Section 5.3

Problem # 14

Let D be the set of all real numbers of the form $m + n\sqrt{2}$, where $m, n \in \mathbb{Z}$. Carry out the construction of the quotient field Q for this integral domain, and show that this quotient field is isomorphic to the set of real numbers of the form $a + b\sqrt{2}$ where a and b are rational numbers.

Solution

Q is the set of all equivalence classes $[m + n\sqrt{2}, r + s\sqrt{2}]$ where $m + n\sqrt{2}, r + s\sqrt{2} \in D$ and r, s are not both equal to 0. Let T be the set of real numbers of the form $a + b\sqrt{2}$ where a and b are rational numbers. Consider the mapping $\phi : Q \to T$ defined by:

$$\phi([m + n\sqrt{2}, r + s\sqrt{2}]) = \frac{m + n\sqrt{2}}{r + s\sqrt{2}}$$

First we show that ϕ preserves addition.

$$\begin{aligned}\phi([m + n\sqrt{2}, r + s\sqrt{2}] + [a + b\sqrt{2}, c + d\sqrt{2}]) &= \phi([(r + s\sqrt{2})(a + b\sqrt{2}) + \\ &\quad (m + n\sqrt{2})(c + d\sqrt{2}), (r + s\sqrt{2})(c + d\sqrt{2})]) \\ &= \frac{(r + s\sqrt{2})(a + b\sqrt{2}) + (m + n\sqrt{2})(c + d\sqrt{2})}{(r + s\sqrt{2})(c + d\sqrt{2})} \\ &= \frac{m + n\sqrt{2}}{r + s\sqrt{2}} + \frac{a + b\sqrt{2}}{c + d\sqrt{2}} \\ &= \phi([m + n\sqrt{2}, r + s\sqrt{2}]) + \phi([a + b\sqrt{2}, c + d\sqrt{2}])\end{aligned} \tag{1}$$

Now we show that ϕ preserves multiplication.

$$\begin{aligned}\phi([m + n\sqrt{2}, r + s\sqrt{2}][a + b\sqrt{2}, c + d\sqrt{2}]) &= \phi([(m + n\sqrt{2})(a + b\sqrt{2}), (r + s\sqrt{2})(c + d\sqrt{2})]) \\ &= \frac{(m + n\sqrt{2})(a + b\sqrt{2})}{(r + s\sqrt{2})(c + d\sqrt{2})} \\ &= \frac{m + n\sqrt{2}}{r + s\sqrt{2}} \cdot \frac{a + b\sqrt{2}}{c + d\sqrt{2}} \\ &= \phi([m + n\sqrt{2}, r + s\sqrt{2}])\phi([a + b\sqrt{2}, c + d\sqrt{2}])\end{aligned} \tag{2}$$

Thus ϕ is a homomorphism. It is also onto, any element $\frac{a}{b} + \frac{c}{d}\sqrt{2}$ in T can is equal to $\frac{ad + bc\sqrt{2}}{bd} = \phi([ad + bc\sqrt{2}, cd + 0\sqrt{2}])$.

To show that ϕ is one to one suppose that $\phi([a+b\sqrt{2}, c+d\sqrt{2}]) = \phi([m+n\sqrt{2}, r+s\sqrt{2}]$. Then

$$\begin{aligned} \frac{a+b\sqrt{2}}{c+d\sqrt{2}} &= \frac{m+n\sqrt{2}}{r+s\sqrt{2}} \\ \implies (r+s\sqrt{2})(a+b\sqrt{2}) &= (c+d\sqrt{2})(m+n\sqrt{2}) \end{aligned} \tag{3}$$

so by the definition of equality in Q, $[a+b\sqrt{2}, c+d\sqrt{2}]$ and $[m+n\sqrt{2}, r+s\sqrt{2}]$ are equivalent and ϕ is an isomorphism.

Problem # 15

Let D be the Gaussian integers, the set of all complex numbers of the form $m+ni$, where $m \in \mathbb{Z}$ and $n \in \mathbb{Z}$. Carry out the construction of the quotient field Q for this integral domain and show that this quotient field is isomorphic to the set of all complex numbers of the form $a+bi$, where a and b are rational numbers.

