Homework 14
Section 5.1, 5.2, 5.3

Jonathan Petersen
A01236750

April 27th, 2016

5.1.1.b. **Let $f(x)$, $g(x)$, $p(x) \in F[x]$, with $p(x)$ nonzero. Determine whether $f(x) \equiv g(x) \pmod{p(x)}$. Show your work. Let $f(x) = x^4 + x^2 + x + 1$, $g(x) = x^4 + x^3 + x^2 + 1$, $p(x) = x^2 + x$, and $F = \mathbb{Q}$.**

To check if $f(x)$ and $g(x)$ are equivalent modulo $p(x)$, we must check to see if the remainders of $f(x)$ and $g(x)$ are the same up to associates when divided by $p(x)$. For $f(x)$, observe that

$$
\begin{array}{r|lllll}
 & & & x^2 & -x & +2 \\ \hline
x^2 + x & x^4 & & +x^2 & +x & +1 \\
 & -x^4 & -x^3 & & & \\ \cline{2-3}
 & & -x^3 & +x^2 & & \\
 & & x^3 & +x^2 & & \\ \cline{3-4}
 & & & 2x^2 & +x & \\
 & & & -2x^2 & -2x & \\ \cline{4-5}
 & & & & -x &
\end{array}
$$

and for $g(x)$ that

$$
\begin{array}{r|lllll}
 & & & x^2 & & +1 \\ \hline
x^2 + x & x^4 & +x^3 & +x^2 & & +1 \\
 & -x^4 & -x^3 & & & \\ \cline{2-3}
 & & & x^2 & & \\
 & & & -x^2 & -x & \\ \cline{4-5}
 & & & & -x &
\end{array}
$$

In other words,

$$
\begin{aligned}
f(x) &= (x^2 + x)(x^2 - x + 2) - x \\
g(x) &= (x^2 + x)(x^2 + 1) - x
\end{aligned}
$$

and since the remainder in both cases is $-x$, $f(x) \equiv g(x) \pmod{p(x)}$.

5.1.1.c. **Let $f(x)$, $g(x)$, $p(x) \in F[x]$, with $p(x)$ nonzero. Determine whether $f(x) \equiv g(x)$ (mod $p(x)$). Show your work. Let $f(x) = 3x^5 + 4x^4 + 5x^3 - 6x^2 + 5x - 7$, $g(x) = 2x^5 + 6x^4 + x^3 + 2x^2 + 2x - 5$, $p(x) = x^3 - x^2 + x - 1$, and $F = \mathbb{R}$.**

As in the above, observe that for $f(x)$

$$
\begin{array}{rl}
 & 3x^2 + 7x + 9 \\
\cline{2-2}
x^3 - x^2 + x - 1 \big) & 3x^5 + 4x^4 + 5x^3 - 6x^2 + 5x - 7 \\
 & -3x^5 + 3x^4 - 3x^3 + 3x^2 \\
\cline{2-2}
 & 7x^4 + 2x^3 - 3x^2 + 5x \\
 & -7x^4 + 7x^3 - 7x^2 + 7x \\
\cline{2-2}
 & 9x^3 - 10x^2 + 12x - 7 \\
 & -9x^3 + 9x^2 - 9x + 9 \\
\cline{2-2}
 & -x^2 + 3x + 2
\end{array}
$$

and for $g(x)$,

$$
\begin{array}{rl}
 & 2x^2 + 8x + 7 \\
\cline{2-2}
x^3 - x^2 + x - 1 \big) & 2x^5 + 6x^4 + x^3 + 2x^2 + 2x - 5 \\
 & -2x^5 + 2x^4 - 2x^3 + 2x^2 \\
\cline{2-2}
 & 8x^4 - x^3 + 4x^2 + 2x \\
 & -8x^4 + 8x^3 - 8x^2 + 8x \\
\cline{2-2}
 & 7x^3 - 4x^2 + 10x - 5 \\
 & -7x^3 + 7x^2 - 7x + 7 \\
\cline{2-2}
 & 3x^2 + 3x + 2
\end{array}
$$

We see that

$$
\begin{aligned}
f(x) &= (x^3 - x^2 + x - 1)(3x^2 + 7x + 9) + (-x^2 + 3x + 2) \\
g(x) &= (x^3 - x^2 + x - 1)(2x^2 + 8x + 7) + (3x^2 + 3x + 2)
\end{aligned}
$$

and since $-x^2 + 3x + 2 \neq 3x^2 + 3x + 2$, $f(x) \not\equiv g(x) \pmod{p(x)}$.

