Math 331: HW 5 Solutions
Tuesday, 3 Oct 2006

3.3: 2, 13, 23; 4.1: 5bd, 12;

3.3.2 Use tables to show that $\mathbb{Z}_2 \times \mathbb{Z}_2$ is isomorphic to the ring R of Exercise 2 in Section 3.1.

We first construct the addition and multiplication tables for $\mathbb{Z}_2 \times \mathbb{Z}_2$.

$+$	(0, 0)	(1, 1)	(1, 0)	(0, 1)
(0, 0)	(0, 0)	(1, 1)	(1, 0)	(0, 1)
(1, 1)	(1, 1)	(0, 0)	(0, 1)	(1, 0)
(1, 0)	(1, 0)	(0, 1)	(0, 0)	(1, 1)
(0, 1)	(0, 1)	(1, 0)	(1, 1)	(0, 0)

$\cdot$	(0, 0)	(1, 1)	(1, 0)	(0, 1)
(0, 0)	(0, 0)	(0, 0)	(0, 0)	(0, 0)
(1, 1)	(0, 0)	(1, 1)	(1, 0)	(0, 1)
(1, 0)	(0, 0)	(1, 0)	(1, 0)	(0, 0)
(0, 1)	(0, 0)	(0, 1)	(0, 0)	(0, 1)

Under the following bijection $\mathbb{Z}_2 \times \mathbb{Z}_2 \to \{0, e, b, c\}$

$$(0,0) \mapsto 0, \quad (1,1) \mapsto e, \quad (1,0) \mapsto b, \quad (0,1) \mapsto c$$

the addition and multiplication tables become:

$+$	0	e	b	c
0	0	e	b	c
e	e	0	c	b
b	b	c	0	e
c	c	b	e	0

$\cdot$	0	e	b	c
0	0	0	0	0
e	0	e	b	c
b	0	b	b	0
c	0	c	0	c

These are precisely the tables used to construct the ring R of Exercise 2 in Section 3.1. Hence, $\mathbb{Z}_2 \times \mathbb{Z}_2$ is isomorphic to the ring R. ◆

3.3.13 Let $f : R \to S$ be a homomorphism of rings. If r is a zero divisor in R, is $f(r)$ a zero divisor in S?

Not necessarily; consider the homomorphism $f : \mathbb{Z}_4 \to \mathbb{Z}_2$ given by $f([a]_4) = [a]_2$. Then $[2]_4$ is a zero divisor in $\mathbb{Z}_4$ (since $[2]_4 \neq 0$ and $[2]_4[2]_4 = [4]_4 = 0$) but $f([2]_4) = [2]_2 = 0$ is not a zero divisor in $\mathbb{Z}_2$. ◆

3.3.23 Let L be the ring of all matrices of the form $\left(\begin{smallmatrix} a & 0 \\ b & c \end{smallmatrix}\right)$. Show that the function $f : L \to \mathbb{Z}$ given by $f\left(\begin{smallmatrix} a & 0 \\ b & c \end{smallmatrix}\right) = a$ is a surjective homomorphism but not an isomorphism.

We first show that f is a homomorphism. We must verify that the definition (on page 71) is satisfied. Let $x, y \in L$ be given. Then there exist $a, b, c, d, e, f \in \mathbb{Z}$ so that $x = \left(\begin{smallmatrix} a & 0 \\ b & c \end{smallmatrix}\right)$ and $y = \left(\begin{smallmatrix} d & 0 \\ e & f \end{smallmatrix}\right)$. Note that by the definition of f we have $f(x) = a$ and $f(y) = d$. Hence, by the usual rules of matrix arithmetic and the definition of f

$$f(x+y) = f\Big(\left(\begin{smallmatrix} a & 0 \\ b & c \end{smallmatrix}\right) + \left(\begin{smallmatrix} d & 0 \\ e & f \end{smallmatrix}\right)\Big) = f\left(\begin{smallmatrix} a+d & 0 \\ b+e & c+f \end{smallmatrix}\right) = a + d = f(x) + f(y),$$

$$f(xy) = f\Big(\left(\begin{smallmatrix} a & 0 \\ b & c \end{smallmatrix}\right)\left(\begin{smallmatrix} d & 0 \\ e & f \end{smallmatrix}\right)\Big) = f\left(\begin{smallmatrix} ad & 0 \\ bd+ce & cf \end{smallmatrix}\right) = ad = f(x)f(y).$$

Note that f is surjective: let $a \in \mathbb{Z}$ be given; then $a = f\left(\begin{smallmatrix} a & 0 \\ 0 & 0 \end{smallmatrix}\right)$. But f is not injective since

$$f\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) = 1 = f\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \quad \text{but} \quad \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \neq \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right).$$

Thus, f is not an isomorphism. ◆

4.1.5 Find polynomials $q(x)$ amd $r(x)$ such that $f(x) = g(x)q(x) + r(x)$, and $r(x) = 0$ or $\deg r(x) < \deg g(x)$:

(b) $f(x) = x^4 - 7x + 1$ and $g(x) = 2x^2 + 1$ in $\mathbb{Q}[x]$.

Using long division in $\mathbb{Q}[x]$ one obtains $q(x) = \frac{1}{2}x^2 - \frac{1}{4}$ and $r(x) = -7x + \frac{5}{4}$. ◆

(d) $f(x) = 4x^4 + 2x^3 + 6x^2 + 4x + 5$ and $g(x) = 3x^2 + 2$ in $\mathbb{Z}_7[x]$.

Note that $3 \cdot 5 = 1$ in $\mathbb{Z}_7$. Using long division in $\mathbb{Z}_7[x]$ one obtains $q(x) = 6x^2 + 3x + 5$ and $r(x) = 5x + 2$. ◆

4.1.12 Let F be a field and let $f(x)$ be a nonzero polynomial in $F[x]$. Show that $f(x)$ is a unit in $F[x]$ if and only if $\deg f(x) = 0$.

Note first that F is an integral domain by Theorem 3.9. Suppose that $f(x)$ is a unit in $F[x]$. Then there is a nonzero polynomial $g(x)$ in $F[x]$ such that $f(x)g(x) = 1$. Then by Theorem 4.2, we have

$$\deg f(x) + \deg g(x) = \deg[f(x)g(x)] = \deg 1 = 0.$$

Then since $\deg f(x), \deg g(x) \geq 0$, we must have $\deg f(x) = 0$.

Conversely, suppose that $\deg f(x) = 0$. Then $f(x)$ is a constant polynomial, say $f(x) = a$ for some $a \in F \subseteq F[x]$. Then since $a \neq 0$ and F is a field a has a multiplicative inverse, a^{-1}. Recall that F is a subring of $F[x]$ (and $1_F = 1_{F[x]}$). Setting $g(x) = a^{-1}$, we have (noting that $F[x]$ is commutative):

$$g(x)f(x) = f(x)g(x) = aa^{-1} = 1.$$

Hence, $f(x)$ is a unit in $F[x]$. ◆