Solution

Q is the set of all equivalence classes $[m+ni, r+si]$ where $m+ni, r+si \in D$ and r, s are not both equal to 0. Let T be the set of real numbers of the form $a+bi$ where a and b are rational numbers. Consider the mapping $\phi : Q \to T$ defined by:

$$\phi([m+ni, r+si]) = \frac{m+ni}{r+si}$$

First we show that ϕ preserves addition.

$$\begin{aligned} \phi([m+ni, r+si] + [a+bi, c+di]) &= \phi([(r+si)(a+bi) + (m+ni)(c+di), (r+si)(c+di)]) \\ &= \frac{(r+si)(a+bi) + (m+ni)(c+di)}{(r+si)(c+di)} \\ &= \frac{m+ni}{r+si} + \frac{a+bi}{c+di} \\ &= \phi([m+ni, r+si]) + \phi([a+bi, c+di]) \end{aligned} \tag{4}$$

Now we show that ϕ preserves multiplication.

$$\begin{aligned} \phi([m+ni, r+si][a+bi, c+di]) &= \phi([(m+ni)(a+bi), (r+si)(c+di)]) \\ &= \frac{(m+ni)(a+bi)}{(r+si)(c+di)} \\ &= \frac{m+ni}{r+si} \cdot \frac{a+bi}{c+di} \\ &= \phi([m+ni, r+si])\phi([a+bi, c+di]) \end{aligned} \tag{5}$$

Thus ϕ is a homomorphism. It is also onto, any element $\frac{a}{b} + \frac{c}{d}i$ in T can is equal to $\frac{ad+bci}{bd} = \phi([ad+bc\sqrt{i}, cd+0i])$.

To show that ϕ is one to one suppose that $\phi([a+bi, c+di]) = \phi([m+ni, r+si])$. Then

$$\begin{aligned} \frac{a+bi}{c+di} &= \frac{m+ni}{r+si} \\ \implies (r+si)(a+bi) &= (c+di)(m+ni) \end{aligned} \tag{6}$$

so by the definition of equality in Q, $[a+bi, c+di]$ and $[m+ni, r+si]$ are equivalent and ϕ is an isomorphism.

Problem # 17

Assume R is a ring, and let S be the set of all ordered pairs (m, x) where $m \in \mathbb{Z}$ and $x \in R$. Equality in S is defined by

$$(m, x) = (n, y) \text{ if and only if } m = n \text{ and } x = y$$

Addition and multiplication in S are defined by

$$(m, x) + (n, y) = (m+n, x+y)$$

and

$$(m, x) \cdot (n, y) = (mn, my + nx + xy),$$

where my and nx are *multiples* of y and x in the ring R.

(a) Prove that S is a ring with unity

(b) Prove that $\phi : R \to S$ defined by $\phi(x) = (0, x)$ is an isomorphism from R to a subring R' of S. This result shows that any ring can be embedded in a ring that has a unity.

Solution

Part (a)

In order to show S is a ring we first show that it is an abelian group under addition.

(a) Identity
The element $(0, 0_R)$ where 0_R is the additive identity in R is the identity element in $(S, +)$. $(m, x) + (0, 0_R) = (m, x) = (0, 0_R) + (m, x)$.

(b) Closed
$(m, x) + (n, y) = (m+n, x+y)$. R and $\mathbb{Z}$ are both closed under addition so the result is an element of S and S is closed under addition.

(c) Inverses
We know that both R and $\mathbb{Z}$ contain inverses so $-(m, x) = (-m, -x)$. $(m, x) + (-m, -x) = (0, 0_R) = (-m, -x) + (m, x)$.

(d) Commutative
We know R and $\mathbb{Z}$ are commutative with respect to addition so $(m, x) + (n, y) = (m+n, x+y) = (n+m, y+x) = (n, y) + (m, x)$.

Now we show that the distributive laws hold in S.

$$\begin{aligned}(m,x)[(n,y)+(s,z)] &= (m,x)(n+s,y+z)\\ &= (m(n+s),m(y+z)+(n+s)x+x(y+z))\\ &= (mn+ms,my+mz+nx+sx+xy+xz)\\ &= (mn,my+nx+xy)+(ms,mz+sx+xz)\\ &= (m,x)(n,y)+(m,x)(s,z)\end{aligned} \tag{7}$$

$$\begin{aligned}[(n,y)+(s,z)](m,x) &= (n+s,y+z)(m,x)\\ &= ((n+s)m,(y+z)m+x(n+s)+(y+z))x\\ &= (nm+sm,ym+zm+xn+xs+yx+zx)\\ &= (nm,ym+xn+yx)+(sm,zm+xs+zx)\\ &= (n,y)(m,x)+(s,z)(m,x)\end{aligned} \tag{8}$$