5.1.3. **How many distinct congruence classes are there modulo x^3+x+1 in $\mathbb{Z}_2[x]$? List them.**

We know from the definition of congruence classes that there must be a distinct congruence class for every distinct remainder value when an indeterminate polynomial in $\mathbb{Z}_2[x]$ is divided by $x^3 + x + 1$. We also know that the degree of the remainder in such a case must be less than the degree of $x^3 + x + 1$, and as such all possible remainders can be represented as a list of all possible polynomials of degree 2 in $\mathbb{Z}_2[x]$. They are as follows:

(a) $[0]x^2 + [0]x + [0] = [0]$
(b) $[0]x^2 + [0]x + [1] = [1]$
(c) $[0]x^2 + [1]x + [0] = x$
(d) $[0]x^2 + [1]x + [1] = x + [1]$

(e) $[1]x^2 + [0]x + [0] = x^2$

(f) $[1]x^2 + [0]x + [1] = x^2 + [1]$

(g) $[1]x^2 + [1]x + [0] = x^2 + x$

(h) $[1]x^2 + [1]x + [1] = x^2 + x + [1]$

and as we can see, there are eight possible values. Therefore, there must be eight distinct congruence classes in $\mathbb{Z}_2[x]$ (mod $x^3 + x + 1$).

5.1.12. **If $f(x)$ is relatively prime to $p(x)$, prove that there is a polynomial $g(x) \in F[x]$ such that $f(x)g(x) \equiv 1_F \pmod{p(x)}$.**

Since $f(x)$ and $p(x)$ are relatively prime, $f(x)$ must be a unit in $F[x]/ < p(x) >$. Furthermore, by Theorem 4.8 there must be polynomials $g(x)$, $h(x)$ such that

$$\begin{aligned} f(x)g(x) + p(x)h(x) &= [1] \\ f(x)g(x) - [1] &= -p(x)h(x) \\ &= p(x)(-h(x)) \end{aligned}$$

and by Theorem 5.3, this implies that

$$[f(x)g(x)] = [1]$$

or rather that $f(x)g(x) \equiv 1_F \pmod{p(x)}$ ∎

5.2.2. **Write out the addition and multiplicaiton tables for $\mathbb{Z}_3[x]/ < x^2 + 1 >$. Is $\mathbb{Z}_3[x]/ < x^2 + 1 >$ a field?**

Since $x^2 + 1$ is irreducible in $\mathbb{Z}_3[x]$, $\mathbb{Z}_3[x]/ < x^2 + 1 >$ is a field.

5.2.14.a. **Explain why $[f(x)] = [2x-3] \in \mathbb{Q}[x]/ < x^2-2 >$ is a unit and find its inverse.**

Since x^2-2 is irreducible in $\mathbb{Q}[x]$, $\mathbb{Q}[x]/ < x^2-2 >$ is a field, and so every nonzero element of $\mathbb{Q}[x]/ < x^2-2 >$ is a unit. Since $[2x-3]$ is a nonzero element of $\mathbb{Q}[x]/ < x^2-2 >$, it must also be a unit.

By Theorem 4.8, there must be some $g(x)$, $q(x)$ such that if $p(x) = x^2-2$

$$f(x)g(x) + p(x)q(x) = [1]$$

We also know that $g(x)$ and $q(x)$ must have degree smaller than $p(x)$, namely degree one. Therefore, without loss of generality, we can assume that

$$\begin{aligned}
f(x)(ax+b) + p(x)(cx+d) &= 1 \\
(2x-3)(ax+b) + (x^2-2)(cx+d) &= 1 \\
2ax^2 + 2bx - 3ax - 3b + cx^3 + dx^2 - 2cx - 2d &= 1 \\
cx^3 + (2a+d)x^2 + (2b-3a-2c)x + (-3b-2d) &= 1
\end{aligned}$$

Which, by equality of polynomials, leads to the system of equations

$$\begin{aligned}
c &= 0 \\
2a+d &= 0 \\
2b-3a-2c &= 0 \\
-3b-2d &= 1
\end{aligned}$$

So therefore

$$\begin{aligned}
a &= -2 \\
b &= -3 \\
c &= 0 \\
d &= 4
\end{aligned}$$

and the inverse of $[f(x)] = [2x-3]$ is $[g(x)] = [-2x-3]$.

