy}{dx}[y^7 + 2] = 7y^6 \) which means \( p \) divides \( y^7 + 2 - \frac{7}{y} \cdot (7y^6) = 2 \). Since 2 is a unit in \( \mathbb{C}[y] \) and \( p \) is not a unit by assumption, \( p^2 \) does not divide \( y^7 + 2 \). By Eisenstein’s criterion, \( x^7 + y^7 + 2 \) is irreducible in \( \mathbb{C}[y][x] \). 

\[
\varphi(a, b) = (a - b, asn' + brm')
\]

We will show \( \varphi \) is well-defined. Observe that \( \forall k, \ell \in Z \),

\[
\varphi(a + km, b + \ell n) = (a + km - (b + \ell n), (a + km)sn' + (b + \ell n)rm')
\]

\[
= (a - b + (km - \ell n), asn' + brm' + (kmsn' + \ell nr'm'))
\]

\[
= (a - b, asn' + brm' + \frac{kms + \ell nrm}{\gcd(m, n)})
\]

\[
= (a - b, asn' + brm' + \frac{mn(ks + \ell r)}{\gcd(m, n)})
\]

\[
= (a - b, asn' + brm' + \lcm(m, n)(ks + \ell r))
\]

\[
= (a - b, asn' + brm')
\]
Thus, $\varphi$ does not depend on our choice of representatives of $\mathbb{Z}/m$ and $\mathbb{Z}/n$ and is therefore well-defined. Next we will show $\varphi$ is injective. Assume $\varphi(a, b) = (0, 0) \in \mathbb{Z}/\gcd(m, n) \oplus \mathbb{Z}/\lcm(m, n)$. By construction of $\varphi$, there is an integer $k$ such that $a = k \gcd(m, n) + b$. Thus,

$$0 \equiv asn' + brm'$$

$$\equiv (k \cdot \gcd(m, n) + b)sn' + brm'$$

$$\equiv ksn' \cdot \gcd(m, n) + b(sn' + rm')$$

$$\equiv ksn' \cdot \gcd(m, n) + b$$

$$\equiv ksn + b$$

$$\equiv b \mod n$$

By a similar argument, there is an integer $\ell$ such that $0 \equiv \ell rm + a \equiv a \mod m$. Therefore, $a = b = 0$ when $\varphi(a, b) = (0, 0)$, so $\varphi$ is injective. Clearly $\varphi$ is surjective since

$$|\mathbb{Z}/m \oplus \mathbb{Z}/n| = m \cdot n = \gcd(m, n) \cdot \lcm(m, n) = |\mathbb{Z}/\gcd(m, n) \oplus \mathbb{Z}/\lcm(m, n)|$$

by properties of direct sums of cyclic groups, so $\varphi$ is an isomorphism. \qed

8. Explicitly determine all fields between $\mathbb{Q}$ and $\mathbb{Q}(\zeta)$, where $\zeta$ is a primitive $12^{th}$ root of unity.

Proof. Since $\mathbb{Q}(\zeta)$ is a cyclotomic field, it is certainly separable, splitting, and hence Galois. By the Fundamental Theorem of Galois Theory, intermediate fields of $\mathbb{Q}(\zeta)/\mathbb{Q}$ are in one-to-one correspondence with the (proper) subgroups of $G = \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Thus, we proceed to identify the Galois group, its proper subgroups, and the corresponding field extensions.

The Galois group $G$ consists of the automorphisms of $\mathbb{Q}(\zeta)$ which fix $\mathbb{Q}$ and permute the primitive $12^{th}$ roots of unity. Since 1, 5, 7, and 11 are relatively prime to 12, the primitive $12^{th}$ roots of unity are $\zeta$, $\zeta^5$, $\zeta^7$, and $\zeta^{11}$ where $\zeta = e^{\pi i/12}$. Since there are 4 primitive $12^{th}$ roots of unity, there are exactly 4 such automorphisms in the Galois group (whose action on $\mathbb{Q}(\zeta)$ is completely determined by $\zeta$ since all roots of unity are multiples):

$$\sigma_1(\zeta) = \zeta \quad \sigma_5(\zeta) = \zeta^5 \quad \sigma_7(\zeta) = \zeta^7 \quad \sigma_{11}(\zeta) = \zeta^{11}$$

Thus, $G = \{\sigma_1, \sigma_5, \sigma_7, \sigma_{11}\}$.