Finally we show that S is closed under an associative multiplication.

$$(m,x)\cdot(n,y) = (mn,my+nx+ny)$$

The integers are closed under multiplication so $mn \in \mathbb{Z}$ and R is closed under repeated addition so $my+nx+ny \in R$ and $(mn,my+nx+ny) \in S$.

$$\begin{aligned}[(m,x)(n,y)](s,z) &= (mn,my+nx+xy)\\ &= (mns,mnz+s(my+nx+xy)+(my+nx+xy)z)\\ &= (mns,mnz+smy+snx+sxy+myz+nxz+xyz)\\ &= (mns,mnz+msy+myz+nsx+xnz+xsy+xyz)\end{aligned} \tag{9}$$

Thus S is a ring under addition and multiplication defined as given. S has the unity $(1,0)$. $(m,x)(1,0)=(m,x)=(1,0)(m,x)$.

Part (b)

R' is clearly nonempty. For two elements $(0,x),(0,y) \in R'$, $(0,x)+(0,y)=(0,x+y) \in R'$ and $(0,x)(0,y)=(0,0) \in R'$. To show that the mapping is one to one consider elements $x,y \in R$ such that $\phi(x)=\phi(y)$. Then $(0,x)=(0,y)$ and $x=y$ by the definition of equality in R'. It is clear that the mapping is onto. For any $(0,x) \in R'$, $\phi(x)=(0,x)$ where x is an element in R.
Thus the two rings are isomorphic.

Section 6.1

Problem # 17

In the ring $\mathbb{Z}$ of integers, prove that every subring is an ideal.

Solution

For a subring I of $\mathbb{Z}$, in order to show that I is an ideal, we need to show that for any $x \in I$ and$r \in R$, xr and rx are in I.
If $r = 0$, $rx = xr = 0 \in I$. If $r > 0$ then, beacuse multiplication is simply repeated addition $rx = xr = x + x + \cdots + x$ for r terms. I is closed under addition so the result is in I. If $r < 0$ then $rx = xr = (-x) + (-x) + \cdots + (-x)$ for r terms. I is closed under addition and $-x \in I$ so the result is in I. Thus I is an ideal in $\mathbb{Z}$.

Problem # 18

Let $a \neq 0$ in the ring of integers $\mathbb{Z}$. Find $b \in \mathbb{Z}$ such that $a \neq b$ but $(a) = (b)$.

Solution

$$b = -a$$

Problem # 19

Let m and n be nonzero integers. Prove that $(m) \subseteq (n)$ if and only if n divides m.

Solution

First assume that $(m) \subseteq (n)$. Then every multiple of m is also a multiple of n. In particular, $1 \cdot m = nq$ for some integer q. Thus n divides m.
Now assume that n divides m. Then m can be written as nq for some integer q and every multiple km of m can be written as knq. Thus every multiple of m is also a multiple of n and $(m) \subseteq (n)$.

Problem # 20

If a and b are nonzero integers and m is the least common multiple of a and b, prove that $(a) \cap (b) = (m)$.

Solution

m is a multiple of both a and b so it can be written as as or bt for some integers s, t. Then any multiple km of m for some integer k can be written as ask or tbk. Thus $(m) \subseteq (a) \cap (b)$. By definition every number that is a multiple of both a and b must be a multiple of the least common multiple of a and b so $(a) \cap (b) \subseteq (m)$. So $(a) \cap (b) = (m)$.

Section 6.2

Problem # 18

Let $\theta : M_2(\mathbb{Z}) \to \mathbb{Z}$ where $M_2(\mathbb{Z})$ is the ring of 2×2 matrices over the integers $\mathbb{Z}$. Prove or disprove that each of the following mappings is a homomorphism.

(a)

$$\phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = ad - bc$$

(b)

$$\theta\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = a + d$$

(This mapping is the **trace** of the matrix.)

Solution

Part (a)

$$\phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix}\right) = \phi\left(\begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix}\right) = (a+e)(d+h) - (b+f)(c+g)$$

this is not equal to

$$\phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) + \phi\left(\begin{bmatrix} e & f \\ g & h \end{bmatrix}\right) = ad - bc + eh - fg$$

So it is not a homomorphism.

