1. Describe all abelian groups of order 72.

By the fundamental theorem of finite abelian groups, a group $G$ of order 72 will be isomorphic to one of the following:

$$
\begin{align*}
\mathbb{Z}_{72} &\cong \mathbb{Z}_9 \times \mathbb{Z}_8 \\
\mathbb{Z}_9 \times \mathbb{Z}_4 \times \mathbb{Z}_2 \\
\mathbb{Z}_9 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \\
\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_8 \\
\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_2 \\
\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 
\end{align*}
$$

since $72 = 3^2 \cdot 2^3$.

2. Construct a non-abelian group of order 27.

Obviously, $27 = 3^3$. Let’s create an embedding $f : \mathbb{Z}_3 \rightarrow Aut(\mathbb{Z}_9) \cong \mathbb{Z}_6$. Suppose $f(x) = 2^x$. Then the group $\mathbb{Z}_3 \times \mathbb{Z}_9$ with the group operation, $\ast$, defined as

$$(x_1, y_1) \ast (x_2, y_2) = \left( x_1 + x_2, \ (f(x_1^{-1}) \cdot y_1) + y_2 \right)$$

is of order 27, but is not abelian since

$$(1, 2) \ast (2, 1) = (1 + 2, (2^1 \cdot 2) + 1) = (0, 5)$$

but

$$(2, 1) \ast (1, 2) = (2 + 1, (2^2 \cdot 1) + 2) = (0, 6).$$
3. Find all pairs of integers \( x, y \) such that \( 157x + 101y = 1 \).

By the Euclidean Algorithm, we get
\[
\begin{align*}
157 &= 101 + 56 \\
101 &= 56 + 45 \\
56 &= 45 + 11 \\
45 &= 11(4) + 1.
\end{align*}
\]
So the greatest common divisor of 157 and 101 is 1.

Now, let \( V \) be a \( \mathbb{C} \)-linear map of a finite-dimensional \( \mathbb{C} \)-vectorspace to itself. Prove that there is at least one simultaneous eigenvector.

Suppose that \( A = \{ T_1, T_2, \ldots, T_n \} \). Then, we can notice that \( T_i T_j = T_j T_i \), for every \( i, j = 1, \ldots, n \). So every eigenspace of \( T_i \) is \( T_j \)-stable (i.e., \( T_j \) stabilizes every eigenspace of \( T_i \)).

Proof. Let \( v \) be a \( \lambda \)-eigenvector of \( T_i \), then
\[
T_i (T_j v) = (T_j T_i) v = (T_i T_j) v = T_j (T_i v) = T_j (\lambda v) = \lambda \cdot T_j v
\]
Thus, if \( v \) is a \( \lambda \)-eigenvector of \( T_i \), then \( T_j v \) is too.

Now, let \( f_1(x) \in \mathbb{C}[x] \) be the minimal polynomial of \( T_1 \), then since \( \mathbb{C} \) is algebraically closed, \( f_1(x) \) has a root \( \lambda_1 \in \mathbb{C} \), an eigenvalue for \( T_1 \). Let \( V_{\lambda_1} \) represent the \( \lambda_1 \)-eigenspace of \( T_1 \), which is \( T_2 \)-stable. Let \( f_2(x) \in \mathbb{C}[x] \) be the minimal polynomial of \( T_2 \) restricted to \( V_{\lambda_1} \). Now, again since \( \mathbb{C} \) is algebraically closed, \( f_2(x) \) has a root \( \lambda_2 \in \mathbb{C} \), which is an eigenvalue of \( T_2 \). Let \( V_{\lambda_2} \) represent the \( \lambda_2 \)-eigenspace of \( T_2 \), which is \( T_3 \)-stable.

By induction, we will get that \( V_{\lambda_{n-1}} \) is the \( \lambda_{n-1} \)-eigenspace of \( T_{n-1} \), which is \( T_n \)-stable. Let \( f_n(x) \in \mathbb{C}[x] \) be the minimal polynomial of \( T_n \) restricted to \( V_{\lambda_{n-1}} \). \( \mathbb{C} \) is algebraically closed, so \( f_n(x) \) has a root \( \lambda_n \in \mathbb{C} \), which is an eigenvalue of \( T_n \) with some corresponding eigenvector \( v \).

Thus, \( v \) is a \( \lambda_{i} \)-eigenvector of \( T_i \), for each \( i = 1, \ldots, n \), as required.
5. Prove that the ideal generated by 7 and \(x^2 + 1\) is a maximal ideal in \(\mathbb{Z}[x]\).

First notice that
\[
\mathbb{Z}[x]/\langle 7, x^2 + 1 \rangle \simeq \mathbb{Z}_7[x]/\langle 7 \rangle.
\]
Now, since \(\mathbb{Z}_7\) is a field, we know that \(\mathbb{Z}_7[x]\) is Euclidean, thus a principle ideal domain. Now, in a principal ideal domain all prime ideals are maximal.