5.2.14.b. **Explain why $[f(x)] = [x^2+x+1] \in \mathbb{Z}_3[x]/ < x^2+1 >$ is a unit and find its inverse.**

Let $p(x) = x^2+1$ in $\mathbb{Z}_3[x]$. Since $f(x)$ and $p(x)$ are relatively prime, $f(x)$ must be a unit in $\mathbb{Z}_3[x]/ < x^2+1 >$. By the same logic as the previous problem, there must be a $g(x) = ax+b$ and $q(x) = cx+d$ such that

$$\begin{aligned}
f(x)g(x) + p(x)q(x) &= 1 \\
(x^2+x+1)(ax+b) + (x^2+1)(cx+d) &= 1 \\
ax^3 + ax^2 + ax + bx^2 + bx + b + cx^3 + dx^2 + cx + d &= 1 \\
(a+c)x^3 + (a+b+d)x^2 + (a+b+c)x + (b+d) &= 1
\end{aligned}$$

Which, by equality of polynomials, leads to the system of equations

$$\begin{aligned} a + c &= 0 \\ a + b + d &= 0 \\ a + b + c &= 0 \\ b + d &= 1 \end{aligned}$$

And therefore

$$\begin{aligned} a &= -1 \\ b &= 0 \\ c &= 1 \\ d &= 1 \end{aligned}$$

so the inverse of $[f(x)]$ is $[g(x)] = [-x]$.

5.3.1.a. **Determine whether $\mathbb{Z}_3[x]/ < x^3 + 2x^2 + x + 1 >$ is a field. Justify your answer.**

$\mathbb{Z}_3[x]/ < x^3 + 2x^2 + x + 1 >$ is a field if and only if $x^3 + 2x^2 + x + 1$ is irreducible in $\mathbb{Z}_3[x]$. Since $x^3 + 2x^2 + x + 1$ is a cubic function, if it does reduce it must factor into a quadratic term and a linear term. By Corollary 4.19 this is equivalent to saying that x^3+2x^2+x+1 is irreducible if and only if $x^3 + 2x^2 + x + 1$ has no roots. The possible roots in $\mathbb{Z}_3[x]$ are [0], [1], and [2].

Observe that

$$\begin{aligned} [0]^3 + 2[0]^2 + [0] + 1 &= [1] \\ [1]^3 + 2[1]^2 + [1] + 1 &= [2] \\ [2]^3 + 2[2]^2 + [2] + 1 &= [1] \end{aligned}$$

so we can conclude that $x^3 + 2x^2 + x + 1$ is irreducible and thus that $\mathbb{Z}_3[x]/ < x^3 + 2x^2 + x + 1 >$ is a field.

5.3.1.b. **Determine whether $\mathbb{Z}_5[x]/ < 2x^3 - 4x^2 + 2x + 1 >$ is a field. Justify your answer.**

By the same logic as the previous problem, we must check if $2x^3 - 4x^2 + 2x + 1$ is irreducible in $\mathbb{Z}_5[x]$ to see if $\mathbb{Z}_5[x]/ < 2x^3 - 4x^2 + 2x + 1 >$ is a field. Since $2x^3 - 4x^2 + 2x + 1$ is cubic, if it's reducible it must factor into a quadratic term and a linear term, or in other words it must have a root. In $\mathbb{Z}_5[x]$, the possible roots are [0], [1], [2], [3], and [4].

Observe that

$$\begin{aligned} 2[0]^3 - 4[0]^2 + 2[0] + [1] &= [1] \\ 2[1]^3 - 4[1]^2 + 2[1] + [1] &= [1] \\ 2[2]^3 - 4[2]^2 + 2[2] + [1] &= [0] \end{aligned}$$

We see that [2] is a root, so $2x^3 - 4x^2 + 2x + 1$ is reducible in $\mathbb{Z}_5[x]$ and $\mathbb{Z}_5[x]/ < 2x^3 - 4x^2 + 2x + 1 >$ is not a field.

