Problem 1. [10 points.]

(a) Give the definition of a finite-dimensional vector space over a field \( F \).

A vector space over a field \( F \) is a set \( V \) equipped with operations \( + : V \times V \rightarrow V \) and \( \cdot : F \times V \rightarrow V \) such that \( V \) is a vector space over \( + \); \( \cdot \) is associative; the multiplicative identity \( 1 \in F \) is also an identity for \( \cdot \); and \( \cdot \) distributes over addition on both sides. The vector space \( V \) is finite-dimensional if there exists a finite set \( B \) such that every element of \( V \) can be written (in at least one way) as a linear combination of \( B \).

(b) State the Cayley-Hamilton theorem for matrices over a field \( F \).

Let \( A \) be an \( n \times n \) matrix over \( F \) for some positive integer \( n \). The characteristic polynomial of \( A \) is the polynomial \( p(t) = \det(tI - A) \) where \( I \) is the \( n \times n \) identity matrix over \( F \). The Cayley-Hamilton theorem states that \( p(A) \) is the zero matrix.

(c) State the unique factorization theorem for polynomials (in one variable) over a field \( F \).

A polynomial \( p \in F[x] \) is irreducible if it is not a constant and, for every factorization \( p = qr \) in \( F[x] \), one of \( q \) or \( r \) is a constant. The unique factorization theorem
states that every monic polynomial in \( F[x] \) can be factored as a product of monic irreducible polynomials, and this factorization is unique up to permutations of the factors.

**Problem 2. [10 points.]**

Consider the system of linear equations

\[
3x_1 - 2x_2 = 1 \\
5x_1 + 4x_2 = 3.
\]

(a) Solve this system over \( F_5 \).

In \( F_5 \), the second equation becomes \( 4x_2 = 3 \) and hence \( x_2 = -3 = 2 \). Substituting into the first equation, \( 3x_1 = 1 + 2x_2 = 1 + 2 \times 2 = 0 \) and so \( x_1 = 0 \).

(b) Solve this system over \( F_7 \).

There are several ways to do this (including Cramer’s rule); here, let me use row reduction of the augmented matrix. Start with

\[
\begin{pmatrix}
3 & 5 & 1 \\
5 & 4 & 3
\end{pmatrix}
\]

and multiply the first row by 5:

\[
\begin{pmatrix}
1 & 4 & 5 \\
5 & 4 & 3
\end{pmatrix}
\]

Now subtract 5 times the first row from the second:

\[
\begin{pmatrix}
1 & 4 & 5 \\
0 & 5 & 6
\end{pmatrix}
\]

multiply the second row by 3:

\[
\begin{pmatrix}
1 & 4 & 5 \\
0 & 1 & 4
\end{pmatrix}
\]

and subtract 4 times the second row from the first:

\[
\begin{pmatrix}
1 & 0 & 3 \\
0 & 1 & 4
\end{pmatrix}
\]

to get \( x_1 = 3, x_2 = 4 \).
(c) Determine the number of solutions of this system over $\mathbb{F}_{11}$.

Again we do row reduction of the augmented matrix. Start with

$$
\begin{pmatrix}
3 & 9 & 1 \\
5 & 4 & 3 
\end{pmatrix}
$$

and multiply the first row by 4:

$$
\begin{pmatrix}
1 & 3 & 4 \\
5 & 4 & 3 
\end{pmatrix}
$$

Now subtract 5 times the first row from the second:

$$
\begin{pmatrix}
1 & 3 & 4 \\
0 & 0 & 5 
\end{pmatrix}
$$

and note that the system is inconsistent. Therefore, there are no solutions.

**Problem 3.** [10 points.]

Let $A$ be a $3 \times 3$ matrix over a field $F$. Let $\lambda_1, \lambda_2, \lambda_3, \lambda_4 \in F$ be four distinct elements. Let $v_1, v_2, v_3, v_4 \in F^3$ be elements such that $Av_i = \lambda_i v_i$ for $i = 1, 2, 3, 4$. Prove that $v_1, \ldots, v_4$ cannot all be nonzero.

It is a theorem in the book (Proposition 4.5.14) that a linear operator on $F^3$ has at most 3 eigenvalues. (Proof: the eigenvalues are all roots of the characteristic polynomial, which has degree 3; and a polynomial of degree 3 over a field can have at most 3 distinct roots). Consequently, one of the $\lambda_i$ must fail to be an eigenvalue of $A$, and then the only solution of $Av_i = \lambda_i v_i$ is the zero vector $v_i = 0$.

