1. Let $H$ be a subgroup of index 2 in a finite group $G$. Show that $H$ is normal.

Let $g \in G \setminus H$, then the two left cosets of $H$ in $G$ are $1H$ and $gH$. Since $1H = H$, and the cosets partition $G$ we must have that $gH = G \setminus H$. 

Now, the two right cosets of $H$ in $G$ are $H1 = H$ and $Hg'$ for some $g' \in G \setminus H$, thus $Hg' = G \setminus H$ and since $g \in G \setminus H$ implies $Hg' = Hg$, we have that $Hg = G \setminus H = gH$, thus $Hg = gH$, so $H$ is normal in $G$, as required.

2. Let $G$ be the group of invertive 2-by-2 matrices over the field $\mathbb{F}_p$ with $p$ elements, where $p$ is prime. Find a $p$-Sylow subgroup of $G$.

Since $G = \text{GL}_2(\mathbb{F}_p)$, the order of $G$ is $(p^2 - 1)(p^2 - p) = p(p + 1)(p^2 - 1)^2$. So a Sylow-$p$ subgroup of $G$ will be of order $p$. Let

$$H_p = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in \mathbb{F}_p \right\}$$

be a subgroup of $G$ of order $p$ since

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x + y \\ 0 & 1 \end{pmatrix} \in H_p.$$

Obviously, $H_p$ is closed under inverses since

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix}.$$

Also, we can notice that

$$H_p = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle.$$
3. Prove that the polynomial $x^5 + y^5 + z^5$ is irreducible in $\mathbb{C}[x,y,z]$.

First notice that

$$x^5 + y^5 + z^5 = (x^5 + y^5) + z^5 \in \mathbb{C}[x,y,z] \subset \mathbb{C}(x)[y] \subset \mathbb{C}(x,y)[z].$$

Now, we want to be able to use Eisenstein’s Criterion. Since $\mathbb{C}(x)[y]$ is a unique factorization domain, there exists some $p(y) \in \mathbb{C}(x)[y]$, which is irreducible such that $p(y)$ divides $x^5 + y^5$ and is not a unit, therefore the degree of $p(y)$ is at least one.

Now, we need to show that $(p(y))^2$ does not divide $x^5 + y^5$, this is equivalent to showing that $p(y)$ does not divide $\frac{\partial}{\partial y}[x^5 + y^5] = 5y^4$. Since $\mathbb{C}(x)[y]$ is an Euclidean domain, we can write

$$x^5 + y^5 = \frac{1}{5} y (5y^4) + x^5,$$

where $x^5$ is a unit in $\mathbb{C}(x)[y]$ since $\mathbb{C}(x)$ is a field.

From this we see that the greatest common divisor of $x^5 + y^5$ and $5y^4$ is a unit. Now since $p(y)$ is not a unit, and $p(y)$ does divide $x^5 + y^5$, it must be that $p(y)$ does not divide $5y^4$.

Thus, $(p(y))^2$ does not divide $x^5 + y^5$. Also, $p(y)$ does not divide 1, which is the coefficient of $z^5$ in $x^5 + y^5 + z^5 \in \mathbb{C}(x)[y][z]$.

Thus, by Eisenstein’s Criterion, $x^5 + y^5 + z^5$ is irreducible in $\mathbb{C}(x)[y,z]$, therefore it is irreducible in $\mathbb{C}[x,y,z]$, as required.

4. For distinct elements $a_1, ..., a_n$ of a field $k$, show that there exist $A_1, ..., A_n$ such that

$$\frac{1}{(x - a_1) \cdots (x - a_n)} = \frac{A_1}{x - a_1} + \cdots + \frac{A_n}{x - a_n}$$

This is equivalent to proving

$$1 = \sum_{i=1}^{n} A_i \prod_{j=1, j \neq i}^{n} (x - a_j).$$

Note that $(x - a_1), ..., (x - a_n)$ are all pairwise relatively prime. Now, since $k[x]$ is an Euclidean domain, there exist polynomials $P_1(x), ..., P_n(x)$ such that

$$1 = \sum_{i}^{n} P_i(x) \prod_{j \neq i} (x - a_j).$$

NEXT: Show that each $P_i(x)$ is constant.

