1. Show that in any group $G$ of order $23 \cdot 24$, the 23-Sylow subgroup is normal.

**Solution**: Write $n_p$ for the number of $p$-Sylow subgroups, $p = 2, 3$ or 23. By the Sylow theorems,

\[
2 \equiv 1 \mod p \quad \text{and} \quad n_p = \left[ G : N_G(G_p) \right] \mid \left[ G : G_p \right],
\]

where $G_p$ is a $p$-Sylow subgroup of $G$.

We wish to show $n_{23} = 1$. By (1), since $\left[ G : G_{23} \right] = 24$, the only other possibility is $n_{23} = 24$, so we argue by contradiction, assuming $n_{23} = 24$. Note that by (1), this implies that

\[
N_G(G_{23}) = G_{23}.
\]

Since $|G_{23}| = 23$ is prime, the intersection of any two distinct 23-Sylow subgroups is the identity. So the number of elements of order 23 is

\[
n_{23}(23 - 1) = 24 \cdot 23 - 24 = |G| - 24
\]

so there are exactly 24 elements whose order is not 23.

Now consider $N_G(G_3)$. If 23 divides the order of $N_G(G_3)$, then $N_G(G_3)$ contains a subgroup $H$ of order 23, in which case $H \cdot G_3$ is a subgroup of $G$ with $G_3 \triangleleft (H \cdot G_3)$. We get

\[
\frac{H}{H \cap G_3} \cong \frac{H \cdot G_3}{G_3}.
\]

Since $H \cap G_3 = e$, $|H \cdot G_3| = 23 \cdot 3$. But any group of order $23 \cdot 3$ has a normal 23-Sylow subgroup, which would give

\[
H \cdot G_3 \subset N_G(H),
\]

contradicting (2). Thus 23 does not divide $N_G(G_3)$.

But then 23 does divide $|G : N_G(G_3)| = n_3$. But this gives at least $23 \cdot 2 = 46$ elements of order 3. Since there are only 24 elements of $G$ of order not 23, this gives the desired contradiction. So $n_{23} = 1$, as desired.

2. Let $F = \mathbb{Q}(\zeta_7)$ with $\zeta_7 = e^{2\pi i/7}$.

(a) What is the Galois group of $F$ over $\mathbb{Q}$?

**Solution**: For any $n$ there is an isomorphism

\[
\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to \text{Aut}(\langle \zeta_n \rangle)
\]

\[
\sigma \mapsto \sigma|_{\langle \zeta_n \rangle},
\]

where $\sigma$ is an automorphism of $\mathbb{Q}(\zeta_n)$.
the restriction of $\sigma$ to the cyclic subgroup $\langle \zeta_n \rangle$ of $\mathbb{Q}(\zeta_n)^\times$ generated by $\zeta_n$. Here $\mathbb{Q}(\zeta_n)^\times$ is the multiplicative group of units of $\mathbb{Q}(\zeta_n)$.

Of course,

$$(4) \quad \text{Aut}(\langle \zeta_n \rangle) \cong \mathbb{Z}_n^\times$$

under the map taking $f \in \text{Aut}(\langle \zeta_n \rangle)$ to the unique element $k \in \mathbb{Z}_n^\times$ with $f(\zeta_n) = \zeta_n^k$. We obtain a composite isomorphism

$$(5) \quad \varepsilon : \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to \mathbb{Z}_n^\times$$

taking $\sigma$ to the unique $\bar{k} \in \mathbb{Z}_n^\times$ with $\sigma(\zeta_n) = \zeta_n^{\bar{k}}$. In particular, for each $k \in \mathbb{Z}$ with $(n, k) = 1$ and $1 \leq k < n$, we can write $\sigma_k$ for the unique element of $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ with $\varepsilon(\sigma_k) = k$. Note that

$$(6) \quad \sigma_k(\zeta_n^\ell) = (\zeta_n^\ell)^k = \zeta_n^{\ell k}.$$ 

Now note that $\mathbb{Z}_7^\times$ is cyclic of order 6, generated by 3.

(b) Find all intermediate fields between $\mathbb{Q}$ and $F$. (Write each in the form $\mathbb{Q}(\alpha)$ for some specific $\alpha \in F$.)