Next we identify the subgroups of $G$ and the corresponding fixed fields. By Lagrange, any proper subgroup will have order 2, and since 2 is prime, it will be cyclic. Consider the subgroup generated by each element in $G$:

$$\langle \sigma_1 \rangle = G \quad \langle \sigma_5 \rangle = \{\sigma_1, \sigma_5\} \quad \langle \sigma_7 \rangle = \{\sigma_1, \sigma_7\} \quad \langle \sigma_{11} \rangle = \{\sigma_1, \sigma_{11}\}$$

By inspection, the only proper subgroups of $G$ are $\langle \sigma_5 \rangle$, $\langle \sigma_7 \rangle$, and $\langle \sigma_{11} \rangle$. Since $\sigma_5$ fixes $\zeta^n$ if and only if $5n \equiv n \mod 12$ (or equivalently, $n \equiv 0 \mod 3$), $\sigma_5$ fixes $\zeta^3, \zeta^6$, and $\zeta^9$ where $\zeta^3 = e^{\pi i/2} = i \notin \mathbb{Q}$. Thus, the fixed field of $\langle \sigma_5 \rangle$ is $\mathbb{Q}(\zeta^3) = \mathbb{Q}(i)$. Similarly, $\sigma_7$ fixes $\zeta^n$ if and only if $7n \equiv n \mod 12$ (or equivalently, $n \equiv 0 \mod 2$). Since $\zeta^2 = 1/2 + i\sqrt{3}/2, 1/2 \in \mathbb{Q}$, and $i\sqrt{3} \notin \mathbb{Q}$, the fixed field of $\langle \sigma_7 \rangle$ is $\mathbb{Q}(\zeta^2) = \mathbb{Q}(i\sqrt{3})$. Now, $\sigma_{11}$ fixes $\zeta^n$ if and only if $11n \equiv n \mod 12$ (or equivalently, $5n \equiv 0 \mod 6$), but $\zeta^6 = -1 \in \mathbb{Q}$, so consider linear combinations of primitive roots. Observe that

$$\sigma_{11}(\zeta + \zeta^{11}) = \sigma_{11}(\zeta) + \sigma_{11}(\zeta^{11}) = \zeta^{11} + \zeta$$

Thus, $\sigma_{11}$ fixes $\zeta + \zeta^{11} = \sqrt{3} \notin \mathbb{Q}$, and the fixed field of $\langle \sigma_{11} \rangle$ is $\mathbb{Q}(\zeta + \zeta^{11}) = \mathbb{Q}(\sqrt{3})$. By pairing all subgroups of the Galois group, we have identified all fields between $\mathbb{Q}$ and $\mathbb{Q}(\zeta)$. To show these fields are distinct, we check that the generators of the intermediate fields aren’t in smaller fields. Here it suffices to check $i \notin \mathbb{Q}(\sqrt{3})$, so assume there are $a, b \in \mathbb{Q}$ such that $i = a\sqrt{3} + b$. Then,

$$-1 = (a\sqrt{3} + b)^2 = 3a^2 + b^2 + 2ab\sqrt{3}$$

Since $\sqrt{3} \notin \mathbb{Q}$, either $a = 0$ or $b = 0$. If $a = 0$, then $b = \pm i \notin \mathbb{Q}$; otherwise, $b = 0$ and $a = \pm i/\sqrt{3} \notin \mathbb{Q}$. Thus, $i \notin \mathbb{Q}(\sqrt{3})$, and our intermediate fields are distinct. \qed