5. Let $X, Y$ be $n$-by-$n$ complex matrices such that $XY = YX$. Suppose that there are $n$-by-$n$ invertible matrices $A, B$ such that $AXA^{-1}$ and $BYB^{-1}$ are diagonal. Show that there is an $n$-by-$n$ invertible matrix $C$ so that $CXC^{-1}$ and $CYC^{-1}$ are diagonal.
6. Describe all intermediate fields between \( \mathbb{Q} \) and \( \mathbb{Q}(\zeta_9) \), where \( \zeta_9 \) is a primitive ninth root of unity.

First, notice that \( [\mathbb{Q}(\zeta_9) : \mathbb{Q}] = \varphi(9) = 6 \), where \( \varphi \) is Euler’s phi function.

Now, recall that all cyclotomic extensions of \( \mathbb{Q} \) are Galois. So

\[
\text{Gal}(\mathbb{Q}(\zeta_9)/\mathbb{Q}) = (\mathbb{Z}_9)^* \cong \mathbb{Z}_6.
\]

Well, \( \mathbb{Z}_6 \) has two subgroups, one of order 3 and one of order 2, and by the fundamental theorem of Galois theory, these subgroups correspond with the intermediate fields between \( \mathbb{Q} \) and \( \mathbb{Q}(\zeta_9) \).

Now, let \( \sigma_a : \zeta_9 \mapsto \zeta_9^a \), where \( \gcd(9,a) = 1 \) and \( a < 9 \). So \( \text{Gal}(\mathbb{Q}(\zeta_9)/\mathbb{Q}) \cong \langle \sigma_2 \rangle \) since \( \langle \sigma_2 \rangle = \{\sigma_2, \sigma_4, \sigma_8, \sigma_7, \sigma_5, \text{id} \} \) is a cyclic group of order 6, thus isomorphic to \( \mathbb{Z}_6 \).

We can see now that \( \langle \sigma_4 \rangle = \{\sigma_4, \sigma_7, \text{id} \} \cong \mathbb{Z}_3 \) is the subgroup of order 3. Similarly, \( \langle \sigma_8 \rangle = \{\sigma_8, \text{id} \} \cong \mathbb{Z}_2 \) is the subgroup of order 2.

By the Fundamental Theorem of Galois Theory, the subgroups of \( \text{Gal}(\mathbb{Q}(\zeta_9)/\mathbb{Q}) \) correspond to the intermediate fields between \( \mathbb{Q} \) and \( \mathbb{Q}(\zeta_9) \).

Now, we know that \( \zeta_9 \) is the a primitive \( 9^{th} \) root of unity, so \( \zeta_9^3 \) is a primitive cube root of unity, which generates a degree 2 extension over \( \mathbb{Q} \) since

\[
\zeta_9^3 = \zeta_3 = e^{2\pi i/3} = \cos \left( \frac{2\pi}{3} \right) + i \sin \left( \frac{2\pi}{3} \right) = -\frac{1}{2} + i \frac{\sqrt{3}}{2}.
\]

So \( \mathbb{Q}(\sqrt{-3}) \) is an intermediate field, which is fixed by \( \langle \sigma_4 \rangle \) since

\[
\sigma_4(\zeta_9^3) = \zeta_9^{12} = \zeta_9^3 \quad \text{and} \quad \sigma_7(\zeta_9^3) = \zeta_9^{21} = \zeta_9^3.
\]

