

Assignment Nine

Lizzy Hunt

March 26, 2023

1 Section 5.1

1.1 Question One

1.1.1 b

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

$$\begin{array}{r} x \\ x^2 + 1 \overline{) x^3 + x} \\ \underline{-x^3 - x} \\ 0 \end{array}$$

1.1.2 c

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

$$\begin{array}{r}
x^3 - x^2 + x - 1 \bigg) \overline{\begin{array}{r} x^2 - x + 2 \\ x^5 - 2x^4 + 4x^3 - 8x^2 + 3x - 2 \\ -x^5 + x^4 - x^3 + x^2 \\ \hline -x^4 + 3x^3 - 7x^2 + 3x \\ x^4 - x^3 + x^2 - x \\ \hline 2x^3 - 6x^2 + 2x - 2 \\ -2x^3 + 2x^2 - 2x + 2 \\ \hline -4x^2 \end{array}}
\end{array}$$

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 - TODO

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 - TODO

2.3 Question Three - TODO

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 $[ax + b] + [cx + d] = [(a + c)x + bd]$.

$$(ax + b)(cx + d) = acx^2 + dax + bcx + bd = acx^2 + (da + bc)x + bd$$

$$\begin{array}{r} x^2 - 2) \quad \begin{array}{r} \quad \quad \quad ac \\ \quad \quad \quad + bd \\ - acx^2 \quad \quad \quad + 2ac \\ \hline \quad \quad \quad (1ad + 1bc)x + (2ac + 1bd) \end{array} \end{array}$$

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 $d = \frac{b}{a^2 + b^2}$.

$$\begin{array}{r} x^2 + 1) \quad \begin{array}{r} \quad \quad \quad ac \\ \quad \quad \quad + bd \\ - acx^2 \quad \quad \quad - ac \\ \hline \quad \quad \quad (1ad + 1bc)x + (-1ac + 1bd) \end{array} \end{array}$$

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

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 $\mathbb{Q}(\sqrt{2})$ is $0 + 0\sqrt{2}$ 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:

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

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 of redemption from my midterm ☺):

- 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 $[ax + b]$
- $f([ax + b] + [cx + d]) = f([(a + c)x + (b + d)]) = (a + c) + (b + d)\sqrt{2} = (a + b\sqrt{2}) + (c + d\sqrt{2}) = f([ax + b]) + f([cx + d])$

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 $\mathbb{Q}(\sqrt{3})$ is $0 + 0\sqrt{3}$ 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, $\frac{r}{r^2 - 3s^2} - \frac{s}{r^2 - 3s^2}\sqrt{3}$:

$$\begin{aligned} (a + b\sqrt{3})x &= 1 \Rightarrow x = \frac{1}{a + b\sqrt{3}} \\ \Rightarrow x &= \frac{a - b\sqrt{3}}{(a + b\sqrt{3})(a - b\sqrt{3})} \\ \Rightarrow x &= \frac{a}{a^2 - 3b^2} - \frac{b}{a^2 - 3b^2}\sqrt{3} \end{aligned}$$