Assignment Nine

Lizzy Hunt

March 27, 2023

1 Section 5.1

1.1 Question One

1.1.1 b

Yes. In F, $f(x) - g(x) = -x^3 + x = x^3 + x$.

$$\begin{array}{r} x \\ \hline x^2+1\big) \;\; x^3 + x \\ -x^3 - x \\ \hline 0 \end{array}$$

1.1.2 c

No. $f(x) - g(x) = x^5 - 2x^4 + 4x^3 - 8x^2 + 3x - 2$

$$
\begin{array}{r}
\multicolumn{2}{r}{x^2 \;\; - x + 2} \\
\cline{2-2}
x^3 - x^2 + x - 1 \big) & x^5 - 2x^4 + 4x^3 - 8x^2 + 3x - 2 \\
& \underline{- x^5 \;\; + x^4 \;\; - x^3 \;\; + x^2} \\
& \quad - x^4 + 3x^3 - 7x^2 + 3x \\
& \quad \underline{x^4 \;\; - x^3 \;\; + x^2 \;\; - x} \\
& \qquad 2x^3 - 6x^2 + 2x - 2 \\
& \qquad \underline{- 2x^3 + 2x^2 - 2x + 2} \\
& \qquad\quad - 4x^2
\end{array}
$$

1.2 Question Three

$|\{\ 0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\ \}| = 8$

1.3 Question Four

For every $a, b, c \in \mathbb{Z}_3$ we can generate a polynomial $ax^2 + bx + c$, by part two of Corollary 5.5. $3^3 = 27$

1.4 Question Six

By Corollary 5.5, all the congruence classes in $F[x]$ are $c \ni c \in F$.

1.5 Question Eight

$$
\begin{aligned}
f(x)k(x) &\equiv_{p(x)} g(x)k(x) \\
&\Rightarrow p(x) | f(x)k(x) - g(x)k(x) \\
&\Rightarrow p(x) | (f(x) - g(x))(k(x))
\end{aligned}
$$

By Theorem 4.10, since $p(x)$ is relatively prime to $k(x)$, $p(x)|f(x) - g(x) \Rightarrow f(x) \equiv_{p(x)} g(x)$

1.6 Question Eleven

Since $p(x)$ is reducible, it can be rewritten as $p(x) = f(x)g(x)$ with $f(x), g(x) \in F[x]$ with each $f(x)$ and $g(x)$ having a degree greater than 0, summing to the degree of $p(x)$.
Then, it is impossible for $p(x)$ to divide $f(x)$ or $g(x)$ since $p(x)$ has a higher degree. So, neither $f(x)$ or $g(x)$ can \$ $\equiv_{p(x)} 0_F$\$.
Still, $f(x)g(x) \equiv_{p(x)} p(x) \equiv_{p(x)} 0_F$ since $p(x)|p(x)$.

2 Section 5.2

2.1 Question One

The congruence classes are those in Section 5.1, Question Three as above.

+	[0]	[1]	[x]	[x + 1]	[x^2]	[x^2 + 1]	[x^2 + x]	[x^2 + x + 1]
[0]	[0]	[1]	[x]	[x + 1]	[x^2]	[x^2 + 1]	[x^2 + x]	[x^2 + x + 1]
[1]	[1]	[0]	[x+1]	[x]	[x^2 + 1]	[x^2]	[x^2 + x + 1]	[x^2 + x]
[x]	[x]	[x + 1]	[0]	[1]	[x^2 + x]	[x^2 + x + 1]	[x^2]	[x^2 + 1]
[x + 1]	[x + 1]	[x]	[1]	[0]	[x^2 + x + 1]	[x^2 + x]	[x^2 + 1]	[x^2]
[x^2]	[x^2]	[x^2 + 1]	[x^2 + x]	[x^2 + x + 1]	[0]	[1]	[x]	[x + 1]
[x^2 + 1]	[x^2 + 1]	[x^2]	[x^2 + x + 1]	[x^2 + x]	[1]	[0]	[x + 1]	[x]
[x^2 + x]	[x^2 + x]	[x^2 + x + 1]	[x^2]	[x^2 + 1]	[x]	[x+1]	[0]	[1]
[x^2 + x + 1]	[x^2 + x + 1]	[x^2 + x]	[x^2 + 1]	[x^2]	[x+1]	[x]	[1]	[0]

