(1) (5 points each) In the following, \(a\), \(b\) and \(m\) are integers. Complete the following definitions.
   \[
   \text{(a) We say that } a \text{ divides } b \text{ if } \ldots \\
   \text{(b) We say that } a \text{ is congruent to } b \text{ modulo } m \text{, if } \ldots 
   \]

(2) (5 points each) In the following, \(f\), \(g\) and \(h\) are polynomials with coefficients in a field \(F\). Complete the following definitions.
   \[
   \text{(a) We say } h \text{ is a greatest common divisor of } f \text{ and } g \text{, if } \ldots \\
   \text{(b) We say that } f(x) \text{ is irreducible, if } \ldots 
   \]

(3) (5 points each) Complete the following definitions.
   \[
   \text{(a) If } G \text{ is a group and } x \in G, \text{ the cyclic subgroup generated by } x \text{ is } \ldots \\
   \text{(b) An abelian group is } \ldots 
   \]

(4) (5 points each) State without proof the following.
   \[
   \text{(a) The division algorithm for the ring of integers.} \\
   \text{(b) The division algorithm for the ring of polynomials } F[x] \text{ over a field } F. 
   \]

(5) (5 points each) True or false? If true, give a proof. If false, give a counterexample. In the following, \(a\), \(b\) and \(c\) are numbers.
   \[
   \text{(a) If } (a, b) = 1 \text{ and } (b, c) = 1, \text{ then } (a, c) = 1. \\
   \text{(b) If } a \mid c \text{ and } b \mid c, \text{ then } ab \mid c. 
   \]

(6) Prove the following.
   \[
   \text{(a) (10 points) For numbers } a, b, c, \text{ if } a \mid bc \text{ and } (a, b) = 1, \text{ then } a \mid c. \text{ (Use Bezout’s Identity.)} \\
   \text{(b) (10 points) If } G \text{ is a finite group, and } x \in G, \text{ and } H \text{ is a subgroup of } G, \text{ then } H \text{ and } xH \text{ have the same number of elements.} \\
   \text{(c) (10 points) If } G \text{ is a finite abelian group of order } n \text{ and } x \in G, \text{ then } x^n = e. \\
   \text{(d) (10 points) For integers } r, a, b, m, \text{ if } ra \equiv rb \pmod{m}, \text{ and } (r, m) = 1, \text{ then } a \equiv b \pmod{m}. 
   \]

(7) (20 points) Give an example for each of the following. If none exists, say so.
   \[
   \text{(a) A field of characteristic 0.} \\
   \text{(b) A field with 9 elements.} \\
   \text{(c) A field with 12 elements.} \\
   \text{(d) An abelian group of order 100.} \\
   \text{(e) A non-abelian group.} \\
   \text{(f) A non-commutative ring.} \\
   \text{(g) A ring with 16 elements which is not a field.} \\
   \text{(h) An irreducible cubic polynomial in } F_3[x]. \\
   \text{(i) An irreducible cubic polynomial in } Q[x]. \\
   \text{(j) An irreducible cubic polynomial in } R[x]. 
   \]

(8) (15 points) Find all solutions \(x \pmod{86}\).
   \[
   \text{(a) } 22x \equiv 84 \pmod{86} \\
   \text{(b) } 22x \equiv 85 \pmod{86} \\
   \text{(c) } 21x \equiv 84 \pmod{86} 
   \]
Let $F$ be a field and $f$ a polynomial in $F[x]$ of degree $d$. Assume $d \geq 1$. Prove the following.

(a) (10 points) The polynomial $f$ factors into irreducibles. In other words, for some $n \geq 1$ there are irreducible polynomials $p_1, \ldots, p_n$ in $F[x]$ such that $f = p_1 \cdots p_n$.

(b) (10 points) Given any $g$ in $F[x]$, there exists a polynomial $r$ in $F[x]$ such that $g \equiv r \pmod{f}$ and the degree of $r$ is less than $d$.

(c) (15 points) The ring $F[x]/(f)$ is a field if and only if $f$ is irreducible.

(10) (20 points) Let $f(x) = x^2 + x + 1$ and $R = \mathbb{F}_3[x]/f(x)$.

(a) Show that $R$ is not a field.

(b) In $R$ find all units and zero divisors. For each unit, find the inverse. For each unit, find the order.

(c) Find all solutions $a \in R$ to each equation.
   
   (i) $a^2 = 0$
   (ii) $a^2 = 1$
   (iii) $a^3 = 1$
   (iv) $a^3 = a$

(11) (20 points) Let $f(x) = x^3 + x + 1$. Let $F = \mathbb{F}_2[x]/f(x)$.

(a) Prove that $F$ is a field.

(b) Find the units of $F$. For each unit, find the order and the inverse.

(c) Find a primitive element for $F$.

(d) Find all solutions $a \in F$ to each equation.

   (i) $a^2 = 0$
   (ii) $a^2 = 1$
   (iii) $a^3 = 1$
   (iv) $a^3 = a$