5.3.1.c. **Determine whether $\mathbb{Z}_2[x]/ < x^4 + x^2 + 1 >$ is a field. Justify your answer.**

By the same logic above, we must check to see if $x^4 + x^2 + 1$ factors. Since the equation has no roots, if it does factor it must factor into the product of two quadratics. The only quadratic terms in $\mathbb{Z}_2[x]$ are x^2, x^2+1, x^2+x, and $x^2 + x + 1$.

Observe that

$$(x^2 + 1)(x^2 + 1) = x^4 + x^2 + x^2 + 1(x^2 + 1)(x^2 + x + 1) = x^4 + x^3 + x^2 + x^2 + x + 1$$

5.3.5.a. **Verify that $\mathbb{Q}(\sqrt{3}) = \{r + s\sqrt{3} \mid r, s \in \mathbb{Q}\}$ is a subfield of $\mathbb{R}$.**

To show that $\mathbb{Q}(\sqrt{3})$ is a subfield of $\mathbb{R}$, we must show that $\mathbb{Q}(\sqrt{3})$ is closed under the subtraction and multiplication rules of $\mathbb{R}$.

Consider the case of subtraction, given two arbitrary elements of $\mathbb{Q}(\sqrt{3})$

$$\begin{aligned} (a + b\sqrt{3}) - (c + d\sqrt{3}) &= a + b\sqrt{3} - c - d\sqrt{3} \qquad a, b, c, d \in \mathbb{Q} \\ &= (a - c) + (b - d)\sqrt{3} \end{aligned}$$

Therefore $\mathbb{Q}(\sqrt{3})$ is closed under subtraction.

Now consider multiplication, again with arbitrary elements.

$$\begin{aligned} (a + b\sqrt{3}) * (c + d\sqrt{3}) &= ac + ad\sqrt{3} + bc\sqrt{3} + bd(3) \\ &= (ac + 3bd) + (ad + bc)\sqrt{3} \end{aligned}$$

and $\mathbb{Q}(\sqrt{3})$ is closed under multiplication.

Since $\mathbb{Q}(\sqrt{3})$ is closed under subtraction and multiplication, it is a subring of $\mathbb{R}$.

5.3.5.b. **Show that $\mathbb{Q}(\sqrt{3})$ is isomorphic to $\mathbb{Q}[x]/ < x^2 - 3 >$.**

5.3.10. **Show that $\mathbb{Q}[x]/ < x^2 - 2 >$ is not isomorphic to $\mathbb{Q}[x]/ < x^2 - 3 >$.**

Since $\mathbb{Q}[x]/ < x^2 - 2 >$ is isomorphic to $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}[x]/ < x^2 - 3 >$ is isomorphic to $\mathbb{Q}(\sqrt{3})$, we can see that if $\mathbb{Q}[x]/ < x^2 - 2 >$ is isomorphic to $\mathbb{Q}[x]/ < x^2 - 3 >$ it must be that $\mathbb{Q}(\sqrt{2})$ is isomorphic to $\mathbb{Q}(\sqrt{3})$. As shown in class, this is not true by the following:

Let f be an isomorphism from $\mathbb{Q}(\sqrt{2})$ to $\mathbb{Q}(\sqrt{3})$. Then we know that

$$\begin{aligned}
f(\sqrt{2}) &= r + s\sqrt{3} \qquad r, s \in \mathbb{Q} \\
f(2) &= f(1+1) = f(1) + f(1) \\
f(1) &= 1 \\
f(2) &= 2 \\
f(2) &= f(\sqrt{2} * \sqrt{2}) = f(\sqrt{2}) * f(\sqrt{2}) \\
&= (r + s\sqrt{3})(r + s\sqrt{3})
\end{aligned}$$

Then it must be that

$$\begin{aligned}
2 &= (r + s\sqrt{3})2 \\
&= r2 + 3s2 + 2rs\sqrt{3} \\
2 + 0\sqrt{3} &= r2 + 3s2 + 2rs\sqrt{3}
\end{aligned}$$

And

$$\begin{aligned}
2 &= r2 + 3s2 \\
0 &= 2rs
\end{aligned}$$

Which is a contradiction.