.	[0]	[1]	[x]	[x + 1]	[x^2]	[x^2 + 1]	[x^2 + x]	[x^2 + x + 1]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[x]	[x + 1]	[x^2]	[x^2 + 1]	[x^2 + x]	[x^2 + x + 1]
[x]	[0]	[x]	[x^2]	[x^2+x]	[x+1]	[1]	[x^2+x+1]	[x^2+1]
[x + 1]	[0]	[x + 1]	[x^2 + x]	[x^2+1]	[x^2+x+1]	[x^2]	[1]	[x]
[x^2]	[0]	[x^2]	[x+1]	[x^2+x+1]	[x^2+x]	[x]	[x^2+1]	[1]
[x^2 + 1]	[0]	[x^2 + 1]	[1]	[x^2]	[x]	[x^2+x+1]	[x+1]	[x^2+x]
[x^2 + x]	[0]	[x^2 + x]	[x^2+x+1]	[1]	[x^2+1]	[x+1]	[x]	[x+1]
[x^2 + x + 1]	[0]	[x^2 + x + 1]	[x^2+1]	[x]	[1]	[x^2+x]	[x^2]	[x+1]

Yes, this is a field since by Theorem 5.7, it is a commutative ring with identity, and each non-zero row in the multiplication table contains the multiplicative identity (each is a unit).

2.2 Question Two

+	[0]	[1]	[2]	[x]	[x+1]	[x+2]	[2x]	[2x+1]	[2x+2]
[0]	[0]	[1]	[2]	[x]	[x+1]	[x+2]	[2x]	[2x+1]	[2x+2]
[1]	[1]	[2]	[0]	[x+1]	[x+2]	[x]	[2x+1]	[2x+2]	[2x]
[2]	[2]	[0]	[1]	[x+2]	[x]	[x+1]	[2x+2]	[2x]	[2x+1]
[x]	[x]	[x+1]	[x+2]	[2x]	[2x+1]	[2x+2]	[0]	[1]	[2]
[x+1]	[x+1]	[x+2]	[x]	[2x+1]	[2x+2]	[2x]	[1]	[2]	[0]
[x+2]	[x+2]	[x]	[x+1]	[2x+2]	[2x]	[2x+1]	[2]	[0]	[1]
[2x]	[2x]	[2x+1]	[2x+2]	[0]	[1]	[2]	[x]	[x+1]	[1]
[2x+1]	[2x+1]	[2x+2]	[2x]	[1]	[2]	[0]	[x+1]	[x+2]	[x]
[2x+2]	[2x+2]	[2x]	[2x+1]	[2]	[0]	[1]	[x+2]	[x]	[x+1]

·	[0]	[1]	[2]	[x]	[x+1]	[x+2]	[2x]	[2x+1]	[2x+2]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[x]	[x+1]	[x+2]	[2x]	[2x+1]	[2x+2]
[2]	[0]	[2]	[1]	[2x]	[2x+2]	[2x+1]	[x]	[x+2]	[x+1]
[x]	[0]	[x]	[2x]	[2]	[x+2]	[2x+2]	[1]	[x+1]	[2x+1]
[x+1]	[0]	[x+1]	[2x+2]	[x+2]	[2x]	[1]	[2x+1]	[2]	[x]
[x+2]	[0]	[x+2]	[2x+1]	[2x+2]	[1]	[x]	[x+1]	[2x]	[2]
[2x]	[0]	[2x]	[x]	[1]	[2x+1]	[x+1]	[2]	[2x+2]	[x+2]
[2x+1]	[0]	[2x+1]	[x+2]	[x+1]	[2]	[2x]	[2x+2]	[x]	[1]
[2x+2]	[0]	[2x+2]	[x+1]	[2x+1]	[x]	[2]	[x+2]	[1]	[2x]

Yes, this is a field since by Theorem 5.7, it is a commutative ring with identity, and each non-zero row in the multiplication table contains the multiplicative identity (each is a unit).

