1. Show that all groups of order 35 are cyclic.

The factors of 35 are 1, 5, 7, and 35.

By Sylow’s $p$-subgroup Theorem, there exists a subgroup of order 5, and the number of subgroups of order 5 divides 35 and is 1 mod 5.

$5, 7, 35 \neq 1 \mod 5$, so there is a unique subgroup of order 5.

Call this group $P$.

Since $P$ is the only subgroup of this order, it must be normal.

By Sylow’s $p$-subgroup Theorem, there exists a subgroup of order 75, and the number of subgroups of order 7 divides 35 and is 1 mod 7.

$5, 7, 35 \neq 1 \mod 7$, so there is a unique subgroup of order 7.

Call this group $Q$.

Since $Q$ is the only subgroup of this order, it must be normal.

By Lagrange, $P, Q$ are cyclic.

Let $a$ be a generator of $P$, $b$ a generator of $Q$.

Note that $aba^{-1}b^{-1} \in P \cap Q$ because $P, Q$ are normal.

Then $aba^{-1}b^{-1} = e$.

$ab = ba$.

$ab \in P \times Q \subseteq G$.

$(ab)^1 = ab \neq e$.

$(ab)^5 = a^5b^5 = b^5 \neq e$.

$(ab)^7 = a^7b^7 = a^2 \neq e$.

So, $ab$ has order 35.

$G = \langle ab \rangle$ and is cyclic.
2. Let $G$ be a finite group and $H$ a subgroup of index 2. Show $H$ is normal.

Choose $g \in G$.

If $g \in H$, then so is $g^{-1}$ and $gHg^{-1} = H$.

If $g \notin H$, then $gH \neq H$.

$g \in gH$.

So, $e \in gHg^{-1}$.

Since $H$ has index 2, either $gHg^{-1} = H$ or $gHg^{-1} = G \setminus H$.

$e \in gHg^{-1}$ and $e \notin G \setminus H$.

So, $gHg^{-1} = H$ and $H$ is normal.

3. Let $S, T$ be diagonalizable linear operators on a finite-dimensional $\mathbb{C}$-vectorspace $V$ with $ST = TS$. Show that $V$ has a basis of simultaneous eigenvectors for $S, T$.

$T$ is diagonalizable, so $V = \sum_{\lambda \text{ an eigenvalue of } T} V_{\lambda}$ where $V_{\lambda}$ is the $\lambda$ eigenspace of $T$ on $V$.

Let $v \in V_{\lambda}$.

\[
TSv = STv \\
= S(\lambda v) \\
= \lambda Sv
\]

So, $S(V_{\lambda}) \subseteq V_{\lambda}$.

Let $f(x)$ be the minimal polynomial of $S$ on $V, f_{\lambda}(x)$ be the minimal polynomial of $S$ of $V_{\lambda}$.

Since $f(S)$ vanishes on $V$, it also vanishes on $V_{\lambda}$.

This means $f_{\lambda}(x)$ divides $f(x)$.

Since $S$ is diagonalizable, $f(x)$ factors into linear factors.

This means $f_{\lambda}(x)$ must also factor into linear factors.

So, $S$ is diagonalizable on $V_{\lambda}$.

Each eigenvector for $S$ on $V_{\lambda}$ is also an eigenvector for $T$.

Each $V_{\lambda}$ has a basis of simultaneous eigenvectors for $S$ and $T$.

So $V$ has a basis of simultaneous eigenvectors for $S$ and $T$. 
4. Prove that \( x^5 + y^7 + z^{11} \) is irreducible in \( \mathbb{C}[x, y, z] \).

Notice that \( \mathbb{C}[x, y, z] \subset \mathbb{C}(x)[y, z] \), so if \( x^5 + y^7 + z^{11} \) is irreducible in the larger ring, then it is also irreducible in the smaller one.

First look at \( x^5 + y^7 \in \mathbb{C}(x)[y] \).
\( \mathbb{C}(x)[y] \) is a UFD, so \( \exists p(y) \) an irreducible nonunit in \( \mathbb{C}(x)[y] \) dividing \( x^5 + y^7 \).

If \( p^2(y) \) divides \( x^5 + y^7 \), then \( p(y) \) divides \( 7y^6 \).

Suppose this is the case.
Then \( x^5 + y^7 = \frac{p}{7}(7y^6) + x^5 \) means \( p(y) \) divides \( x^5 \).
But this would imply \( p(y) \) was a unit which is a contradiction.

\( p(y) \) does not divide \( x^5 + y^7 \), so \( p^2(y) \) does not divide \( x^5 + y^7 \).

\( p(y) \) divides \( x^5 + y^7 + x^{11} \) is irreducible in \( \mathbb{C}[x, y, z] \).

5. Describe all intermediate fields between \( \mathbb{Q} \) and \( \mathbb{Q}(\xi_{12}) \) where \( \xi_{12} \) is a primitive twelfth root of unity.

The conjugates to \( \xi_{12} \) are \( \xi_{12}^5, \xi_{12}^7, \) and \( \xi_{12}^1 \).