Now, \( \sigma_8 \) fixes \( \zeta_9 + \zeta_9^8 = \zeta_9 + \zeta_9^{-1} \). So let’s consider the ninth cyclotomic polynomial

\[
\Phi_9(x) = x^6 + x^3 + 1, \quad \text{and we know} \quad \Phi_9(\zeta_9) = \zeta_9^6 + \zeta_9^3 + 1 = 0
\]

so

\[
0 = \zeta_9^{-3} + \zeta_9^3 + 1 = (\zeta_9 + \zeta_9^{-1})^3 - 3(\zeta_9 + \zeta_9^{-1}) + 1
\]

since

\[
(\zeta_9 + \zeta_9^{-1})^3 = \zeta_9^3 + 3\zeta_9^2 + 3\zeta_9 + 3\zeta_9^{-1} + 3 - 3(\zeta_9 + \zeta_9^{-1}) + 1
\]

Therefore, \( \zeta_9 + \zeta_9^8 \) is a root of \( f(x) = x^3 - 3x + 1 \), which is irreducible since \( f(x + 1) = x^3 - 3x^2 + 3 \) is irreducible by Eisenstein’s Criterion with \( p = 3 \).

Thus, \( \mathbb{Q}(\zeta_9 + \zeta_9^8) \) is a degree 3 extension over \( \mathbb{Q} \) generated by the minimal polynomial \( f(x) = x^3 - 3x + 1 \) and fixed by \( \langle \sigma_8 \rangle \).

So the intermediate fields between \( \mathbb{Q} \) and \( \mathbb{Q}(\zeta_9) \) are \( \mathbb{Q}(\sqrt{-3}) \) and \( \mathbb{Q}(\zeta_9 + \zeta_9^8) \), as required. 

7. Show that in $\mathbb{F}_2[x]$, where $\mathbb{F}_2$ is the field with 2 elements, $(x^{31} - 1)/(x - 1)$ is the product of six irreducible quintic factors.

First notice that
\[
\Phi_{31}(x) = \frac{x^{31} - 1}{x - 1}
\]
is the 31st cyclotomic polynomial. Thus, since 2 does not divide 31, if $\alpha$ is a root of $\Phi_{31}(x)$ then $\alpha$ is a primitive 31st root of unity, i.e.
\[
\alpha^{31} = 1 \quad \text{and} \quad \alpha^t \neq 1, \text{ for all } t < 31.
\]

Now, notice that $\mathbb{F}_{2^5}$ is a degree 5 field extension of $\mathbb{F}_2$. Also, $(\mathbb{F}_{2^5})^\times$ is a cyclic group of order $2^5 - 1 = 31$ and is canonically the set of 31st roots of unity. Since $(\mathbb{F}_{2^5})^\times$ is cyclic, there must be some $\beta \in (\mathbb{F}_{2^5})^\times$ of order 31, i.e. $\beta^{31} = 1$ and $\beta^t \neq 1, \forall t < 31$, thus $\beta$ is a root of $\Phi_{31}(x)$. Also, $\beta$ is not in $\mathbb{F}_2, \mathbb{F}_{22}, \mathbb{F}_{23}, \mathbb{F}_{24}$, since none of those fields contain elements of order 31.

So the minimal polynomial of $\beta$ in $\mathbb{F}_2[x]$ is of degree 5, and divides $\Phi_{31}(x)$, i.e. the minimal polynomial of $\beta$ is irreducible and quintic in $\mathbb{F}_2[x]$.

Note that $\{\beta, \beta^2, \beta^3, \ldots, \beta^{30}\} \subset \langle \beta \rangle$ is the set of primitive 31st roots of unity, which lies in $\mathbb{F}_{2^5}$, and since the order of $\beta$ is 31, this set lies only in $\mathbb{F}_{2^5}$ and no lower extension of $\mathbb{F}_2$. So, for every $i = 1, \ldots, 30$, the minimal polynomial of $\beta^i$ is quintic and divides $\Phi_{31}(x)$.

Now, 30 is the degree of $\Phi_{31}(x)$, which is reducible into polynomials of degree 5 in $\mathbb{F}_2[x]$, and $30 = 6 \cdot 5$, so it must be that $\Phi_{31}(x) = (x^{31} - 1)/(x - 1)$ is the product of six irreducible quintic polynomials in $\mathbb{F}_2[x]$, by the pigeonhole principle. 

$\blacksquare$