1. Let $G$ be a group (not necessarily finite), and suppose that $H$ is a subgroup of index $n$. Show that there is a normal subgroup $N$ of $G$ with $n! \geq [G : N] \geq n$.

Solution: There is a natural action of $G$ on $G/H$ by left multiplication on the coset representative. This gives us an orbit map $g \mapsto -\cdot g' H$ for every coset $g' H \in G/H$. Since $H$ is a finite index subgroup, $G/H$ is finite. All finite groups can be embedded into a symmetric group of appropriate size, so there is a map $\varphi : G/H \to S_n$ where $|G/H| = [G : H] = n$. Therefore, for any coset $g' H$, we can compose the orbit map with this embedding to get a map $G \to S_n$ defined by $g \mapsto \varphi(g \cdot g' H)$. The kernel $K$ of this map is a normal subgroup of $G$. Also, $G/K$ is isomorphic to a subgroup of $S_n$, so $|G/K| = [G : K] \leq n!$.

On the other hand, the action of $G$ on $G/H$ is transitive, so $|G/K| = [G : K] \geq n$.

2. Determine, up to isomorphism, the number of groups of order 70.

Solution: $70 = 2 \cdot 5 \cdot 7$, so the Sylow theorems tell us there are subgroups, call them $P_2, P_5, P_7$ of sizes 2, 5, 7 respectively. We also know the number of such subgroups, $n_p$, divides the index $[G : P_p]$ and $n_p \equiv 1 \mod p$. Thus $n_7 = 1$ and so $P_7$ has no conjugate subgroups and is normal. Then $P_7 P_5 \leq G$ and because $P_7 \cap P_5 = \{e\}$, $P_7 \rtimes_{\psi} P_5$ where $\psi : P_5 \to \text{Aut}(P_7)$. We can think of $\psi : \mathbb{Z}/5 \to \text{Aut}(\mathbb{Z}/7) \cong \mathbb{Z}/6$ and such a map is determined by $\psi(1)$, because there are no elements in $\mathbb{Z}/6$ of order 5, it must be that $\psi(1) = 1$ and $H = P_7 P_5 \cong \mathbb{Z}/7 \times \mathbb{Z}/5$. Now note that $[G : H] = 2$ so it is a normal subgroup, thus $HP_2 \leq G$ and because $H \cap P_2 = \{e\}$ we get $G = H \rtimes_{\varphi} P_2$ where $\varphi : \mathbb{Z}/2 \to \text{Aut}(\mathbb{Z}/7 \times \mathbb{Z}/5) \cong \mathbb{Z}/6 \times \mathbb{Z}/4$. Then $\varphi$ is determined by $\varphi(1)$ which must have order dividing 2, so $\varphi(2) \in \{(0,0), (0,2), (3,0), (3,2)\}$. Thus, there are 4 groups of order 70.

3. Let $p$ be a prime integer, and $G$ a group in which $g^p$ is the identity for each $g$ in $G$. Show that $G$ must be abelian if $p = 2$. Give an example where $G$ is not abelian.
Solution: If \( p = 2 \) then \( g^2 = 1 \) for all \( g \in G \), so \( g^{-1} = g \). Let \( g, h \in G \), then \((gh)^2 = ghgh = 1\) and the commutator
\[ ggh^{-1}h^{-1} = ghg = 1 \]
so \( G \) is abelian.

To see that this need not hold for \( p \neq 2 \) consider the subgroup of \( M_3(\mathbb{Z}/3) \) of matrices of the form
\[
\begin{pmatrix}
1 & x & y \\
0 & 1 & z \\
0 & 0 & 1
\end{pmatrix}
\]
This is a subgroup because
\[
\begin{pmatrix}
1 & x & y \\
0 & 1 & z \\
0 & 0 & 1
\end{pmatrix}^2 = \begin{pmatrix}
1 & 2x & 2y + xz \\
0 & 1 & 2z \\
0 & 0 & 1
\end{pmatrix}
\]
and every element has order 3 because
\[
\begin{pmatrix}
1 & x & y \\
0 & 1 & z \\
0 & 0 & 1
\end{pmatrix}^3 = \begin{pmatrix}
1 & 3x & 3y + 3xz \\
0 & 1 & 3z \\
0 & 0 & 1
\end{pmatrix} = \begin{pmatrix}
1 & 0 & 0 \\
0 & 1 & 0 \\
0 & 0 & 1
\end{pmatrix}
\]
However the group is not abelian because, for example
\[
\begin{pmatrix}
1 & 1 & 1 \\
0 & 1 & 0 \\
0 & 0 & 1
\end{pmatrix} \begin{pmatrix}
1 & 2 & 0 \\
0 & 1 & 1 \\
0 & 0 & 1
\end{pmatrix} = \begin{pmatrix}
1 & 0 & 2 \\
0 & 1 & 1 \\
0 & 0 & 1
\end{pmatrix}
\]
\[
\begin{pmatrix}
1 & 2 & 0 \\
0 & 1 & 1 \\
0 & 0 & 1
\end{pmatrix} \begin{pmatrix}
1 & 1 & 1 \\
0 & 1 & 0 \\
0 & 0 & 1
\end{pmatrix} = \begin{pmatrix}
1 & 0 & 1 \\
0 & 1 & 1 \\
0 & 0 & 1
\end{pmatrix}
\]

