Homework 8
Abstract Algebra
Math 320
Stephen Giang

Section 3.3 Problem 19: $S = \{0, 4, 8, 12, 16, 20, 24\}$ is a subring of $\mathbb{Z}_{28}$. Prove that the map $f : \mathbb{Z}_7 \to S$ given by $f([x]_7) = [8x]_{28}$ is an isomorphism.

Let $S = \{0, 4, 8, 12, 16, 20, 24\}$ be a subring of $\mathbb{Z}_{28}$. Notice:

$$\begin{aligned} f([0]_7) &= [0]_{28} \\ f([1]_7) &= [8]_{28} \\ f([2]_7) &= [16]_{28} \\ f([3]_7) &= [24]_{28} \\ f([4]_7) &= [32]_{28} = [4]_{28} \\ f([5]_7) &= [40]_{28} = [12]_{28} \\ f([6]_7) &= [48]_{28} = [20]_{28} \end{aligned}$$

Because for all x in $\mathbb{Z}_7$, f maps x to a unique y in S, f is injective. Because for all y in S, there exists an x in $\mathbb{Z}_7$ such that f maps x to y, f is also surjective, thus being bijective.

Let $x_1, x_2 \in \mathbb{Z}_7$

$$\begin{aligned} f(x_1) + f(x_2) &= [8x_1]_{28} + [8x_2]_{28} = [8(x_1 + x_2)]_{28} = f(x_1 + x_2) \\ f(x_1)f(x_2) &= [8x_1]_{28} \times [8x_2]_{28} = [64]_{28}[x_1x_2]_{28} = [8]_{28}[x_1x_2]_{28} \\ &= [8(x_1x_2)]_{28} = f(x_1x_2) \end{aligned}$$

This shows that f is a homomorphism.

Thus f is an isomorphism.

Section 3.3 Problem 21: Let $\mathbb{Z}^*$ denote the ring of integers with the $\oplus$ and $\odot$ operations defined as:

$$a \oplus b = a + b - 1$$
$$a \odot b = a + b - ab$$

Prove that $\mathbb{Z}$ is isomorphic to $\mathbb{Z}^*$.

Let $f : \mathbb{Z} \to \mathbb{Z}^*$ such that $f(x) = 1 - x$, with $x \in \mathbb{Z}$

Let $\exists x_1, x_2 \in \mathbb{Z}$, such that $f(x_1) = f(x_2)$

$$f(x_1) = 1 - x_1 = 1 - x_2 = f(x_2).$$

Thus $x_1 = x_2$, proving that f maps x to a unique y in $\mathbb{Z}^*$, which proves injectivity.

Let $y \in \mathbb{Z}^*$

$$y = 1 - x = f(x) \qquad \text{f.s } x \in \mathbb{Z}$$

Because for all $y \in \mathbb{Z}^*$, y can be written as a function of f, this proves surjectivity.

Let $a, b \in \mathbb{Z}$

$$\begin{aligned} f(a) \oplus f(b) &= (1 - a) + (1 - b) - 1 \\ &= 2 - a - b - 1 = 1 - (a + b) = f(a + b) \\ f(a) \odot f(b) &= (1 - a) + (1 - b) - (1 - a)(1 - b) \\ &= 2 - (a + b) - 1 + (a + b) - ab = 1 - ab = f(ab) \end{aligned}$$

This shows that f is a homomorphism.

Thus f is an isomorphism, with $\mathbb{Z}$ being isomorphic to $\mathbb{Z}^*$.

