13.5

Separable & Inseparable Extensions

Separable Extensions

Def. (Separable Polynomials)

A polynomial over F is <u>separable</u> if it has no multiple roots (i.e. all roots are distinct). A polynomial that isn't separable is called <u>inseparable</u>.

Ex. (1) The polynomial x^2-2 over $\mathbb{Q}$ is separable, since its roots $\pm\sqrt{2}$ are distinct. $(x^2-2)^n$ for $n>1$ is inseparable since it has 2 roots $\pm\sqrt{2}$, both of multiplicity n.

(2) The polynomial $x^2-t \in \mathbb{F}_2[x]$ is inseparable: if $\sqrt{t}$ denotes a root in an extension of $\mathbb{F}_2$,

$$(x-\sqrt{t})^2 = x^2-2\sqrt{t}x+t = x^2+t = x^2-t,$$

so x^2-t only has a root $\sqrt{t}$ of multiplicity 2.

- Checking separability of polynomials:

Def. The derivative of the polynomial

(Calculus?)

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in F[x]$$

is $$D_x f(x) = n a_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + 2a_2 x + a_1 \in F[x].$$

※ The derivative formulas in calculus are the same as the derivative formulas in algebra:

$$D_x(f(x)+g(x)) = D_x f(x) + D_x g(x)$$
$$D_x(f(x)g(x)) = f(x)D_x g(x) + (D_x f(x))g(x)$$

which can be proven directly from polynomials.

#1 Prop. (Separability & Derivatives)

A polynomial $f(x)$ has a multiple root α if and only if α is also a root of $D_x f(x)$, i.e. $f(x)$ and $D_x f(x)$ are both divisible by the minimal polynomial for α. In particular, $f(x)$ is separable if and only if it is relatively prime to its derivative: $(f(x), D_x f(x)) = 1$.

"Only if":

Proof. Suppose α is a multiple root of $f(x)$. Then over a splitting field,

$$f(x) = (x-\alpha)^n g(x)$$

for some integer $n \geq 2$ and polynomial $g(x)$. Taking derivatives we obtain

$$D_x f(x) = n(x-\alpha)^{n-1} g(x) + (x-\alpha)^n D_x g(x)$$

so for $n \geq 2$, $D_x f(x)$ has α as a root.

"If": Conversely, suppose that α is a root of both $f(x)$ and $D_x f(x)$. Write

$$f(x) = (x-\alpha)h(x)$$

and take the derivative $D_x f(x) = (x-\alpha) D_x h(x) + h(x)$.

Since $(x-\alpha)$ is a factor of $D_x f(x)$, $(x-\alpha)$ is a factor of $h(x)$. Then

$$f(x) = (x-\alpha)^2 h_1(x) \quad \text{for some } h_1(x).$$

Therefore α is a multiple root of $f(x)$.

Ex. (1) The polynomial $x^{p^n} - x$ over $\mathbb{F}_p$ has derivative $p^n x^{p^n - 1} - 1 = -1$. Since this derivative has no roots, $x^{p^n} - x$ is separable.

(2) The polynomial $x^n - 1$ has derivative nx^{n-1}. Over any field of characteristic not dividing n (including $\mathrm{ch}(F) = 0$), nx^{n-1} has only root 0, which is not a root of $x^n - 1$. Therefore $x^n - 1$ is separable, and there are n distinct roots of unity.

(3) If F is of characteristic p & p|n, then there are fewer than n distinct roots of unity over F. The derivative $nx^{n-1} = 0$ since $n = 0$ in F, so every root of $x^n - 1$ is multiple.

18.23)

#1 Cor. Every irreducible polynomial over a field of characteristic 0 (e.g. $\mathbb{Q}$) is separable. A polynomial over such a field is separable if and only if it is the product of distinct irreducible polynomials.

Proof: Suppose F is a field of characteristic 0 and $p(x) \in F[x]$ is an irreducible polynomial with degree n. Then its derivative $D_x p(x)$ has degree $n-1$. Since the factors of $p(x)$ over F are 1 and $p(x)$, $D_x p(x)$ and $p(x)$ are coprime. Therefore $p(x)$ is separable. ☺

This also applies to products of distinct irreducible polynomials since they do not have zeros in common. ☺

☺ See this proposition on P570:

A polynomial $f(x) \in F[x]$ has α as a root if and only if $m_{\alpha,F}(x)$ divides $f(x)$ in $F[x]$.