4. Let \( R = \mathbb{Q}[x] \) and let \( M \) be the cokernel of the map from \( R^2 \to R^3 \) given by the matrix
\[
\begin{pmatrix}
x & 0 \\
x & x^2 \\
1 & 1
\end{pmatrix}
\]
Write \( M \) as a direct sum of cyclic \( R \)-modules.

Solution: The Smith normal form of the matrix is
\[
\begin{pmatrix}
1 & 0 & 0 \\
0 & x & 0 \\
0 & 0 & 0
\end{pmatrix}
\]
Hence the cokernel is \( R \oplus R/(1) \oplus R/(x) \).

5. Compute the characteristic polynomial, minimal polynomial and the Jordan form of the matrix
\[
\begin{pmatrix}
3 & 1 & -1 \\
2 & 2 & -1 \\
2 & 2 & 0
\end{pmatrix}
\]
8. Prove that the polynomial $x^9$ is irreducible over $\mathbb{Q}$.

Solution: Let $f(x) = x^9 - 1$, note that $f(0) = -1$, $f(1) = -1$ and $f(2) = -1$ so $f(x)$ has no roots in $\mathbb{F}_3$. (Also see this by noting that $\mathbb{F}_3^x \cong \mathbb{Z}/2$ so $a^5 = a$ for all $a \in \mathbb{F}_3^x$). So $p$ has no linear factors and if it factors over $\mathbb{F}_3$ then it must be the product of a degree 2 and a degree 3 irreducible polynomial.

There are 9 distinct monic polynomials of degree 2 in $\mathbb{F}_3[x]$. Because there are 3 degree 1 polynomials, there are 6 reducible degree 2 polynomials, so 3 irreducible polynomials of degree 2. Direct check shows that they are: $x^2 + 1, x^2 + x + 2, x^2 + 2x + 2$. Polynomial long division shows that none of these are a factor of $p(x)$, thus $p$ is irreducible over $\mathbb{F}_3$.

Let $\alpha$ be any root of $p$ and $K = \mathbb{F}_3(\alpha)$, then $[K : \mathbb{F}_3] = 5$, so $K \cong \mathbb{F}_{3^5}$. If $\alpha \in \mathbb{F}_9$ then we’d get a tower of fields $\mathbb{F}_3 \subseteq \mathbb{F}_3(\alpha) \subseteq \mathbb{F}_9$ but $[\mathbb{F}_9 : \mathbb{F}_3] = 2$, so $p$ has no roots in $\mathbb{F}_9$.

Whenever 5 divides $n$, $\mathbb{F}_{3^5}$ contains a copy of $\mathbb{F}_{3^5}$ and contains a root of $p$ so $p$ is not irreducible... unsure if $p$ is irreducible when 5 does not divide $n$.

9. Show that $K = \mathbb{Q}(\sqrt{1+\sqrt{3}})$ is not Galois over $\mathbb{Q}$ and compute $[K : \mathbb{Q}]$.

Solution: $\sqrt{1+\sqrt{3}}$ is a root of $f(x) = x^4 - 2x^2$ which is irreducible by Eisenstein’s criteria, and as such is the minimal polynomial of $\sqrt{1+\sqrt{3}}$. The roots of $f$ are $\{\pm\sqrt{1+\sqrt{3}}, \pm\sqrt{1-\sqrt{3}}\}$, two of which are imaginary and do not live in $K$. Thus $K \supset \mathbb{Q}$ is not normal and not Galois.
\[ [K : \mathbb{Q}] = \deg(\text{min. poly of } \sqrt[4]{1 + \sqrt{3}}) = 4 \]

10. Let \( p \) be a prime integer, and set \( f(x) = x^{p-1} + x^{p-2} + \ldots + x + 1 \). Suppose a prime integer \( q \) divides \( f(a) \) for some integer \( a \), prove that either \( q = p \) or \( q \equiv 1 \mod p \).

Use this to prove that the arithmetic sequence \( 1, 1+p, 2+p, \ldots \) contains infinitely many prime integers.

**Solution:** This was a homework problem.