I worked alone without getting any help, except asking questions on Piazza and reading the Notes of this course.

1 Polynomial Practice

(a)

(i) At least: **0**. At most: $\mathbf{max(deg(}f\mathbf{), deg(}g\mathbf{))}$

Since we can't guarantee that the resulting polynomial $f + g$ always has a real root, so the least number of roots is 0.

WLOG, let $\deg(f) \le \deg(g)$. Consider $f+g$, since it is non-zero, so it is a polynomial whose degree is at most $\deg(g)$, and since a polynomial with degree d has at most d roots, so $f + g$ has at most $\deg(g)$ roots. Vice versa for the case of $\deg(f) > \deg(g)$, which gives us that the polynomial $f+g$ has at most $\max(\deg(f), \deg(g))$ roots.

(ii) At least: **0**. At most: $\mathbf{deg(}f\mathbf{)} + \mathbf{deg(}g\mathbf{)}$

Consider $f = g = x^2 + 1$, so f, g have no roots, so $f \cdot g$ also have no roots, which implies that $f \cdot g$ is not guaranteed to have any roots, so the least number of roots is 0.

Let $a = \deg(f)$ and $b = \deg(g)$. Since $x^a \cdot x^b = x^{a+b}$, so the degree of the polynomial $f \cdot g$ is $a + b$, which is $\deg(f) + \deg(g)$. Again, using the property of polynomials, so $f \cdot g$ has at most $\deg(f) + \deg(g)$ roots.

(iii) At least: **0**. At most: $\mathbf{deg(}f\mathbf{)} - \mathbf{deg(}g\mathbf{)}$

Again, we can't guarantee that f/g always has a root. For example, let $f = x^2 + 1$ and $g = 1$, so $f/g = x^2 + 1$ does not have a root. So, the least number of roots is 0.

Let $a = \deg(f)$ and $b = \deg(g)$. Since $\frac{x^a}{x^b} = x^{a-b}$ and that we are given that f/g is a polynomial, so the degree of the polynomial f/g is $a - b$, which is $\deg(f) - \deg(g)$. Again, using the property of polynomials, so f/g has at most $\deg(f) - \deg(g)$ roots.

(b)

(i) No, it isn't.

We proceed by providing a counterexample. Consider $p = 2,\ f(x) = x,\ g(x) = x + 1$. For all $x \in GF(p)$, namely, $x_1 = 0$ or $x_2 = 1$, we have that when $x_1 = 0$, $f \cdot g(x) = 0 \cdot 1 = 0$; when $x_2 = 1$, $f \cdot g(x) = 1 \cdot 2 \equiv 0 \pmod 2$, which gives us that $f \cdot g = 0$.

Yet, when $x = 1$, $f(x) = 1 \neq 0$; when $x = 0$, $g(x) = 1 \neq 0$, which implies that $f \neq 0$ and $g \neq 0$. Thus, this is a counterexample, so if f, g are polynomials over $GF(p)$ and $f \cdot g = 0$, it isn't necessarily true that either $f = 0$ or $g = 0$.

(ii) Direct Proof.

Proof. We proceed by a direct proof. Suppose f be a polynomial over $GF(p)$, and that $\deg(f) \ge p$.

Now, let $f(i) = y_i\ \forall i \in \{0, 1, ..., p-1\}$, which means that we have p pairs $(0, y_0), (1, y_1), ..., (p - 1, y_{p-1}$ with all the x_i distinct. Thus, by Property 2 of polynomials, so there is a unique polynomial $h(x)$ of degree (at most) $p - 1$, which means that h is a polynomial with $\deg(h) \le p - 1 < p$ such that $f(x) = h(x)$ for all $x \in \{0, 1, ..., p - 1\}$, as desired. Thus, such a polynomial h exists.

Q.E.D.

(iii) p^d

For a polynomial f with degree $d < p$, so $f(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0$, where

$a_i \in \{0, 1, ..., p-1\}\ \forall\ i \in \mathbb{N}, i \leq d$.

Then, the only constraint on f is that $f(0) = a_0 = a$ where $a \in \{0, 1, ..., p-1\}$. So only one coefficient, a_0, of f is set, which means that $\forall\ 1 \leq i \leq d, i \in \mathbb{N}$, we have that a_i could be any value in the set $\{0, 1, ..., p-1\}$. Thus, there are p possible values for each coefficient a_i of f, and there are d-many coefficients we could assign values arbitrarily (as long as they are in $\{0, 1, ..., p-1\}$), which implies that there are p^d-many such polynomials f.

(c) $f = 4x^2 + 1$. There are **25** such polynomial.

Part (1) Finding one such polynomial f

We first use Lagrange interpolation to find one such f. So, we have that $8^{-1} \equiv 2 \pmod 5$ with $8 \cdot 2 = 16 = 5 \cdot 3 + 1$, and similarly, $(-4)^{-1} \equiv 1 \pmod 5$ with $-4 \cdot 1 = -4 = 5 \cdot (-1) + 1$.

Thus, using Lagrange interpolation, we have:

$$\Delta_1(x) = \frac{(x-2)(x-4)}{(0-2)(0-4)} = \frac{x^2-6x+8}{8} = 2(x^2 - 6x + 8) = 2x^2 - 12x + 16$$

$$\Delta_2(x) = \frac{(x-0)(x-4)}{(2-0)(2-4)} = \frac{x^2-4x}{-4} = 1(x^2 - 4x) = x^2 - 4x$$

$$\Delta_3(x) = \frac{(x-0)(x-2)}{(4-0)(4-2)} = \frac{x^2-2x}{8} = 2(x^2 - 2x) = 2x^2 - 4x$$

Thus, the polynomial $f(x)$ is therefore given by:

$f(x) = 1 \cdot \Delta_1(x) + 2 \cdot \Delta_2(x) + 0 \cdot \Delta_3(x) = 1(2x^2 - 12x + 16) + 2(x^2 - 4x) + 0(2x^2 - 4x) = (2 + 2)x^2 + (-12 - 8)x + 16 = 4x^2 - 20x + 16$

Since f is a polynomial over $GF(5)$, and that we have $-20 = 5 \cdot (-4) + 0, 16 = 5 \cdot 3 + 1$, which gives us that $-20 \equiv 0 \pmod 5, 16 \equiv 1 \pmod 5$, so we have that $f(x) = 4x^2 + 1$.

Part (2) Showing that there are 25 such polynomials

Since we define f over $GF(5)$, so the value of x is also confined within $\{0, 1, 2, 3, 4\}$. Now, since $f(0) = 1, f(2) = 2, f(4) = 0$, so we only have $x = 1, x = 3$ that we can arbitrarily assign values to, with $f(x)$ still confined within $\{0, 1, 2, 3, 4\}$. So, we have $5 \cdot 5 = 25$ different combinations of value assignments to $f(x), 0 \leq x \leq 4$. Then, by the property of polynomials, we can construct a unique polynomial based on each of these assignments, which means that there are 25 different such polynomials.