Homework 9
Abstract Algebra
Math 320
Stephen Giang

Problem 1: Let $f(x), g(x) \in F[x]$, not both zero. Prove that if there exist $u(x), v(x) \in F[x]$ such that $f(x)u(x) + g(x)v(x) = 1_F$, then $f(x)$ and $g(x)$ are relatively prime.

By Theorem 4.8, $f(x)u(x) + g(x)v(x) = d(x) = 1_F$, such that $d(x) = gcd(f(x), g(x))$. Because $d(x) = gcd(f(x), g(x)) = 1_F$, by definition of relatively prime, $f(x)$ and $g(x)$ are relatively prime.

Problem 2: List all associates of $x^2 + x + 1$ in $\mathbb{Z}_5[x]$.

All associates of $f(x) = x^2 + x + 1$ can be written as $cf(x)$ for $c \in \mathbb{Z}_5$.

$$\begin{aligned}
1(x^2 + x + 1) &= x^2 + x + 1 \\
2(x^2 + x + 1) &= 2x^2 + 2x + 2 \\
3(x^2 + x + 1) &= 3x^2 + 3x + 3 \\
4(x^2 + x + 1) &= 4x^2 + 4x + 4
\end{aligned}$$

Problem 3: Show that $x - 1_F$ divides $a_n x^n + ... + a_2 x^2 + a_1 x + a_0 \in F[x]$ if and only if $a_n + a_{n-1} + ... + a_2 + a_1 + a_0 = 0_F$.

(=>). Let $f(x) = a_n x^n + ... + a_2 x^2 + a_1 x + a_0 \in F[x]$ such that $x - 1_F$ divides $f(x)$

Because $x - 1_F$ divides $f(x)$, 1_F is a root of $f(x)$, such that

$$f(1_F) = a_n + a_{n-1} + ... + a_2 + a_1 + a_0 = 0_F$$

(<=). Let $a_n + a_{n-1} + ... + a_2 + a_1 + a_0 = 0_F$.

Thus there exists $f(x) \in F[x]$, with $f(x) = a_n x^n + ... + a_2 x^2 + a_1 x + a_0$, such $f(1_F) = 0_F$. Because $f(1_F) = 0_F$, 1_F is a root, meaning that $x - 1_F$ divides $f(x)$

$\square$

Problem 4: We say that $a \in F$ is a multiple root of $f(x) \in F[x]$ if $(x-a)^k$ is a factor of $f(x)$ for some $k \geq 2$

(a) Prove that $a \in \mathbb{R}$ is a multiple root of $f(x) \in \mathbb{R}[x]$ if and only if a is a root of both $f(x)$ and $f'(x)$, where $f'(x)$ is the derivative of $f(x)$. You may assume that the Product Rule is true

(=>). Let $a \in \mathbb{R}$ be a multiple root of $f(x) \in \mathbb{R}[x]$.

So $\exists u(x) \in \mathbb{R}[x]$, such that $f(x) = u(x)(x-a)^k$, with $k \geq 2$. Notice that:

$$\begin{aligned} f'(x) &= u(x)(k(x-a)^{k-1}) + u'(x)(x-a)^k, \text{ with } (k-1) \geq 1 \\ &= (x-a)\left[u(x)(k(x-a)^{k-2}) + u'(x)(x-a)^{k-1}\right] \end{aligned}$$

Because $(x-a)$ is a factor of both $f(x)$ and $f'(x)$, a is a root of both $f(x)$ and $f'(x)$

(<=) Let a be a root of both $f(x)$ and $f'(x)$.

Thus $\exists u(x) \in \mathbb{R}[x]$, such that $f(x) = u(x)(x-a)^k$.

If $(k < 1)$, then a would not be a root of $f(x)$.
If $(k = 1)$, then $f'(x) = u(x) + u'(x)(x-a)^k$, meaning a would not be a root of $f'(x)$.
If $(k > 1)$, then $f'(x) = (x-a)\left[u(x)(k(x-a)^{k-2}) + u'(x)(x-a)^{k-1}\right]$.

Thus $k > 1$, or $k \geq 2$, to have a be a root of both $f(x)$ and $f'(x)$. And because $k \geq 2$, a is a multiple root of $f(x)$

$\square$

(b) If $f(x) \in \mathbb{R}[x]$ and $f(x)$ is relatively prime to $f'(x)$, prove that f(x) has no multiple roots in $\mathbb{R}$.

So we can prove this by proving the contraposition.

If f(x) has multiple roots in $\mathbb{R}$, then $f(x) \in \mathbb{R}[x]$ and $f(x)$ is not relatively prime to $f'(x)$

Solution 4b. By part (a), if $f(x)$ has multiple roots in $\mathbb{R}$, then $f(x)$ and $f'(x)$ share a root a, thus sharing a factor $x - a$. Thus $f(x)$ is not relatively prime to $f'(x)$

$\square$

Problem 5: Determine if the following polynomials are irreducible:

(a) $x^3 - 9$ in $\mathbb{Z}_{11}[x]$

We can use the Rational Roots Theorem, and see if it contains any roots, $\pm 1, \pm 9$. Let $f(x) = x^3 - 9 \in \mathbb{Z}_{11}[x]$

$$f(1) = -8 \qquad f(-1) = -10$$
$$f(9) = 720 = 5 \qquad f(-9) = -738 = 1$$

Because the degree of $f(x)$ is 3, then its factors must be of degree 1 and 2, meaning that its factors will contain its root, but because there does not exist a root in $\mathbb{Z}_{11}[x]$, (a) is irreducible.

(b) $x^4 + x^2 + 2$ in $\mathbb{Z}_3[x]$

We can use the Rational Roots Theorem, and see if it contains any roots, $\pm 1, \pm 2$. Let $f(x) = x^4 + x^2 + 2 \in \mathbb{Z}_3[x]$

$$f(1) = f(-1) = 4 = 1$$
$$f(2) = f(-2) = 22 = 1$$

Because there does not exist a root, the only factors of $f(x)$ have to be of degree 2, such that for $a, b, c, d \in \mathbb{Z}_3[x]$

$$\begin{aligned} f(x) = x^4 + x^2 + 2 &= (x^2 + ax + b)(x^2 + cx + d) \\ &= x^4 + (a + c)x^3 + (ac + b + d)x^2 + (bc + ad)x + bd \end{aligned}$$

Now we just need to solve for a, b, c, d

$$a + c = 0 \tag{1}$$
$$ac + b + d = 1 \tag{2}$$
$$bc + ad = 0 \tag{3}$$
$$bd = 2 \tag{4}$$

Now we can see that $c = -a$ from (1), and $b = 2, d = 1$ or $b = 1, d = 2$, such that $b + d = 3 = 0$ from (4). Now by evaluating, we can see in (2), $a^2 = -1 = 2$. Because there does not exist an $a \in \mathbb{Z}_3$, such that $a^2 = 2$, there does not exist any factors of $f(x)$. Proving that $f(x)$ is irreducible.