13.5 Separable extensions.

Outlook towards Galois Theory. Study K/F via the group

$$\mathrm{Aut}\,(K/F) := \{\sigma\colon K \to K \mid \sigma \text{ is a field automorphism and } \sigma|_F = \mathrm{id}_F\}.$$

Lemma. *Let $\varphi\colon F \to F'$ be an isomorphism, K the splitting field of $f(x) \in F[x]$, K' the splitting field of $\varphi(f)(x) \in F'[x]$. Then*

$$|\{\sigma\colon K \to K' \mid \sigma \text{ is an isomorphism}, \sigma|_F = \varphi\}| \le [K:F]$$

with equality iff f has no multiple roots in K.

Proof. by induction on $[K:F]$.

Assume $[K:F] > 1$. Then

$$f(x) = p(x)\,q(x)$$

for $p(x) \in F[x]$ irreducible, $\deg p > 1$.

Fix $\alpha \in K$ with $p(\alpha) = 0$. For each $\beta \in K'$ with $\varphi(p)(\beta) = 0$, we have an extension

$$\begin{tikzcd} K & & K' \\ F(\alpha) \arrow[u, phantom, "\subseteq" rotate=90] \arrow[rr, "\hat\varphi_{\alpha,\beta}"] & & F'(\beta) \arrow[u, phantom, "\subseteq" rotate=90] \\ F \arrow[u, hook] \arrow[rr, "\varphi"] & & F' \arrow[u, hook] \end{tikzcd}$$

choices for $\hat\varphi_{\alpha,\beta}$ are # roots of $\varphi(p) \le [F(\alpha):F]$.

Hence by induction assumption

$$|\{\sigma : K \to K' : \sigma|_F = \varphi\}| \le [F(\alpha):F] \cdot [K:F(\alpha)] = [K:F]$$

with equality iff all roots of f are distinct. $\square$

Corollary. *Let K be a splitting field of $f(x) \in F[x]$. Then*

$$|\mathrm{Aut}\,(K/F)| \le [K:F]$$

with equality iff f has no multiple roots in K.

Separable polynomials.

Definition. $f \in F[x]$ is *separable* if f has no multiple roots in any splitting field K (By the uniqueness of splitting fields, the choice of K does not matter).

Definition. The *derivative*

$$D_x\colon F[x] \to F[x], \ \sum_{i=0}^{n} a_i x^i \mapsto \sum_{i=1}^{n} i a_i x^{i-1},$$

is an F-vector space homomorphism (not a ring homomorphism).

$D_x(f \cdot g) = D_x(f)\, g + f\, D_x(g)$

Lemma. *$f \in F[x]$ is separable iff* $\gcd(f, D_x(f)) = 1$.

Proof. Let $f(x) = (x-\alpha)^n g(x)$, $n \geq 1$,
over the splitting field K/F.
Then $D_x(f(x)) = n(x-\alpha)^{n-1} g(x) + (x-\alpha)^n D_x(g(x))$
Then $(x-\alpha) \mid D_x(f(x))$ iff $n \geq 2$.
Hence $f(x), D_x(f(x))$ have a common factor iff $f(x)$ is not separable. □

Irreducible vs separable.

Theorem. *Assume* $\mathrm{ch}(F) = 0$. *Then* $f(x) \in F[x]$ *is separable iff* $f(x)$ *is the product of distinct irreducibles in* $F[x]$.

Proof. $\Rightarrow$ ✓

$\Leftarrow$ Suffices to show that $f(x)$ irreducible is separable.
Assume $\deg f(x) = n > 0$.
Then $\deg D_x(f(x)) = n-1$ $(*)$
$0 \neq D_x(f(x)) \nmid f(x)$
Since $f(x)$ is irreducible, $\gcd(f(x), D_x(f(x))) = 1$ □

Note: The proof fails in characteristic $p > 0$ exactly if $D_x(f(x)) = 0$ (see $(*)$)
i.e., $f(x) = g(x^p)$.

Finite fields.

Let F be a finite field. Then

- $\mathrm{ch}F = p$ is prime,
- F is an extension of its prime subfield F_p, hence $|F| = p^{[F:F_p]}$.

Theorem. *For any prime power q, there exists a unique (up to isomorphism) field F_q of order q.*

Proof. Let K be the splitting field of $x^q - x \in F_p[x]$ (assuming $q = p^n$).