Section 4.1 Problem 5 (d): Find Polynomials $q(x)$ and $r(x)$ such that $f(x) = g(x)q(x) + r(x)$, and $r(x) = 0$ or deg $r(x) <$ deg $g(x)$:

$$
\begin{aligned}
f(x) &= 4x^4 + 2x^3 + 6x^2 + 4x + 5 \\
g(x) &= 3x^2 + 2
\end{aligned}
$$

with $f(x), g(x) \in \mathbb{Z}_7[x]$

$$
\begin{array}{r}
\frac{4}{3}x^2 + \frac{2}{3}x + \frac{10}{9} \\
3x^2 + 2 \overline{\big)\, 4x^4 + 2x^3 + 6x^2 + 4x + 5} \\
-(4x^4 + \qquad + \frac{8}{3}x^2) \\
\hline
2x^3 + \frac{10}{3}x^2 + 4x + 5 \\
-(2x^3 + \qquad + \frac{4}{3}x) \\
\hline
\frac{10}{3}x^2 + \frac{8}{3}x + 5 \\
-(\frac{10}{3}x^2 + \qquad + \frac{20}{9}) \\
\hline
\frac{8}{3}x + \frac{25}{9}
\end{array}
$$

$$
\begin{aligned}
q(x) &= 4(3^{-1})x^2 + 2(3^{-1})x + 10(9^{-1}) \\
r(x) &= 8(3^{-1})x + 25(9^{-1})
\end{aligned}
$$

Notice: Because the polynomials are in $\mathbb{Z}_7[x]$, $3^{-1} = 5$ and $9^{-1} = 4$

$$
\begin{aligned}
q(x) &= 4(5)x^2 + 2(5)x + 10(4) \\
&= 20x^2 + 10x + 40 \\
&= 6x^2 + 3x + 5 \\
r(x) &= 8(5)x + 25(4) \\
&= 40x + 100 \\
&= 5x + 2
\end{aligned}
$$

Section 4.1 Problem 18: Let $\phi : R[x] \to R$ be the function that maps each polynomial in $R[x]$ onto its constant term (an element of R). Show that ϕ is a surjective homomorphism of rings.

Let $\phi(f(x)) = \phi(ax^n + ... + C) = C$

Let $c \in R$

$$c = \phi(ax^n + ... + c)$$

Because for all $c \in R$, there exists a polynomial in which $c = \phi(ax^n + ... + c)$, thus $\phi(f(x)) = c$ is surjective.

Let $a, b \in R[x]$, with $ax^n + ... + c_1$ and $bx^m + ... + c_2$

$$\phi(a+b) = \phi(ax^n + bx^m + ... + (c_1 + c_2)) = c_1 + c_2 = \phi(a) + \phi(b)$$
$$\phi(ab) = \phi(abx^{n+m} + ... + c_1c_2) = c_1c_2 = \phi(a)\phi(b)$$

This proves that ϕ is a surjective homomorphism of rings.

Section 4.1 Problem 20: Let $D : R[x] \to R[x]$ be the derivative map defined by

$$D(a_0 + a_1x + ... + a_nx^n) = a_1 + ... + na_nx^{n-1}$$

Is D a homomorphism of rings? An isomorphism?

Notice:

$$D(x)D(x^2+1) = 1(2x) = 2x \neq 3x^2 + 1 = D(x(x^2+1))$$

Because D is not a homomorphism, as it does not hold for multiplication of polynomials, D is also not an isomorphism.

Section 4.2 Problem 14: Let $f(x)g(x)h(x) \in F[x]$, with $f(x)$ and $g(x)$ relatively prime. If $f(x)|h(x)$ and $g(x)|h(x)$, prove that $f(x)g(x)|h(x)$

Let $f(x), g(x), h(x), u(x), v(x), w(x) \in F[x]$. Assume $f(x)|h(x)$ and $g(x)|h(x)$, and $f(x)$ and $g(x)$ relatively prime.

$$h(x) = f(x)u(x) = g(x)v(x)$$

Now we can see that $f(x)|g(x)v(x)$. Because $f(x)$ and $g(x)$ relatively prime, we know that $f(x)|v(x)$

$$\begin{aligned} v(x) &= f(x)w(x) \\ h(x) &= g(x)v(x) = g(x)f(x)w(x) \end{aligned}$$

Thus $f(x)g(x)|h(x)$.