**Problem 4.** [10 points.]

For each of the following examples, specify whether or not it is a ring. If it is a ring, do nothing more; if it is not a ring, state one condition from the definition of a ring that is violated by the example (in some cases, there may be more than one correct answer).

(a) The set of nonnegative integers, with usual addition and multiplication. **This is not a ring: the element 1 does not have an additive inverse.**

(b) The set of complex numbers of the form $a + b\sqrt{-3}$ with $a, b \in \mathbb{Z}$, with usual addition and multiplication. **This is a ring.**

(c) The set of continuous functions $\mathbb{R} \to \mathbb{R}$, with $(f+g)(x) = f(x) + g(x)$ and $(fg)(x) = (f \circ g)(x)$ (composition). **This is not a ring: multiplication is not commutative.** For example, if $f(x) = x + 1$ and $g(x) = 2x$, then $(fg)(x) = 2x + 1$ but $(gf)(x) = 2(x + 1) = 2x + 2$. 

Another possible answer: multiplication does not distribute over addition. For example, if $f(x) = x + 1$, $g(x) = x$ and $h(x) = x$, then $(f(g + h))(x) = f(2x) = 2x + 1$ while $(fg + fh)(x) = (x + 1) + (x + 1) = 2x + 2$.

Problem 5. [10 points.]

Find (with justification) generators of the kernels of the following homomorphisms.

(a) $\mathbb{R}[x, y] \rightarrow \mathbb{R}$ defined by $f(x, y) \mapsto f(0, 1)$;

The kernel is generated by $x$ and $y - 1$ (which are obviously elements). For $p(x, y) \in \mathbb{R}[x, y]$, form the Taylor expansion $p(x, y) = \sum_{i,j=0}^{\infty} p_{ij}(x, y)x^i(y - 1)^j$ at the point $(0, 1)$; note that only finitely many of the terms are nonzero. In this notation, $p(x, y) = 0$ if and only if $p_{00}(x, y) = 0$. In every other summand, either $i > 0$, in which case the summand is divisible by $x$; or $j > 0$, in which case the summand is divisible by $y - 1$. Consequently, every element of the kernel can be written as a multiple of $x$ plus a multiple of $y - 1$. (An alternate approach would be to perform long division by $x$ in $(\mathbb{R}[y])[x]$, then divide the remainder by $y - 1$ in $\mathbb{R}[y]$.)

(b) $\mathbb{Z}[x] \rightarrow \mathbb{R}$ defined by $f(x) \mapsto f(2 - \sqrt{3})$;

The kernel is generated by $(x - 2 - \sqrt{3})(x - 2 + \sqrt{3}) = (x - 2)^2 - 3 = x^2 - 4x + 1$. By Euclidean division, every element in the kernel is congruent modulo $x^2 - 4x + 1$ to a polynomial of the form $a + bx$ for some $a, b \in \mathbb{Z}$. But if there were a nonzero polynomial of this form in the kernel, then $2 - \sqrt{3}$ would equal the rational number $-a/b$ and so $\sqrt{3}$ would be irrational, which we know is not true by unique factorization of integers. Hence the kernel consists only of the multiples of $x^2 - 4x + 1$.

(c) $\mathbb{R}[x] \rightarrow \mathbb{C}$ defined by $f(x) \mapsto f(1 - 3i)$.

Similarly, the kernel is generated by $(x - 1 + 3i)(x - 1 - 3i) = (x - 1)^2 + 3 = x^2 - 2x + 4$. Again, by Euclidean division, every element in the kernel is congruent modulo $x^2 - 2x + 4$ to a polynomial of the form $a + bx$ for some $a, b \in \mathbb{R}$. But if there were a nonzero polynomial of this form in the kernel, then $1 - 3i$ would equal the rational number $-a/b$ which is obviously impossible (by comparing real and imaginary parts). Hence the kernel consists only of the multiples of $x^2 - 2x + 4$.

Problem 6. [10 points.]

Prove that the following pairs of rings are not isomorphic.

(a) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/8\mathbb{Z}$.

Isomorphic rings have isomorphic additive groups. But in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ there is no element of order 8, whereas there is one in $\mathbb{Z}/8\mathbb{Z}$; so even the additive groups cannot be isomorphic.
(b) $\mathbb{F}_2[x]/(x^2)$ and $\mathbb{F}_2[x]/(x^2 + x + 1)$.

In the first ring, the element $x$ is nilpotent (its square is zero); if there were an isomorphism with the second ring, then the second ring would also have a nonzero nilpotent element. However, the second ring is a field because $x^2 + x + 1$ is irreducible (since it is quadratic, to check irreducibility it is enough to check that there are no roots in $\mathbb{F}_2$) and so its only nilpotent element is 0.