Since the factors of irreducible $p(x) \in F[x]$ are uniquely 1 and $p(x)$ (and $m_{\alpha,F}(x) = p(x)$ for any root α of $p(x)$), distinct irreducible polynomials do not have common roots.

☺ Where is the converse?

Suppose $p(x) \in F[x]$ ($ch(F) = 0$) is separable. Then we can factor $p(x)$ over F into the products of irreducible polynomials

Proof (by contradiction): Suppose an irreducible factor $g(x)$ has multiplicity ≥ 2. Then the roots of $p(x)$ given by the roots of $g(x)$ have multiplicity ≥ 2, contradicting separability of p.

$\Rightarrow$ $p(x)$ is the product of <u>distinct</u> irreducible polynomials.

※ Why this fails in $ch(F) = p$:

In $ch(F) = p$, the derivative of deg $p(x) = n$ isn't necessarily of degree $n-1$. Consider, for example:

$$D_x x^{pm} = pm(x^{pm-1}) = 0.$$

If we add the condition that $D_x p(x) \neq 0$, then the corollary stands.

Note that if $D_x f(x) = 0$ over F with $ch(F) = p$, then $f(x)$ must be of the form

$$f(x) = a_m x^{pm} + a_{m-1} x^{p(m-1)} + \cdots + a_1 x^m + a_0$$

where all indices of x are multiples of p.

#2 Prop. (Cool result in field with characteristic p.)

Let $ch(F) = p$. Then for $a, b \in F$,

$$(a+b)^p = a^p + b^p \quad ; \quad (ab)^p = a^p b^p.$$

Proof. (1) Binomial Expansion:

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

All of $\binom{p}{1}, \ldots, \binom{p}{p-1}$ are multiples of p, so they are identically 0 in F. Therefore $(a+b)^p = a^p + b^p$.

(2) Multiplication is commutative by field axioms.

※ This gives an injective homomorphism $\varphi(a) = a^p$ from F to F.

Def (Frobenius Endomorphism)

The map $\varphi: F \to F$ for field of characteristic p

$$\varphi(a) = a^p$$

is called the Frobenius Endomorphism of F.

#2 Cor. (Applying Frobenius Endomorphism)

Suppose F is a field, $ch(F) = p$. Then every element of F is a p^{th} power in F, i.e. $F = F^p$.

Proof. Since the Frobenius endomorphism is injective, and $|F| = |F^p|$ when F is finite, so φ is also surjective.

#3 Prop. (Extension of #1 Prop.)

Every irreducible polynomial over a finite field F is separable. A polynomial in $F[x]$ is separable if and only if it's a product of distinct irreducible polynomials in $F[x]$.

Proof. (by contradiction)

Let F be a finite field and $p(x) \in F[x]$ be an irreducible polynomial. Suppose, for a contradiction, that $p(x)$ is inseparable. Then as seen in #1 Prop., $p(x) = q(x^p)$ for some $q(x) \in F[x]$. Let

$g(x) = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0$.

Then $p(x) = a_m x^{pm} + a_{m-1} x^{p(m-1)} + \cdots + a_1 x^p + a_0$.

By #2 Cor, each coefficient $a_0, \ldots, a_m$ is a power of p in F:

$$\begin{aligned} p(x) &= (b_m)^p (x^m)^p + (b_{m-1})^p (x^{m-1})^p + \cdots + b_1^p x^p + b_0^p \\ &= (b_m x^m)^p + (b_{m-1} x^{m-1})^p + \cdots + (b_1 x)^p + b_0^p \\ &= (b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0)^p \end{aligned}$$

contradicting irreducibility of p.

$\Rightarrow p(x)$ is separable.

Def. (Perfect Fields)

A field K of characteristic p is called perfect if every element of K is a pth power in K, i.e. $K = K^p$. Any field of characteristic 0 is also perfect.

$\Rightarrow$ Examples of perfect fields: all finite fields, fields with characteristic 0

Ex. (Existence & Uniqueness of Finite Fields) I Love this Theorem ♡

- Existence: Let $n > 0$ be any integer and consider $x^{p^n} - x \in F_p[x]$.

This polynomial is separable (it is equal to $x(x^{p^n-1} - 1)$) and therefore has p^n distinct roots.

Consider the splitting field of $x^{p^n} - x$ over $F_p[x]$. Let α, β be roots of $x^{p^n} - x$. Since $\alpha^{p^n} = \alpha$ and $\beta^{p^n} = \beta$,

$$(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta, \quad (\alpha^{-1})^{p^n} = \alpha^{-1} \text{ and } (\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta,$$

so the set F containing all the roots of $x^{p^n} - x$ is closed under addition, multiplication & inverses, and F is a field. Since F is a subfield of the splitting field, F is the splitting field.

