1. Consider the polynomial \( p(x) = x^3 + x^2 + 3x + 4 \in \mathbb{Z}_5[x] \). [15 pts]
   (a) Show that \( p(x) \) is irreducible over \( \mathbb{Z}_5[x] \).
   (b) Describe an element in \( \mathbb{Z}_5[x]/\langle x^3 + x^2 + 3x + 4 \rangle \) as succinctly as possible. How many such elements are there?
   (c) Calculate the simplest form of the product:
   \[
   (x^2 + 2x + 2 + \langle x^3 + x^2 + 3x + 4 \rangle) (x^2 + 3x + 4 + \langle x^3 + x^2 + 3x + 4 \rangle)
   \]

2. On of our major field theory theorems tells us that if \( a \in \mathbb{R} \) is the root of a monic and irreducible \( p(x) \in \mathbb{Q}[x] \) then \( \mathbb{Q}[x]/\langle p(x) \rangle \approx \mathbb{Q}(a) \) [15 pts]
   Given:
   \[
   a = \sqrt{21 + \sqrt{439}}
   \]
   (a) Find the monic and irreducible polynomial \( p(x) \in \mathbb{Q}[x] \) for which \( a \) is a root. You must prove it is minimal.
   (b) State the result of the theorem as it applies here and give the corresponding isomorphism.
   You do not need to prove it is an isomorphism.
   (c) Find a basis for \( \mathbb{Q}\left(\sqrt{21 + \sqrt{439}}\right) \) as an extension of \( \mathbb{Q}\left(\sqrt{439}\right) \). Justify.

3. Suppose \( G \) is a group and \( g \in G \) has \( |g| = 245 \). [15 pts]
   (a) Calculate \( |g^{196}| \).
   (b) Calculate the elements in \( \langle g^{140} \rangle \) with minimal nonnegative exponents.
   (c) What can you say about the number of elements of order 35 in \( \langle g \rangle \)?
   (d) What can you say about the number of elements of order 35 in \( G \)?

4. Consider the group \( G = \mathbb{Z}_{2541} \oplus \mathbb{Z}_{4851} \). [15 pts]
   (a) Find the number of elements of order 21 in \( G \).
   (b) Find the number of cyclic subgroups of order 21 in \( G \).

5. In \( \mathbb{Q}[x] \) find an irreducible polynomial \( p(x) \) of minimal degree satisfying:
   \[
   \langle p(x) \rangle = \langle 5x^3 + 7x^2 + 19x + 19, x^2 + 2x + 3 \rangle
   \]
   Make sure you prove all of equality, minimal degree and irreducibility. If your \( p(x) \) turns out to be a unit you can ignore proving irreducibility.

6. Show that the element \( 93 + 71\sqrt{-5} \) is irreducible in \( \mathbb{Z}[\sqrt{-5}] \). [15 pts]

7. Determine if \( U(29) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_{14} \). [10 pts]
8. Suppose $G$ is a group and $M \leq G$ and $N \leq G$. Define:

$$MN = \{mn \mid m \in M, n \in N\}$$

(a) Show that it is not necessarily the case that $MN \leq G$.

(b) Prove that if $M \triangleleft G$ and $N \triangleleft G$ and if $MN \leq G$ then $MN \triangleleft G$.

9. Let $R$ be a commutative ring with unity.

(a) An element $a \in R$ is idempotent if $a^2 = a$. Prove that if $a \in R$ is idempotent then so is $1 - a$.

(b) An element $a \in R$ is nilpotent if $a^n = 0$ for some $n \in \mathbb{Z}^+$. Prove that if $a, b$ are nilpotent then so is $a + b$.

10. Prove using the definition of a principal ideal that $\langle x, 2 \rangle$ is not a principal ideal of $\mathbb{Z}[x]$.

11. Find all ring homomorphisms from $\mathbb{Q}$ to $\mathbb{Q}$.

12. Let $F$ be a field and let $K \subseteq F$ with at least two elements. Suppose $K$ has the property that if $a, b \in K$ with $b \neq 0$ then $a - b \in K$ and $ab^{-1} \in K$.

(a) Prove that $1 \in K$

(b) Prove that if $a \in K$ then $a^{-1} \in K$.

(c) Prove that if $a, b \in K$ then $ab \in K$.

(d) Explain why $K$ is a subring of $F$.

(e) Explain why $K$ is commutative.

(f) Explain why $K$ is a subfield of $F$.

13. For a ring $R$ define the center of $R$ to be $Z(R) = \{x \in R \mid rx = xr \text{ for all } r \in R\}$ Prove that $Z(R)$ is a subring of $R$.

14. Suppose a group $G = \{1, A, B, C, D, E\}$ has the following operation table:

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>A</td>
<td>B</td>
<td>C</td>
<td>D</td>
<td>E</td>
</tr>
<tr>
<td>A</td>
<td>A</td>
<td>1</td>
<td>D</td>
<td>E</td>
<td>B</td>
<td>C</td>
</tr>
<tr>
<td>B</td>
<td>B</td>
<td>C</td>
<td>1</td>
<td>A</td>
<td>E</td>
<td>D</td>
</tr>
<tr>
<td>C</td>
<td>C</td>
<td>B</td>
<td>E</td>
<td>D</td>
<td>1</td>
<td>A</td>
</tr>
<tr>
<td>D</td>
<td>D</td>
<td>E</td>
<td>A</td>
<td>1</td>
<td>C</td>
<td>B</td>
</tr>
<tr>
<td>E</td>
<td>E</td>
<td>D</td>
<td>C</td>
<td>B</td>
<td>A</td>
<td>1</td>
</tr>
</tbody>
</table>

(a) Determine if $G$ is Abelian. Justify.

(b) Determine if $G$ is cyclic. Justify.

(c) Find the inverse of $D$.

(d) Find all subgroups of order 2.

(e) Find a subgroup of order 3.

(f) Find an element $x \in G$ such that $AxC = E$. 