$\gcd(x^q - x, qx^{q-1} - 1) = \gcd(x^q - x, -1) = 1$

So $x^q - x$ is separable and has q distinct roots in K.

Claim: $F_q := \{\alpha \in K : \alpha^q = \alpha\}$ is a field of order q.

For roots α, β we have $\alpha^q = \alpha$, $\beta^q = \beta$.

Then $(\alpha\beta)^q = \alpha\beta$, $\alpha^{-q} = \alpha^{-1}$ if $\alpha \neq 0$, $(\alpha+\beta)^q = \alpha^q + \underbrace{\binom{q}{1}}_{=0}\alpha^{q-1}\beta + \dots + \underbrace{\binom{q}{q-1}\alpha\beta^{q-1}}_{=0} + \beta^q$

$= \alpha^q + \beta^q = \alpha + \beta$

Since $x^q - x$ splits in $F_q \leq K$, we have $F_q = K$.

Assume L is a field of size q. Then $x^{q-1} = 1$ for all $x \in L^*$. Then all elements of L satisfy $x^q = x$, i.e., L is the splitting field of $x^q - x$. So $L \cong F_q$. □

Theorem. *F_q^* is cyclic.*

Proof. Since F_q^* is abelian

$F_q^* \cong \mathbb{Z}_{p_1^{n_1}} \times \dots \times \mathbb{Z}_{p_k^{n_k}}$ for primes $p_1, \dots, p_k$.

$m := \exp F_q^* = \mathrm{lcm}(p_1^{n_1}, \dots, p_k^{n_k}) \leq \prod p_i^{n_i} = q - 1$

For $\alpha \in F_q^*$, we have $\alpha^m = 1$

Since $x^m - 1$ has at most m roots, it follows that $m = q-1$.

Hence F_q^* is the direct product of cyclic groups of coprime order, hence cyclic. □

Frobenius endomorphism.

Definition. Let F be a field of characteristic $p > 0$. Then

$$\varphi\colon F \to F,\ x \mapsto x^p,$$

is the *Frobenius endomorphism* of F.

(1) Homomorphism property and injectivity is straightforward.
(2) If F is finite, then φ is an automorphism.

Perfect fields.

Definition. A field F of characteristic $p > 0$ is *perfect* if

$$F = \{x^p \ : \ x \in F\}$$

(i.e. the Frobenius endomorphism is surjective).
Fields of characteristic 0 are also *perfect.*

Theorem. *Every irreducible polynomial over a perfect field is separable.*

Proof. Assume $\operatorname{ch} F = p > 0$.
Suppose $f(x) \in F[x]$ is irreducible but not separable.
Recall: Then $D_x f(x) = 0$ and

$$f(x) = a_0 + a_1 x^p + a_2 x^{2p} + \dots + a_k x^{kp}$$

Since F is perfect, $\forall i \ \exists b_i \in F: \ a_i = b_i^p$

$$f(x) = b_0^p + b_1^p x^p + \dots + b_k^p x^{kp}$$
$$= (b_0 + b_1 x + \dots + b_k x^k)^p$$

Contradicting that f is irreducible. □

Theorem. *Let F be of characteristic p and $f(x) \in F[x]$ irreducible.*
Then $\exists$ unique $k \geq 0$ and unique irreducible, separable $g(x) \in F[x]$ such that

$$f(x) = g(x^{p^k}).$$

k is then called the separable degree *of $f(x)$.*

Proof. If $f(x)$ is separable, then $g = f$, $k = 0$.
Else $f(x) = g_1(x^p)$; if $g_1(x)$ is not separable, then

$$f(x) = g_2(x^{p^2})$$

Repeat.

$$\deg f > \deg g_1 > \deg g_2 > \dots$$

So there exists some $g_k(x^{p^k}) = f(x)$ and g_k is separable.
$g_k(x)$ is irreducible since f is. □

Example. Let $K := F_p(t)$ be the field of fractions for $F_p[t]$.

K is not perfect.
$f(x) = x^p - t$ is irreducible in $K[x]$ (by Eisenstein)
$D_x f(x) = 0$, so $f(x)$ is not separable,
for $g_1(x) = x - t$ we see that $f(x)$ has separable degree 1.

Definition. An algebraic extension K/F is *separable* if $m_{\alpha,F}(x)$ is separable for all $\alpha \in K$.

Example. Every algebraic extension of a perfect field is separable.