1 Extension Fields

We continue our discussion on extension fields.

1.1 Formal Derivative

Definition 1.1: Formal Derivative

The **formal derivative** of $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in F[x]$ is $f'(x) = a_n n x^{n-1} + \cdots + a_1 \in F[x]$.

Lemma 1.1: Properties of the Derivative

Let $f(x), g(x) \in F[x]$ and $a \in F$, where F is a field. Then:

1. $(f(x) + g(x))' = f'(x) + g'(x)$.
2. $(af(x))' = af'(x)$.
3. $(f(x)g(x))' = f(x)g'(x) + g(x)f'(x)$.

1.1.1 Example 1: Derivative

The derivative of $x^3 + x^2 + 1$ is $3x^2 + 2x$.

1.2 Criterion for Multiple Zeros

Theorem 1.1

$f(x) \in F[x]$ has a multiple zero in an extension E/F if and only if $f(x)$ and $f'(x)$ have a common factor in $F[x]$.

1.2.1 Example 1: Multiple Roots

Consider $f(x) = x^2 + 2x + 1 = (x+1)^2$. Then, $f'(x) = 2x + 2 = 2(x+1)$. Here, $x + 1$ is a common factor.

1.2.2 Example 2: Multiple Roots

Consider $g(x) = x^4 + 2x^2 + 1 = (x^2+1)^2$. Then, $g'(x) = 4x^3 + 4x = 4x(x^2+1)$. Here, $x^2 + 1$ is a common factor.

1.2.3 Example 3: Multiple Roots

Consider $f(x) = x^5 + x^3 + x^2 + 1 \in \mathbb{F}_3[x]$. We note that

$$f'(x) = 5x^4 + 3x^2 + 2x \equiv 2x^4 + 2x \in \mathbb{F}_3[x]$$

We now want to see if both polynomials have a common factor. We start with $f'(x)$.

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

We see that $x = 2$ is a root. So:

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

We note that $x^2 + 2x + 1$ is reducible, so:

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

Now, if $f(x)$ and $f'(x)$ have a common factor $p(x)$, then either $x|p(x)$ or $x+1|p(x)$. Because $p(x)$ is a factor of $f(x)$, this implies that $x|f(x)$ or $x+1|f(x)$. Note that:

- $x|f(x) \iff f(0) = 0$.
- $x+1|f(x) \iff f(2) = 0$ since $x+1$ is the same thing as $x-2$. Here, we see that $f(2) = 0$, so $f(x)$ have multiple zeros.

1.3 Zeros of an Irreducible

Theorem 1.2

Let $f(x) \in F[x]$ be irreducible. If F has characteristic 0, then $f(x)$ has no multiple roots. If F has characteristic p, then $f(x)$ has multiple roots if and only if $f(x) = g(x^p)$ for some $g(x)$ in $F[x]$.

1.3.1 Example 1: Irreducible Polynomials

Consider $x^6 + x^2 + 1 \in \mathbb{F}_2[x]$. Knowing that char $\mathbb{F}_2 = 2$, we have

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