1. (5 points each)

(a) Define the term *cyclic group*.

(b) Show that every group of prime order is cyclic.
2. (3 points each) Consider the following permutation in $S_6$:

$$
\sigma = \begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 \\
3 & 6 & 4 & 1 & 5 & 2
\end{pmatrix}
$$

(a) Find $\sigma^{-1}$.

(b) Express $\sigma$ as a product of disjoint cycles.

(c) Express $\sigma$ as a product of transpositions.

(d) Is $\sigma$ even or odd? Explain.

(e) Find the order of $\sigma$. 

3. (10 points) The group $S_3$ consists of the following six permutations.

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = () \quad \mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2,3)$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1,2,3) \quad \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1,3)$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1,3,2) \quad \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1,2)$$

Find all subgroups of $S_3$, and say which ones are normal.
4. (4 points each)

(a) Define the term zero divisor.

(b) Define the term unit.

(c) List the units and the zero divisors in the ring $\mathbb{Z}_{10}$. 
5. (3 points each) Which of the following polynomials is irreducible? Justify your answers.

(a) $x^2 - 2$ in $\mathbb{Q}[x]$

(b) $x^2 - 2$ in $\mathbb{R}[x]$

(c) $x^2 - 2$ in $\mathbb{Z}_7[x]$

(d) $x^4 + x^2 + 1$ in $\mathbb{R}[x]$

(e) $x^4 + x^2 + 1$ in $\mathbb{Z}_2[x]$

(f) $x^{100} + x^{11} + x + 1$ in $\mathbb{Z}_2[x]$
6. (5 points each)

(a) Let $S = \{ a + b\sqrt{2} : a, b \in \mathbb{Q} \}$. Show that $S$ is a subfield of the field $\mathbb{R}$ of real numbers.

(b) Show that $\mathcal{I} = \{ f(x) \in \mathbb{Q}[x] : f(\sqrt{2}) = 0 \}$ is the principal ideal in $\mathbb{Q}[x]$ generated by $x^2 - 2$.

(c) Show that $S$ is isomorphic to the quotient ring $\mathbb{Q}[x]/(x^2 - 2)$. 
7. (5 points each)

(a) Define the term *principal ideal*.

(b) Prove that every ideal in \( \mathbb{Z} \) is principal.
8. (5 points each)

(a) Define greatest common divisors in an integral domain.

(b) Prove that if $R$ is a principal ideal domain, and $a, b \in R$ are not both 0, then $a$ and $b$ have a greatest common divisor.