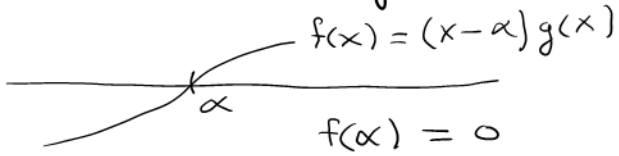
Section 13.5 Separable and Inseparable Extensions

We will here be concerned with multiplicities of roots. It is helpful to review the familiar situation involving $\mathbb{R}$.

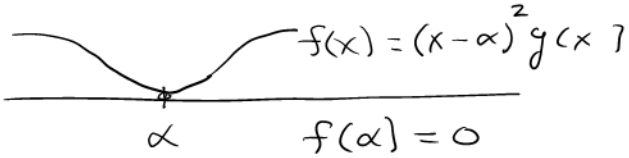
$f(x)$ has a simple root at $x = \alpha$



$f(\alpha) = 0$

$f'(\alpha) \neq 0$

$f(x)$ has a multiple root at $x = \alpha$



$f(\alpha) = 0$

$f'(\alpha) = 0$

Signal for multiple root at α $\begin{cases} f(\alpha) = 0 \\ f'(\alpha) = 0 \end{cases}$

Definitions A polynomial in $F[x]$ is called **separable** if it has no multiple roots. Otherwise its **inseperable**

Separable $f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$

Inseparable $f(x) = (x-\alpha_1)^{n_1}(x-\alpha_2)^{n_2}\cdots(x-\alpha_k)^{n_k}$

$\Big\}$ α_i distinct

- Integer n_i is called the **multiplicity** of root α.
- Note: In general the α_i are in a splitting field or the algebraic closure of F, not necessarily in F itself

Definition The **derivative** of $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ is

$$D_x f(x) = f'(x) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}$$

Check that this satisfies:

- $D_x [f(x) \pm g(x)] = D_x f(x) + D_x g(x)$
- $D_x [f(x) g(x)] = D_x f(x) \cdot g(x) + f(x) D_x g(x)$
- $D_x [f(x)^n] = n f(x)^{n-1} f'(x)$

Proposition 33 Suppose $f(x) \in F[x]$. Then:

$f(x)$ has multiple root at $\alpha \iff f(\alpha) = 0$ and $f'(\alpha) = 0$

$\iff m_\alpha(x) \mid f(x)$ and $m_\alpha(x) \mid f'(x)$

$f(x)$ separable $\iff \gcd(f(x), f'(x)) = 1$.

Corollary 34 Suppose F has characteristic 0. Then:

① Any irreducible $f(x) \in F[x]$ is separable.

② $f(x)$ separable $\iff$ $f(x)$ is product of distinct irreducibles.

Proof Suppose $f(x)$ is irreducible, hence prime. If it is linear, then it's clearly seperable. Thus assume $\deg f > 1$. Then $\gcd(f(x), f'(x)) = 1$. Now apply previous proposition.

($f(x)$: irreducible; $f'(x)$: deg ≥ 1)

Note: This argument could break down in characteristic p because it's possible that $\deg f > 0$ but $f'(x) = 0$. Ex: $f(x) = x^{2p} + x^p + 1$. Then $\gcd(f(x), f'(x)) = f(x) \neq 1$.

So extra work is required for characteristic p:

Proposition 35 If $a, b \in F$, and F has characteristic p, then

$$(a+b)^p = a^p + b^p \quad \text{and} \quad (ab)^p = a^p b^p$$

Proof $(a+b)^p = a^p + pa^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \cdots + \binom{p}{p-2}a^2b^{p-2} + pab^{p-1} + b^p$

$= a^p + b^p$ because $\binom{p}{k} = \frac{p(p-1)(p-2)\cdots(p-k+1)}{k!}$ is a multiple of p when $k < p$.

Consequence:

Frobenius Map: If $ch(F) = p$ the map $\varphi : F \to F$ where $\varphi(x) = x^p$ is an injective homomorphism.

Example $F = \mathbb{F}_2[x]/(x^2+x+1) = \{0, 1, x, 1+x\}$

$0 \xrightarrow{\varphi} 0$

$1 \longrightarrow 1$

$x \longrightarrow x$

$x+1 \longrightarrow x+1$

Consequence If F is a finite field, then Frobenius map is surjective. Hence for every $a \in F$, $a = b^p$ for some b.

Now we can prove an analog of Corollary 34 for finite fields.

Proposition 37 Suppose F is a finite field. Then

1. Any irreducible $f(x) \in F[x]$ is separable
2. $f(x)$ separable $\iff$ $f(x)$ is a product of distinct irreducibles.

Proof of (1). Suppose $f(x)$ is irreducible, hence prime.
If $f(x)$ is linear, it's separable! Thus suppose $\deg f > 1$.

CASE I $f'(x) \neq 0$. Then $\gcd(f(x), f'(x)) = 1$.
Now apply Proposition 33

CASE II $f'(x) = 0$. Then

$$\begin{aligned} f(x) &= a_0 + a_1 x^p + a_2 x^{2p} + \cdots + a_n x^{np} \\ &= b_0^p + b_1^p x^p + b_2^p x^{2p} + \cdots + b_n^p x^{np} \\ &= b_0^p + (b_1 x)^p + (b_2 x^2)^p + \cdots + (b_n x^n)^p \\ &= (b_0 + b_1 x + b_2 x^2 + \cdots + b_n x^n)^p \end{aligned}$$

But this is impossible because $f(x)$ is irreducible.
Case II can't happen — only Case I. ∎

Thus we have seen that as long as F is not an infinite field of characteristic $p < \infty$, we have

$$\left(f(x) \text{ irreducible}\right) \Rightarrow \left(f(x) \text{ separable}\right) \iff \left(\begin{array}{c} f(x) \text{ is a product} \\ \text{of distinct} \\ \text{irreducibles} \end{array}\right)$$