Let \( \alpha \) be the automorphism where \( \alpha(\xi_{12}) = \xi_{12}^5 \), \( \beta \) be the automorphism where \( \beta(\xi_{12}) = \xi_{12}^7 \), and \( \gamma \) be the automorphism where \( \gamma(\xi_{12}) = \xi_{12}^{11} \).

If \( \alpha(\xi_{12}) = \xi_{12}^5 = \xi_{12}^n \), then \( 5n \equiv 0 \text{ mod } 12 \).

So, \( n \equiv 0, 3, 6, 9 \) mod 12.

\( \alpha \) fixes \( \mathbb{Q}(\xi_{12}^3) = \mathbb{Q}(i) \), so \( \mathbb{Q}(i) \) is an intermediate field between \( \mathbb{Q} \) and \( \mathbb{Q}(\xi_{12}) \).

If \( \beta(\xi_{12}) = \xi_{12}^7 = \xi_{12}^n \), then \( 7n \equiv 0 \text{ mod } 12 \).

So, \( n \equiv 0, 2, 4, 6, 8, 10 \) mod 12.

\( \beta \) fixes \( \mathbb{Q}(\xi_{12}^2) = \mathbb{Q}(\xi_6) \).

\( xi_6 = e^{2\pi i/6} = \frac{1}{2} + i\frac{\sqrt{3}}{2} \)

So \( \mathbb{Q}(\sqrt{-3}) \) is an intermediate field between \( \mathbb{Q} \) and \( \mathbb{Q}(\xi_{12}) \).

\( \gamma \) fixes \( \xi_{12} + \xi_{12}^{-1} \)
\( \xi_{12} + \xi_{12}^{-1} = e^{2\pi i/12} + e^{-2\pi i/12} = 2\cos \pi/6 = \sqrt{3} \).

So \( \mathbb{Q}(\sqrt{3}) \) is an intermediate field between \( \mathbb{Q} \) and \( \mathbb{Q}(\xi_{12}) \).

6. Prove that \( x^4 + 1 \) is reducible in the polynomial ring \( \mathbb{F}_p[x] \) over the finite field \( \mathbb{F}_p \) with \( p \) elements, for every prime \( p \).

If \( p = 2 \), \( x^4 + 1 = (x + 1)^4 \), so it is reducible.
Any element of order 8 is a root of $x^4 + 1$.

Suppose $p \equiv 1 \mod 4$.

Then $p = 4m + 1$.

$p^2 - 1 = (4m + 1)(4m + 1) - 1 = 16m^2 + 8m^2$, which is divisible by 8.

Suppose $p \equiv 3 \mod 4$.

Then $p = 4m + 3$.

$p^2 - 1 = (4m + 3)(4m + 3) - 1 = 16m^2 + 24m^2 + 8$, which is divisible by 8.

$\mathbb{F}_{p^2}^\times$ has order $p^2 - 1$, so by Lagrange’s Theorem, $\exists$ an element of order 8.

Let $\alpha$ be an element of order 8 in $\mathbb{F}_{p^2}^\times$.

Let $P$ be the minimal polynomial of $\alpha$ in $\mathbb{F}_p[x]$.

Since $\mathbb{F}_p[x]$ is Euclidean, $x^4 + 1 = PQ + R$ where $Q, R \in \mathbb{F}_p[x]$, $\deg(R) < \deg(P)$.

Then $0 = R(\alpha)$.

By minimality of $P, R$ is identically 0.

So $P$ divides $x^4 + 1$.

$x^4 + 1$ is reducible in $\mathbb{F}_p[x]$.

7. Grant that the right $\mathbb{Z}[i]$ of Gaussian integers is Euclidean, this is a principal ideal domain. Observe that $(2 + i)(2 - i) = 5$. How many isomorphism classes of $\mathbb{Z}[i]$ modules with exactly 5 elements are there?

By the Structure Theorem, all finite $\mathbb{Z}[i]$ modules are $\mathbb{Z}[i]/I_1 \times \ldots \times \mathbb{Z}[i]/I_n$ where $I_1, \ldots, I_n$ are ideals.

Since 5 is prime and $\mathbb{Z}[i]$ is a PID, all $\mathbb{Z}[i]$ modules of order 5 are $\mathbb{Z}[i]/I$ where $I = \langle a + bi \rangle$ and $a^2 + b^2 = 5$.

Then $a + bi$ could be any of $1 + 2i, 1 - 2i, -1 + 2i, -1 - 2i, 2 + i, 2 - i, -2 + i, -2 - i$.

However, $-1(2 + i) = -2 - i, i(2 + i) = -1 + 2i$, and $-i(2 + i) = 1 - 2i$, so the ideals generated by $2 + i, -2 - i, -1 + 2i$, and $1 - 2i$ are the same.

Similarly, the ideals generated by $1 + 2i, -1 - 2i, 2 - i$, and $-2 + i$ are the same.

Let $M = \mathbb{Z}[i]/(2 + i), N = (2 - i)$.

Let $\varphi : M \to N$ be a module homomorphism.

Note that $2 - i \not\in (2 + i)$.

$\varphi(2 - i) = (2 - i)\varphi(1) = 0$.

So a nonzero element in $M$ maps to 0 in $N$.

$\varphi$ is not an isomorphism.

So, there are 2 isomorphism classes of $\mathbb{Z}[i]$ modules with 5 elements.