Separable Extensions

For $f \in F[x]$ and $\beta_1, \dots, \beta_r$ distinct in L/F s.t.

$$f = a_0 (x-\beta_1)^{m_1} \cdots (x-\beta_r)^{m_r}, \quad a_0 \in F,\ m_1, \dots, m_r \geq 1$$

call m_i the multiplicity of β_i. Say β_i is a simple root if $m=1$ and a multiple root if $m_i > 1$.

Defn A poly $f \in F[x]$ is separable if it is nonconstant and its roots in a splitting field are all simple.

Slogan Separable = distinct roots

e.g. $x^2 - 2x + 1 = (x-1)^2$ is not separable

Recall discriminant $\Delta(f)$ of a monic $f \in F[x]$ of deg > 1:

$$\Delta(f) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 \quad \text{when } f = (x-\alpha_1)\cdots(x-\alpha_n)$$

Prop If $f \in F[x]$ is monic and nonconst, then TFAE:

(a) f is separable

(b) $\Delta(f) \neq 0$

(c) f and f' (the derivative of f) are relatively prime in $F[x]$.

Pf Trivially true if $\deg(f) = 1$ since $\Delta(f) = 1$ by convention in this case. Suppose $n = \deg(f) > 1$. (a) $\iff$ (b) clear. ~~Not sure about (a) $\Rightarrow$ (c)~~

Let L be a splitting field of f/F so that $f = (x-\alpha_1)\cdots(x-\alpha_n) \in L[x]$. For a given i, write $f(x) = (x-\alpha_i) h_i(x)$, so $h_i(x) = \prod_{j \neq i} (x-\alpha_j)$. By the product rule, $f'(x) = (x-\alpha_i) h_i'(x) + h_i(x)$. Eval'n at α_i gives $f'(\alpha_i) = h_i(\alpha_i)$. If (c) is false, then f, f' have a common factor g of pos degree. Since $g \mid f$, $g(\alpha_i) = 0$ for some i, and then $g \mid f'$ implies $f'(\alpha_i) = 0$. Hence $0 = f'(\alpha_i) = \prod_{j \neq i} (\alpha_i - \alpha_j)$

$\Rightarrow \alpha_i = \alpha_j$ for some $j \neq i$.

If (c) is true, then $1 = Af + Bf'$ for some $A, B \in F[x]$. Eval'n at α_i gives $1 = B(\alpha_i) f'(\alpha_i)$, so $f'(\alpha_i) \neq 0$, so $\prod_{j \neq i} (\alpha_i - \alpha_j) \neq 0 \quad \forall i$
$\Rightarrow \alpha_1, \dots, \alpha_n$ are distinct. □

Defn For L/F an alg extn,

(a) $\alpha \in L$ is separable over F if $m_{\alpha, F}$ is sep $/F$;

(b) L/F is a separable extension if every $\alpha \in L$ is sep $/F$.

Lemma A nonconstant $f \in F[x]$ is separable iff f is a product of irred polys, each of which is separable and no two of which are multiples of each other. □

Lemma Let $f \in F[x]$ be an irred poly of degree n. Then f is separable if either of the following conditions is satisfied:

(a) F has characteristic 0, or

(b) F has char $p > 0$ and $p \nmid n$.

Pf Let $f = a_0 x^n + \cdots + a_{n-1} x + a_n$, $n > 0$, $a_0 \neq 0$. Then
$f' = n a_0 x^{n-1} + \cdots + a_{n-1}$. By (a) or (b), $n \neq 0 \in F$, so
$a_0 \neq 0 \Rightarrow n a_0 \neq 0 \Rightarrow f' \neq 0$ of deg $n-1$. By irred of f,
$\gcd(f, f') = 1$ or f. Deg of $\gcd \leq n-1$, so in fact $= 1$. □

e.g. $x^n - 1 \in F[x]$ is nonseperable iff $\text{char}(F) = p \mid n$.

Characteristic 0

Cor If $\text{char}(F) = 0$, then

(a) every irred in $F[x]$ is separable

(b) every alg extn of F is separable

(c) a nonconst $f \in F[x]$ is separable iff f is a product of irred polys, no two of which are multiples of each other. □

Prop Let $\text{char } F = 0$, $f \in F[x]$ have fact'n $f = c g_1^{n_1} \cdots g_s^{n_s}$, $c \in F$, $g_i \in F[x]$ monic irred distinct. Then
$\frac{f}{\gcd(f, f')} = c g_1 \cdots g_s$ and $g_1 \cdots g_s$ is sep $/F$ w/ same roots as f in a splitting field.

Pf Reading: pp 112-113.

eg. $f = x^{11} - x^{10} + 2x^8 - 4x^7 + 3x^5 - 3x^4 + x^3 + 3x^2 - x - 1 \in \mathbb{Q}[x]$.

Then $\gcd(f, f') = x^6 - x^5 + x^3 - 2x^2 + 1$ (Euclidean algorithm) so

$\frac{f}{\gcd(f,f')} = x^5 + x^2 - x - 1$ is sep w/ same roots as f.

Characteristic $p > 0$

Lemma char $F = p > 0$, $\alpha, \beta \in F$, then $(\alpha+\beta)^p = \alpha^p + \beta^p$, $(\alpha-\beta)^p = \alpha^p - \beta^p$.

Pf Binomial thm + $p \mid \binom{p}{r}$ for $1 \le r \le p-1$. □

$(\alpha\beta)^p = \alpha^p \beta^p$ so $\alpha \mapsto \alpha^p$ is a homomorphism called the Frobenius homomorphism

HW Hint Use this to think about $x^3 - t$ / $\mathbb{F}_3$.

$f = x^3 - t \in F[x]$, $F = k(t)$, char $k = p$ is nonseparable and irred.