2.3 Question Three

+	[0]	[1]	[x]	[x+1]
[0]	[0]	[1]	[x]	[x+1]
[1]	[1]	[0]	[x+1]	[x]
[x]	[x]	[x+1]	[0]	[1]
[x+1]	[x+1]	[x]	[1]	[0]

·	[0]	[1]	[x]	[x+1]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[x]	[x+1]
[x]	[0]	[x]	[1]	[x+1]
[x+1]	[0]	[x+1]	[x+1]	[0]

Not, this is not a field since by Theorem 5.7, it is a commutative ring with identity, but not every non-zero row in the multiplication table contains the multiplicative identity ($x + 1$ is not a unit).

2.4 Question Six

By Corollary 5.5, each congruence class can be rewritten with $a, b \in \mathbb{Q}$: $[ax + b]$.
Addition is defined as $[ax + b] + [cx + d] = [(a + c)x + bd]$.
$(ax + b)(cx + d) = acx^2 + dax + bcx + bd = acx^2 + (da + bc)x + bd$

$$\begin{array}{r|l} & ac \\ \hline x^2 - 2 & acx^2 + (1ad + 1bc)\,x + bd \\ & \underline{-\,acx^2 \qquad\qquad\quad + 2ac} \\ & (1ad + 1bc)\,x + (2ac + 1bd) \end{array}$$

Multiplication is thusly defined as $[ax + b] \cdot [cx + d] = [(ad + bc)x + (2ac + bd)]$

2.5 Question Nine

Given that $[a + bx]$ is a nonzero congruence class, either $a > 0$ or $b > 0$. Then let $c = \frac{-a}{a^2+b^2}$ and $d = \frac{b}{a^2+b^2}$.

$$\begin{array}{r|l} & ac \\ \hline x^2 + 1 & acx^2 + (1ad + 1bc)\,x + bd \\ & \underline{-\,acx^2 \qquad\qquad\quad - ac} \\ & (1ad + 1bc)\,x + (-1ac + 1bd) \end{array}$$

$$
\begin{aligned}
[ax+b][cx+d] &= [(ad+bc)x + (bd-ac)] \\
&= [(\frac{ab}{a^2+b^2} + \frac{-ab}{a^2+b^2})x + \frac{b^2}{a^2+b^2} - \frac{-a^2}{a^2+b^2}] \\
&= [0x + \frac{b^2+a^2}{a^2+b^2}] \\
&= [1]
\end{aligned}
$$

3 Section 5.3

3.1 Question One

3.1.1 a

$x^3 + 2x^2 + x + 1$ does not have any roots in Z_3, so by Corollary 4.19 it must be irreducible, and thus a field by 5.10

3.1.2 b

This is not a field by Theorem 5.10 since 2 is a root in Z_5, so by Corollary 4.19 it must be reducible.

3.1.3 c

This is not a field by Theorem 5.10 since $x^4 + x^2 + 1 = (x^2 - x + 1)(x^2 + x + 1) \equiv_2 (x^2 + x + 1)^2$ shows $x^4 + x^2 + 1$ is reducible.

3.2 Question Two

3.2.1 a

Since $\mathbb{Q}(\sqrt{2})$ is a subset of $\mathbb{R}$, multiplication and addition are associative, commutative, and distributive.
The additive identity of $\$\mathbb{Q}$ $(\sqrt{2})is0 + 0\sqrt{2}$ and the multiplicative identity is $1 + 0\sqrt{2}$.
It must be a field since every non-zero element $a + b\sqrt{2}$ is a unit:

$$(a+b\sqrt{2})x = 1 \Rightarrow x = \frac{1}{a+b\sqrt{2}}$$
$$\Rightarrow x = \frac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})}$$
$$\Rightarrow x = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}$$

3.2.2 b

Every element in $\mathbb{Q}/(x^2-2)$ can be rewritten as a member of the congruence class $[ax+b]$ with $a, b \in \mathbb{Q}$ by Corollary 5.5.
Then, we can define a function f such that $f([ax+b]) = a+b\sqrt{2}$ so that $f(x) \in \mathbb{Q}(\sqrt{2})$.
f is thus an isomorphism since (a chance at redemption from my midterm $\ddot{\smile}$):

