Mathematics 310
Robert Gross
Homework 9
Answers

1. Suppose that F is a field. Let

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \;\middle|\; a, b, c \in F \right\}$$
$$I = \left\{ \begin{pmatrix} 0 & d \\ 0 & 0 \end{pmatrix} \;\middle|\; d \in F \right\}$$

Show that
  (a) R is a ring.
  (b) I is an ideal of R.
  (c) The function $\phi : R \to F \oplus F$ defined by $\phi\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\right) = (a, c)$ is a ring homomorphism with kernel I.

Answer: (a) We need to verify that R is closed under matrix addition and multiplication to show that R is a ring. Addition is obvious. For multiplication, we have

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} d & e \\ 0 & f \end{pmatrix} = \begin{pmatrix} ad & ae + bf \\ 0 & cf \end{pmatrix} \in R$$

(b) We need to see that I is closed under addition (which is clear), and that if $r \in R$ and $j \in I$, then $rj, jr \in I$. We have

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} 0 & d \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & ad \\ 0 & 0 \end{pmatrix} \in I$$
$$\begin{pmatrix} 0 & d \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} 0 & cd \\ 0 & 0 \end{pmatrix} \in I$$

(c) We have

$$\begin{aligned}
\phi\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} + \begin{pmatrix} d & e \\ 0 & f \end{pmatrix}\right) &= \phi\left(\begin{pmatrix} a+d & b+e \\ 0 & c+f \end{pmatrix}\right) = (a+d, c+f) = (a, c) + (d, f) \\
&= \phi\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\right) + \phi\left(\begin{pmatrix} d & e \\ 0 & f \end{pmatrix}\right) \\
\phi\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} d & e \\ 0 & f \end{pmatrix}\right) &= \phi\left(\begin{pmatrix} ad & ae + bf \\ 0 & cf \end{pmatrix}\right) = (ad, cf) = (a, c)(d, f) \\
&= \phi\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\right) \phi\left(\begin{pmatrix} d & e \\ 0 & f \end{pmatrix}\right)
\end{aligned}$$

These computations show that ϕ is a ring homomorphism. The kernel is the set of matrices so that $\phi\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\right) = 0$, meaning that $(a, c) = (0, 0)$, so $a = c = 0$, and then the kernel consists of matrices $\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$, which is exactly the definition of I.

2. Let p be a prime. Show that the polynomial $x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible in $\mathbf{Q}[x]$.
Answer: We know that $(x^n - 1)/(x - 1) = x^{n-1} + x^{n-2} + \cdots + x + 1$ for any n, so in particular $(x^p - 1)/(x - 1) = x^{p-1} + x^{p-2} + \cdots + x + 1$. Let $x = y + 1$, so $((y + 1)^p - 1)/y = (y + 1)^{p-1} + (y + 1)^{p-2} + \cdots + (y + 1) + 1$.

Now, $(y + 1)^p = y^p + \binom{p}{1} y^{p-1} + \binom{p}{2} y^{p-2} + \cdots py + 1$, and because $p \Big| \binom{p}{k}$ if $1 \le k \le p - 1$, we can apply the Eisenstein Criterion to see that $\frac{(y+1)^p - 1}{y}$ is irreducible. Therefore, our given polynomial is also irreducible.

3. Suppose that K and L are two fields, with $K \subset L$. Suppose that $\dim_K(L) = n$. Let $a \in K$. Show that there are elements $\alpha_0, \alpha_1, \ldots, \alpha_n$ of K, not all zero, so that $\sum_{k=0}^{n} \alpha_k a^k = 0$.
Answer: There are $n + 1$ elements in the set $\{1, a, a^2, \ldots, a^n\}$, so that set must be linearly dependent. Therefore, we can find a non-trivial linear combination of those elements which sums to 0.

4. Let F be a field, let $f(x) \in F[x]$ be an irreducible polynomial, and suppose $\deg(f) = n \ge 1$. Let $M = (f(x))$, and let $K = F[x]/M$. We know that K is a field containing F. Show that $\dim_F(K) = n$.
Answer: Given any elements $g(x) \in F[x]$, we know that we can write $g(x) = q(x)f(x) + r(x)$, where $r = 0$ or $\deg r < n$. Therefore, the coset $g(x) + M = r(x) + M$, and so any non-zero coset in $F[x]/M$ can be written as a polynomial of degree less than n. In other words, the n elements $\{1, x, \ldots, x^{n-1}\}$ span $F[x]/M$.

We now need to show linear independence. Suppose that $b_0 + b_1 x + \cdots + b_{n-1} x^{n-1} = 0 \in F[x]/M$ for some $b_0, b_1, \ldots, b_{n-1} \in F$. Let $g(x) = b_0 + b_1 x + \cdots + b_{n-1} x^{n-1}$. We have supposed that $g(x) \in M$.

We know that $f(x)$ is irreducible, so $(f, g) = 1$. Find polynomials $h, k \in F[x]$ so that $hf + kg = 1$. Then on the one hand, $hf + kg + M = 1 + M$ but on the other hand, $f \in M$ so $hf \in M$, and $g \in M$, so $kg \in M$, and then $hf + kg \in M$, implying that $1 \in M$, which is a contradiction.

Therefore, the set $\{1, x, \ldots, x^{n-1}\}$ is a basis of K over F, showing that $[K : F] = n$.

5. Suppose that F is a field, R is a ring, and $\phi : F \to R$ is a surjective ring homomorphism. Show that ϕ is a bijection, and that R is a field.
Answer: The only ideals of a field are 0 and F. We know that $\phi(1_F) = 1_R$, so the kernel of ϕ cannot be F. Therefore, the kernel is 0, and so ϕ is an injection. We are given that ϕ is a surjection, so it must be a bijection.

Now, if $r \in R$ is any non-zero element in R, we can find $s \in F$ so that $\phi(s) = r$ and $s \ne 0$, and then $\phi(s^{-1}) = r^{-1}$, showing that every non-zero element in R has an inverse.

6. Show that $\mathbf{R} \oplus \mathbf{R}$ is *not* ring isomorphic to $\mathbf{C}$.

Answer: Suppose that $\phi : \mathbf{R} \oplus \mathbf{R} \to \mathbf{C}$ is a ring isomorphism. The multiplicative identity element in $\mathbf{R} \oplus \mathbf{R}$ is $(1, 1)$, so we must have $\phi(1, 1) = 1$. We also have $\phi(0, 0) = 0$. Now, suppose that $\phi(1, 0) = a \in \mathbf{C}$, where $a \neq 0, 1$, because ϕ is an injection. But $\phi(1, 0) = \phi((1, 0)(1, 0)) = \phi(1, 0)^2 = a^2$, so we must have $a^2 = a$. The only solutions in $\mathbf{C}$ to $a^2 = a$ are $a = 0$ or $a = 1$. This is a contradiction.