**Solution:** The inverted lattice of subgroups of $\mathbb{Z}_7^\times$ is

$$\begin{array}{c}
\varepsilon \\
(2) \\
\varepsilon \\
(6)
\end{array}$$

$$\mathbb{Z}_7^\times.$$ 

Here, $\bar{2}$ has order 3 and $\bar{6}$ has order 2. Recalling the definition of $\sigma_k$ from part (a) (see (6)), the lattice of subfields of $\text{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q})$ is given by

$$\begin{array}{ccc}
\mathbb{Q}(\zeta_7) & & \mathbb{Q}(\zeta_7)^{\sigma^2} \\
\mathbb{Q}(\zeta_7)^{\sigma^2} & & \mathbb{Q}(\zeta_7)^{\sigma^6} \\
\mathbb{Q} & & \mathbb{Q},
\end{array}$$

where $\mathbb{Q}(\zeta_7)^\sigma$ consists of the elements of $\mathbb{Q}(\zeta_7)$ fixed by $\sigma$. Since $\text{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q}(\zeta_7)^\sigma) = \langle \sigma \rangle$, $[\mathbb{Q}(\zeta_7) : \mathbb{Q}(\zeta_7)^\sigma] = |\sigma|$, the order of $\sigma$, and hence $[\mathbb{Q}(\zeta_7)^\sigma : \mathbb{Q}] = 6/|\sigma|$. 
In each of the cases under consideration here, \([\mathbb{Q}(\zeta_7)^\sigma : \mathbb{Q}]\) is prime, and hence \(\mathbb{Q}(\zeta_7)^\sigma = \mathbb{Q}(\alpha)\) for any \(\alpha \in \mathbb{Q}(\zeta_7)\) that is fixed by \(\sigma\) and does not lie in \(\mathbb{Q}\).

For \(\sigma_6\), this is easy: as \(\alpha = \zeta_7 + \zeta_7^6\) is fixed by \(\sigma_6\) by (6), this corresponds to the fact that \(\sigma_6\) is easily seen to be given by the restriction to \(\mathbb{Q}(\zeta_7)\) of complex conjugation, as that gives the unique automorphism of \(\mathbb{Q}(\zeta_7)\) of order 2. Thus \(\mathbb{Q}(\zeta_7)^{\sigma_6} = \mathbb{Q}(\zeta_7) \cap \mathbb{R}\). There is a general theorem that
\[
\mathbb{Q}(\zeta_n) \cap \mathbb{R} = \mathbb{Q}(\zeta_n + \zeta_n^{-1}).
\]

(c) For each intermediate field \(E\) above, give the Galois group of \(E\) over \(\mathbb{Q}\).

**Solution:** Since \([\mathbb{Q}(\zeta_7)^{\sigma_2} : \mathbb{Q}] = 2\), \(\text{Gal}(\mathbb{Q}(\zeta_7)^{\sigma_2} / \mathbb{Q})\) is cyclic of order 2. Since \([\mathbb{Q}(\zeta_7)^{\sigma_6} : \mathbb{Q}] = 3\), \(\text{Gal}(\mathbb{Q}(\zeta_7)^{\sigma_6} / \mathbb{Q})\) is cyclic of order 3.

3. Let \(F\) be the splitting field over \(\mathbb{Z}_2\) of \(f = x^6 + x^5 + 1\), an irreducible polynomial over \(\mathbb{Z}_2\).

(a) What is the Galois group of \(F\) over \(\mathbb{Z}_2\)?

**Solution:** Every finite extension of \(\mathbb{Z}_p\) is Galois, so \(F = \mathbb{Z}_2(\alpha)\) for any root \(\alpha\) of \(f\). In particular, \([F : \mathbb{Z}_2] = 6\), and the Galois group of \(F\) over \(\mathbb{Z}_2\) is cyclic of order 6, generated by the Frobenius automorphism \(\varphi(\beta) = \beta^2\) for all \(\beta \in F\).

(b) How many intermediate fields are there between \(\mathbb{Z}_2\) and \(F\) (including \(\mathbb{Z}_2\) and \(F\))? What are their orders as additive groups?

**Solution:** Since \(\text{Gal}(F / \mathbb{Z}_2)\) is cyclic of order 6, its lattice of subgroups is exactly that given in problem 2b above. The intermediate fields are \(F\) (order 64), \(\mathbb{Z}_2\) (order 2), and fields of degree 2 and 3 over \(\mathbb{Z}_2\). The field of degree 2 has order 4 and the one of degree 3 has order 8.

(c) For each intermediate field \(E\) (including \(F\)), what are the possible multiplicative orders of the units \(\beta\) for which \(E = \mathbb{Z}_2(\beta)\)?