Part (b)

$$\theta\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} e & f \\ g & h \end{bmatrix}\right) = \theta\left(\begin{bmatrix} ae+bg & fa+bh \\ ec+gd & gc+dh \end{bmatrix}\right) = ae + bg + fc + dh$$

this is not equal to

$$\theta\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right)\theta\left(\begin{bmatrix} e & f \\ g & h \end{bmatrix}\right) = (a+d)(e+h)$$

So it is not a homomorphism.

Problem # 19

Assume that

$$R = \{\begin{bmatrix} m & 2n \\ n & m \end{bmatrix} \mid m, n \in \mathbb{Z}\}$$

and

$$R' = \{m + n\sqrt{2} \mid m, n \in \mathbb{Z}\}$$

are rings with respect to their usual operations, and prove that R and R' are isomorphic rings.

Solution

Consider the mapping $\phi : R \to R'$ defined by $\phi\left(\begin{bmatrix} a & 2b \\ b & a \end{bmatrix}\right) = a + b\sqrt{2}$. This mapping is clearly onto. Consider $\begin{bmatrix} a & 2b \\ b & a \end{bmatrix}$ and $\begin{bmatrix} c & 2d \\ d & c \end{bmatrix}$ such that $\phi\left(\begin{bmatrix} a & 2b \\ b & a \end{bmatrix}\right) = \phi\left(\begin{bmatrix} c & 2d \\ d & c \end{bmatrix}\right)$. This means that $a + b\sqrt{2} = c + d\sqrt{2}$ and $a = c + (d - b)\sqrt{2}$. a must be an integer and a nonzero rational number times an irrational number is irrational. Thus $d - b = 0$ and $d = b$. This implies that $a = c$ and so the two matrices are equal and ϕ is one to one.

$$\theta\left(\begin{bmatrix} a & 2b \\ b & a \end{bmatrix} + \begin{bmatrix} c & 2d \\ d & c \end{bmatrix}\right) = \theta\left(\begin{bmatrix} a+c & 2(b+d) \\ b+d & a+c \end{bmatrix}\right) = (a+c) + (b+d)\sqrt{2}$$

this is equal to

$$\theta\left(\begin{bmatrix} a & 2b \\ b & a \end{bmatrix}\right) + \theta\left(\begin{bmatrix} c & 2d \\ d & c \end{bmatrix}\right) = (a + b\sqrt{2}) + (c + d\sqrt{2})$$

So the mapping preserves the addition operation.

$$\theta\left(\begin{bmatrix} a & 2b \\ b & a \end{bmatrix}\begin{bmatrix} c & 2d \\ d & c \end{bmatrix}\right) = \theta\left(\begin{bmatrix} ca + 2bd & 2(da + bc) \\ da + bc & ca + 2bd \end{bmatrix}\right) = (ca + 2bd) + (da + bc)\sqrt{2}$$

this is equal to

$$\theta\left(\begin{bmatrix} a & 2b \\ b & a \end{bmatrix}\right)\theta\left(\begin{bmatrix} c & 2d \\ d & c \end{bmatrix}\right) = (a + b\sqrt{2})(c + d\sqrt{2}) = (ca + 2bd) + (da + bc)\sqrt{2}$$

So the mapping also preserves multiplication. Thus θ is a ring isomorphism and R and R' are isomorphic.

Section 8.1

Problem # 12

(a) Find a nonconstant polynomial in $\mathbb{Z}_4[x]$, if one exists, that is a unit.

(b) Find a nonconstant polynomial in $\mathbb{Z}_3[x]$, if one exists, that is a unit.

(c) Prove or disprove that there exist nonconstant polynomials in $\mathbb{Z}_p[x]$ that are units if p is prime.

Solution

Part (a)

$$2x + 1$$

Part (b)

No such element exists.

Part (c)

When p is prime $\mathbb{Z}_p$ is an integral domain. In an integral domain for two polynimials $f(x)$ and $g(x)$, $\deg f(x)g(x) = \deg f(x) + \deg g(x)$. Then in order for their product to be the unity, both $f(x)$ and $g(x)$ must be constant polynomials.