Since $|F| = p^n$, there exists finite fields of order p^n for any prime p and integer n. We can obtain a field of order p^n by finding the splitting field of the polynomial $x^{p^n} - x$ over F_p.

In addition, since $[F : F_p] = n$, there exists finite fields of degree n over F_p for any $n > 0$.

- Uniqueness: Let F be a field of characteristic p. If $[F : F_p] = n$ where F_p is the prime subfield of F, then $|F| = p^n$. Since the multiplicative group $F^\times$ has order $p^n - 1$, $\alpha^{p^n - 1} = 1$ for any $\alpha \in F^\times$, giving $\alpha^{p^n} = \alpha$. Then α is an element in the splitting field of $x^{p^n} - x$ over F_p, which has precisely order p^n. Then F is a splitting field of $x^{p^n} - x$, and is unique up to isomorphism by the properties of splitting fields.

- Conclusion: There exists a unique field of order p^n for prime p and any integer n.

#4 Prop: (More on inseparable irreducible polynomials)

Let $p(x)$ be an irreducible polynomial over a field F of characteristic p. Then there is a unique integer $k \geq 0$ & a unique irreducible separable polynomial $p_{sep}(x) \in F[x]$ s.t.

$$p(x) = p_{sep}(x^{p^k})$$

(18.v5)

Proof: (Similarly to descent but not really)

-Case #1. $p(x)$ is inseparable.

Then $D_x p(x)$ is identically 0 (we have seen this earlier), so $p(x) = p_1(x^p)$ for some $p_1(x) \in F[x]$. $p_1(x)$ may or may not be separable; if $p_1(x)$ is inseparable, then repeat the process to get $p_1(x) = p_2(x^p)$ for some $p_2(x) \in F[x]$. At some point we have $p(x) = p_k(x^{p^k})$ for some $k > 0$, $p_k(x) \in F[x]$, where $p_k(x)$ is irreducible and separable.

$\Rightarrow p(x) = p_{sep}(x^{p^k})$ for some $k > 0$, $p_{sep}(x) \in F[x]$ & irreducible.

-Case #2. $p(x)$ is separable.

The statement is proven by setting $k = 0$ and $p_{sep}(x) = p(x)$. □

Def (Separable & Inseparable Degrees)

Let $p(x)$ be an irreducible polynomial over a field of characteristic p. The degree of $p_{sep}(x)$ (see #4 Prop.) is called the <u>separable degree</u> of $p(x)$, denoted $\deg_s p(x)$; the integer p^k for inseparable $p(x)$ is the <u>inseparable degree</u> of $p(x)$, denoted $\deg_i p(x)$.

※ $\deg p(x) = \deg_s p(x) \deg_i p(x)$.

Ex. (1) The polynomial $p(x) = x^2 - t \in \mathbb{F}_2[x]$ has $\deg_s(x) = 1$ and $\deg_i(x) = 2$. Consider $p_{sep}(x) = x - t$ with $\deg_s(x) = 1$. Then $p(x) = p_{sep}(x^2)$ so $\deg_i(x) = 2$. This is verified by $\deg p(x) = \deg_s p(x) \deg_i p(x) = 2$.

(2) The polynomial $p(x) = x^{2^m} - t \in \mathbb{F}_2[x]$ has $\deg_s(x) = 1$ and $\deg_i(x) = 2^m$, similarly $p_{sep}(x) = x - t$.

(3) The polynomial $(x^{p^2} - t)(x^p - t)$ over $\mathbb{F}_p(x)$ has 2 irreducible & inseparable factors and is therefore inseparable. This polynomial has no equiv. form in $f_{sep}(x^{p^k})$ where $f_{sep}(x)$ is separable, since $(x^{p^2} - t)(x^p - t)$ is reducible.

Def (Separable Fields.)

The field K is said to <u>separable</u> over F if every element of K is the root of a separable polynomial over F (= the minimal polynomial of every element over F is separable). Otherwise the field is <u>inseparable</u>.

#3 Cor (Which Fields are separable ?)

Every finite extension of a perfect field is separable. In particular, every finite extension of either $\mathbb{Q}$ or a finite field is separable.

<u>Reasoning</u>. All minimal polynomials over any field F is irreducible (by def. of a minimal polynomial). In perfect fields, irreducibility implies separability, completing the proof.