- f is injective since $f([ax+b]) = f([cx+d]) \Rightarrow a+b\sqrt{2} = c+d\sqrt{2} \Rightarrow a = c \wedge b = d$
- f is surjective since each $a+b\sqrt{2}$ is uniquely mapped to $[ax+b]$
- $f([ax+b]+[cx+d]) = f([(a+c)x+(b+d)]) = (a+c)+(b+d)\sqrt{2} = (a+b\sqrt{2})+(c+d\sqrt{2}) = f([ax+b])+f([cx+d])$
- And via Question Six from section 5.2 above, $f([ax+b]\cdot[cx+d]) = f([(ad+bc)x+(2ac+bd)]) = (ad+bc)+(2ac+bd)\sqrt{2} = (a+b\sqrt{2})(c+d\sqrt{2}) = f([ax+b])f([cx+d])$

3.3 Question Five

3.3.1 a

Since $\mathbb{Q}(\sqrt{3})$ is a subset of $\mathbb{R}$, multiplication and addition are associative, commutative, and distributive.
The additive identity of \$Q $(\sqrt{3})is0+0\sqrt{3}$ and the multiplicative identity is $1+0\sqrt{3}$.
It must be a field since every non-zero element $r+s\sqrt{3}$ is a unit (by first assuming that the inverse of $r+s\sqrt{3}$ from the back of the book, is $\frac{r}{t}-\frac{s}{t}\sqrt{3}$ with $t = r^2-3s^2$):

$$
\begin{aligned}
1 &= (r + s\sqrt{3})(\frac{r}{t} - \frac{s}{t}\sqrt{3}) \\
&= \frac{r^2}{t} - \frac{sr}{t}\sqrt{3} + \frac{sr}{t}\sqrt{3} - \frac{3s^2}{t} \\
&= \frac{r^2 - 3s^2}{t} \\
&= 1
\end{aligned}
$$

3.3.2 b

1. Quick Lemma In $\mathbb{Q}x^2 - 3$, by Corollary 5.5, each congruence class can be rewritten with $a, b \in \mathbb{Q}$: $[ax + b]$.
   $(ax + b)(cx + d) = acx^2 + dax + bcx + bd = acx^2 + (da + bc)x + bd$

$$
\begin{array}{r|l}
 & ac \\
\hline
x^2 - 3 & acx^2 + (1ad + 1bc)\,x + bd \\
 & \underline{-\,acx^2 \qquad\qquad + 3ac} \\
 & (1ad + 1bc)\,x + (3ac + 1bd)
\end{array}
$$

   Multiplication is thusly defined as $[ax + b] \cdot [cx + d] = [(ad + bc)x + (3ac + bd)]$

2. Yeah, it's an isomorphism
   Every element in $\mathbb{Q}/(x^2 - 3)$ can be rewritten as a member of the congruence class $[ax + b]$ with $a, b \in \mathbb{Q}$ by Corollary 5.5.
   Then, we can define a function f such that $f([rx + s]) = r + s\sqrt{3}$ so that $f(x) \in \mathbb{Q}(\sqrt{3})$.
   f is thus an isomorphism since (a chance of redemption from my midterm $\ddot{\smile}$):

   - f is injective since $f([ax + b]) = f([cx + d]) \Rightarrow a + b\sqrt{3} = c + d\sqrt{3} \Rightarrow a = c \wedge b = d$
   - f is surjective since each $a + b\sqrt{3}$ is uniquely mapped to $[ax + b]$
   - $f([ax + b] + [cx + d]) = f([(a + c)x + (b + d)]) = (a + c) + (b + d)\sqrt{3} = (a + b\sqrt{3}) + (c + d\sqrt{3}) = f([ax + b]) + f([cx + d])$
   - And from the lemma, $f([ax+b]\cdot[cx+d]) = f([(ad+bc)x+(3ac+bd)]) = (ad+bc)+(3ac+bd)\sqrt{3} = (a+b\sqrt{3})(c+d\sqrt{3}) = f([ax+b])f([cx+d])$