Problem # 20

Consider the mapping $\phi : \mathbb{Z}[x] \to \mathbb{Z}_k[x]$ defined by

$$\phi(a_0 + a_1x + \cdots + a_nx^n) = [a_0] + [a_1]x + \cdots + [a_n]x^n,$$

where $[a_i]$ denotes the congruence class of $\mathbb{Z}_k$ that contains a_i. Prove that ϕ is an epimorphism from $\mathbb{Z}[x]$ to $\mathbb{Z}_k[x]$.

Solution

It is clear that the mapping is onto. We must show that it's a homomorphism. We can assume without loss of generality that n is at least as large as k in the following example.

$$\begin{aligned}\phi(a_0 + a_1x + \ldots + a_nx^n + b_0 + b_1 + \ldots + b_k) &= \phi((a_0 + b_0) + (a_1 + b_1)x + \ldots (a_n + b_n)x^n) \\ &= [a_0 + b_0] + [a_1 + b_1]x + \ldots + [a_n + b_n]x^n \\ &= [a_0] + [b_0] + ([a_1] + [b_1])x + \ldots + ([a_n] + [b_n])x^n \\ &= [a_0] + [a_1]x + \ldots + [a_n]x^n + [b_0] + [b_1]x + \ldots + [b_k]^k \\ &= \phi(a_0 + a_1 + \ldots + a_n) + \phi(b_0 + b_1 + \ldots + b_n)\end{aligned} \tag{10}$$

Thus ϕ preserves addition. Now consider what it looks like when two elements are multiplied together.

$$\begin{aligned}\phi((\sum_{i=1}^{n} a_i x_i)(\sum_{j=1}^{n} b_j x_j)) &= \phi(\sum_{i,j=1}^{n} a_i b_j x^{i+j}) \\ &= \sum_{i,j=1}^{n} \phi(a_i)\phi(b_j)x^{i+j}\end{aligned} \tag{11}$$

So ϕ preserves multiplication and ϕ is an epimorphism.

Section 8.2

Problem # 26

Prove that if $d_1(x)$ and $d_2(x)$ are monic polynomials over the field F such that $d_1(x) \mid d_2(x)$ and $d_2(x) \mid d_1(x)$, then $d_1(x) = d_2(x)$.

Solution

If $d_1(x) \mid d_2(x)$ then $d_2(x)$ can be written as $q_1(x)d_1(x)$ for some polynomial $q_1(x)$. Similarly, because $d_2(x) \mid d_1(x), d_1(x)$ can be written as $q_2(x)d_2(x)$ for some polynomial $q_2(x)$. Then $d_1(x) = q_1(x)q_2(x)d_1(x)$. F is an integral domain so $\deg(q_1(x)q_2(x)) = \deg(q_1(x)) + \deg(q_2(x))$. Thus $q_1(x)$ and $q_2(x)$ must both be constants. In fact, because $d_1(x)$ and $d_2(x)$ are monic, they must both be one. Then

$$d_1(x) = q_2(x)d_2(x) = 1 \cdot d_2(x) = d_2(x)$$

Problem # 29

Let $f(x), g(x), h(x) \in F[x]$. Prove that if $f(x) \mid g(x)$ and $g(x) \mid h(x)$ then $f(x) \mid h(x)$.

Solution

If $f(x) \mid g(x)$ and $g(x) \mid h(x)$ then $g(x) = f(x)q_1(x)$ for some polynomial $q_1(x) \in F[x]$ and $h(x) = q_2(x)g(x)$ for some polynomial $q_2(x) \in F[x]$. Then $h(x) = q_2(x)q_1(x)f(x)$ and $f(x) \mid h(x)$.

Section 8.3

Problem # 12

Find all the zeros of each of the following polynomials over the indicated fields.

(a) $x^5 - x$ over $\mathbb{Z}_5$

(b) $x^{11} - x$ over $\mathbb{Z}_{11}$

Solution

Part (a)

The zeros of the polynomial over $\mathbb{Z}_5$ are:

$$[0], [1], [2], [3], [4]$$

Part (b)

The zeros of the polynomial over $\mathbb{Z}_{11}$ are:

$$[0], [1], [2], [3], [4], [5], [6], [7], [8], [9], [10]$$

Problem # 13

Give an example of a polynomial ofdegree 4 over the field $\mathbb{R}$ of real numbers that is reducible over $\mathbb{R}$ and yet has no zeros in the real numbers.

Solution

$$x^4 + 1$$