**Solution:** The multiplicative group \(E^\times\) is cyclic of order \(|E| - 1\). Thus, for each \(k\) dividing \(|E^\times|\), the number of elements in \(E^\times\) of order \(k\) is exactly \(\phi(k)\), where \(\phi\) is the Euler \(\phi\)-function. So if \(k\) also divides the order of the unit group of a subfield of \(E\), then any element \(\beta\) of order \(k\) in \(E\) must lie in that subfield and \(\mathbb{Z}_2(\beta)\) will be that subfield and not \(E\). Thus, the orders of
the units $\beta$ for which $E = \mathbb{Z}_2(\beta)$ will be the divisors of $|E^\times|$ not dividing the order of the unit group of any proper subfield of $E$.

The most interesting case, then, is $F$. The possible orders of units $\beta$ for which $F = \mathbb{Z}_2(\beta)$ are the divisors of 63 that do not divide 1, 3 or 7. Thus, the possible orders of such $\beta$ are 9, 21 and 63.

The other unit groups all have prime order, so the possible orders are that prime.

(d) What is the minimal polynomial of an element of order 9?

Solution: Let $\beta$ have order 9 in $F^\times$. Then $\beta$ is a root of $x^9 - 1 = (x^3)^3 - 1$. To factor this, write $y^3 - 1 = (y - 1)(y^2 + y + 1)$. Thus, $\beta$ is a root of

$$x^9 - 1 = (x^3 - 1)(x^6 + x^3 + 1).$$

Since $\beta$ is not a root of $x^3 - 1$ it must be a root of $g = x^6 + x^3 + 1$. Since $F = \mathbb{Z}_2(\beta)$ by the last part, the minimal polynomial of $\beta$ has degree 6 and divides $g$. Thus, $g$ is the minimal polynomial.

4. Show there is a group of order $7 \cdot 8$ whose 7-Sylow subgroups are not normal.

Solution: The quick way to do this is to consider the field $F$ with 8 elements. $F^\times$ is cyclic of order 7. $F^\times$ acts on $F$ by multiplication, so we can form

$$G = F \rtimes F^\times$$

of order $|F| \cdot |F^\times| = 8 \cdot 7$. The action of $F^\times$ on $F$ is not trivial, so $F^\times$ is not normal in $G$. But $F^\times$ is the 7-Sylow subgroup of $G$.

We can make the same construction via matrices, noting that the $F$ above is additively isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, whose automorphism group is $\text{Gl}_3(\mathbb{Z}_2)$. In particular, all we need is to find a matrix $A \in \text{Gl}_3(\mathbb{Z}_2)$ of order 7. Then $\langle A \rangle$ acts nontrivially on $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ and the resulting group

$$G = (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes \langle A \rangle$$

has a nonnormal 7-Sylow subgroup by the reasoning above.

We now make use of rational canonical form. Any matrix of order 7 is a root of the polynomial

$$x^7 - 1 = (x - 1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1).$$

We wish to factor $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ in $\mathbb{Z}_2[x]$. By direct calculation, this is $(x^3 + x^2 + 1)(x^3 + x + 1)$, so any matrix root of either $x^3 + x^2 + 1$ or $x^3 + x + 1$ will be a root of $x^7 - 1$ of order not equal to 1. In particular, it will have order 7. So we can take $A$ to
be the companion matrix of either $x^3 + x^2 + 1$ or $x^3 + x + 1$, giving
\[
\begin{pmatrix}
0 & 0 & 1 \\
1 & 0 & 0 \\
0 & 1 & 1
\end{pmatrix}
\quad \text{or} \quad
\begin{pmatrix}
0 & 0 & 1 \\
1 & 0 & 1 \\
0 & 1 & 0
\end{pmatrix}.
\]
Either of these has order 7 in $\text{Gl}_3(\mathbb{Z}_2)$, allowing us to complete the construction above.

5. How many similarity classes of elements of order 8 are there in $\text{GL}_2(\mathbb{Z}_3)$? What are their rational canonical forms?

**Solution:** We factor $x^8 - 1$ in $\mathbb{Z}_3[x]$ to find the possible rational canonical forms. In $\mathbb{Z}[x]$, 
\[
x^8 - 1 = (x^4 + 1)(x^2 + 1)(x + 1)(x - 1).
\]
A matrix root of one of the last three factors will have order 4, 2 or 1, respectively, so we have to hope that $x^4 + 1$ factors in $\mathbb{Z}_3[x]$. Fortunately, it does:
\[
x^4 + 1 = (x^2 + x - 1)(x^2 - x - 1) \in \mathbb{Z}_3[x].
\]
This gives us exactly two rational canonical forms for $2 \times 2$ matrices over $\mathbb{Z}_3$ of order 8: $\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$. Thus, there are two conjugacy classes, represented by these two matrices.