**Proof.** Suppose \(R\) is a principle ideal domain and \(I = \langle p \rangle\) is a prime ideal, then \(p\) is prime because if \(p | ab\) then \(ab \in I\) so \(a \in I\) or \(b \in I\), so either \(p | a\) or \(p | b\). Now, if \(J \supseteq I\), then \(J = \langle q \rangle\) and \(q\) divides \(p\). Since \(p\) is irreducible in \(R\), either \(q\) is a unit in \(R\) or \(q = p\). Since \(J \supseteq I\), \(q\) must be a unit in \(R\), so \(J = R\), thus \(I\) is maximal. \(\square\)

Since \(\mathbb{Z}_7[x]\) is a factorial ring (unique factorization domain), so all irreducible elements are prime, hence generating prime ideals. Now \(x^2 + 1\) is irreducible in \(\mathbb{Z}_7[x]\) because, if \(x^2 + 1\) were to factor, then it would have a linear factor, but
\[
\begin{array}{c|c}
0^2 + 1 & 1 \\
1^2 + 1 & 2 \\
2^2 + 1 & 5 \\
3^2 + 1 & 3 \\
4^2 + 1 & 3 \\
5^2 + 1 & 5 \\
6^2 + 1 & 2 \\
\end{array}
\]

none of which are 0, thus \(x^2 + 1\) has no linear factors in \(\mathbb{Z}_7[x]\), therefore, it is irreducible. So \(\langle x^2 + 1 \rangle\) is maximal, which then implies that \(\mathbb{Z}_7[x]/\langle x^2 + 1 \rangle\) is a field, and thus \(\mathbb{Z}[x]/\langle 7, x^2 + 1 \rangle\) is a field, so the ideal \(\langle 7, x^2 + 1 \rangle\) is maximal in \(\mathbb{Z}[x]\), as required. \(\blacksquare\)

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
\[
Gal(\mathbb{Q}(\zeta_9)/\mathbb{Q}) = (\mathbb{Z}_9)^\times \simeq \mathbb{Z}_6.
\]

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 \(\sigma_9: \zeta_9 \mapsto \zeta_9^a\), where \(\gcd(9, a) = 1\) and \(a < 9\). So \(Gal(\mathbb{Q}(\zeta_9)/\mathbb{Q}) \simeq \langle \sigma_2 \rangle\) since \(\langle \sigma_2 \rangle = \{\sigma_2, \sigma_4, \sigma_8, \sigma_7, \sigma_5, id\}\) is a cyclic group of order 6, thus isomorphic to \(\mathbb{Z}_6\).

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

By the Fundamental Theorem of Galois Theory, the subgroups of \(Gal(\mathbb{Q}(\zeta_9)/\mathbb{Q})\) 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
\[
\zeta_9^3 = \zeta_3 = e^{\frac{2\pi i}{3}} = \cos \left(\frac{2\pi}{3}\right) + i \sin \left(\frac{2\pi}{3}\right) = -\frac{1}{2} + i \frac{\sqrt{3}}{2}.
\]

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

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
\[
f(x) = x^3 - 3x + 1 \quad \text{and fixed by} \quad \langle \sigma_8 \rangle.
\]
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.

\[
\boxed{
7. \text{Prove that the tenth cyclotomic polynomial}
\Phi_{10}(x) = \frac{(x^{10} - 1)(x - 1)}{(x^5 - 1)(x^2 - 1)} = x^4 - x^3 + x^2 - x + 1
\]
is \textit{irreducible} in \(\mathbb{F}_3[x]\), where \(\mathbb{F}_3\) is the finite field with 3 elements.
\]

Since \(\text{char}(\mathbb{F}_3) = 3\) does not divide 10, the roots of \(\Phi_{10}(x)\) will have order 10, because the roots of \(\Phi_{10}(x)\) are \textbf{precisely} the primitive tenth roots of unity. However, there are no elements of order 10 in \(\mathbb{F}_3\), so there are no linear factors of \(\Phi_{10}(x)\) in \(\mathbb{F}_3[x]\).

If there are quadratic factors of \(\Phi_{10}(x)\) in \(\mathbb{F}_3[x]\) then the roots of \(\Phi_{10}(x)\) will be in \(\mathbb{F}_3^2\). Again, the roots must be of multiplicative order 10, however, \(|(\mathbb{F}_3^2)^\times| = 8\) and 10 does not divide 8, so there are no elements of order 10 in \(\mathbb{F}_3^2\). Thus, \(\Phi_{10}(x)\) does not have any quadratic factors in \(\mathbb{F}_3[x]\).

Since \(\Phi_{10}(x)\) has no linear factors and no quadratic factors in \(\mathbb{F}_3[x]\), is is irreducible, as required.