

# Advanced Algebra II

## SEPARABILITY AND INSEPARABILITY

We first recall something about separable extension.

To start with, let  $f(x)$  be an irreducible polynomial in  $K[x]$  and  $f'(x)$  be its derivative (formally). More precisely, if  $f(x) = \sum_{i=0}^n a_i x^i$ , then  $f'(x) := \sum_{i=1}^n i a_i x^{i-1}$ . One has the following equivalence:

- (1)  $f(x)$  is separable, i.e. no multiple roots in  $\overline{K}$ .
- (2)  $(f(x), f'(x)) = 1 \in \overline{K}[x]$ .
- (3)  $(f(x), f'(x)) = 1 \in K[x]$ .
- (4)  $f'(x) = 0$ .

Therefore, the only possibility to have non-separable polynomial is  $\text{char}(K) = p$  and  $f(x) = g(x^p)$ .

Given an element  $u$  algebraic over  $K$ , one can define the separable degree to be the number of distinct roots of minimal polynomial. This notion can be extended to a general setting:

**Definition 0.1.** Let  $F/K$  be an extension. Fix an embedding  $\sigma : K \rightarrow L = \overline{L}$ . We define the separable degree of  $F/K$ , denoted  $[F : K]_s$ , to be the cardinality of

$$S_\sigma := \{\tau : F \rightarrow L \mid \tau|_K = \sigma\}.$$

One can check that  $[F : K]_s$  is independent of  $\sigma$  and  $L$ . Hence the definition is well-defined. Moreover, if  $F = K(u)$  for  $u$  algebraic over  $K$ , then  $[F : K]_s = [K(u) : K]_s$  is the number of distinct roots of the minimal polynomial  $p(x)$  of  $u$ . (By considering  $K$ -embedding  $\tau : K(u) \rightarrow \overline{K}$ ,  $\tau(u)$  must be a root of  $p(x)$  and  $\tau$  is determined by  $\tau(u)$ ).

**Proposition 0.2.** If  $K \subset E \subset F$ , then  $[F : K]_s = [F : E]_s [E : K]_s$ . Moreover, if  $F/K$  is finite, then  $[F : K]_s \leq [F : K]$ .

Then we have the following useful criterion:

**Proposition 0.3.** If  $F/K$  is finite, then  $F/K$  is separable if and only if  $[F : K]_s = [F : K]$ .

we can then prove the following:

**Theorem 0.4.** Suppose that  $F = K(S)$  such that each elements of  $S$  is separable over  $K$ , then  $F/K$  is separable.

In particular, let

$$S := \{u \in F \mid u \text{ is separable over } K\}.$$

Then  $S$  is a field extension over  $K$ . And we have

$$[F : K]_s = [S : K]_s = [S : K] [F : K].$$

On the other hand, one have proved the following Proposition which actually gives the definition of inseparable degree

**Proposition 0.5.** *If  $F/K$  is a finite extension, then  $[F : K]_s | [F : K]$ . Moreover,  $[F : K]/[F : K]_s = p^n$  for some  $n$ .*

Before we move onto the study of inseparability, we would like to prove the famous theorem of primitive element.

**Proposition 0.6.** *If  $K$  is a finite field and  $F/K$  is an algebraic field extension. The following are equivalent:*

- (1)  $F/K$  is finite.
- (2)  $F = K(\alpha)$  for some  $\alpha \in F$ . That is,  $F/K$  is a simple extension.
- (3) There is only finitely many intermediate fields.

*Proof.* For (1)  $\Rightarrow$  (2), if  $F/K$  is finite, then  $F$  is finite.  $F^*$  is a cyclic multiplicative group, say  $F^* = \langle \alpha \rangle$ . Then it's clear that  $F = K(\alpha)$ .

(2)  $\Rightarrow$  (1) is trivial.

(1)  $\Rightarrow$  (3). Suppose that  $|K| = q$ ,  $|F| = q^n$ . Let  $E$  be an intermediate field, then it's clear that  $|E| = q^d$  for some  $d|n$ . One can prove that for any  $d|n$ , there is exactly one intermediate field with  $q^d$  elements. Hence there are only finitely many intermediate fields.

(3)  $\Rightarrow$  (1). Suppose on the other hand that  $F/K$  is not finite. Then  $F/K$  is not finitely generated. We can easily get (by axiom of choice) a infinite sequence of intermediate fields

$$K \subset K(a_1) \subset K(a_1, a_2) \dots$$

by adding generators. □

**Proposition 0.7.** *Let  $F/K$  be a finite extension, then  $F = K(\alpha)$  if and only if there is only finitely many intermediate fields.*

*Proof.* If  $K$  is finite, then we are done by the previous Proposition. We assume that  $K$  is infinite.

Suppose that there is only finitely many intermediate fields. For any  $\alpha, \beta \in F$ , we can consider intermediate fields  $K(\alpha + c\beta)$  as  $c$  ranging in  $K$ . Since  $K$  is infinite. There must exist  $c_1, c_2 \in K$  such that  $K(\alpha + c_1\beta) = K(\alpha + c_2\beta)$ . It's easy to check that

$$K(\alpha, \beta) = K(\alpha + c\beta).$$

By induction on number of generators of  $F/K$ , we proved that  $F/K$  is a simple extension.

Suppose now that  $F = K(\alpha)$ . We would like to prove the finiteness by using the following map:

$$\phi : \{E | K \subset E \subset F\} \rightarrow S := \{p_E(x)\},$$

where  $p_E(x)$  denotes the minimal polynomial of  $\alpha$  over  $E$ . Since every  $p_E(x)$  is a divisor of  $p_K(x)$  in the algebraic closure (or in the splitting field), it's clear that  $S$  is finite.

It's enough to prove that  $\phi$  is injective. To this end, let  $E_0$  be the extension over  $K$  generated by coefficient of  $p_E(x)$ . One sees that

$p_E(x) \in E_0[x]$  is irreducible and hence a minimal polynomial of  $\alpha$ . Hence we have

$$[K(\alpha) : E] = \deg(p_E(x)) = [K(\alpha) : E_0].$$

It follows that  $E = E_0$ . Thus, if  $\phi(E) = \phi(E')$ , then  $E = E_0 = E'$ . This proved the injectivity.  $\square$

**Theorem 0.8.** *If  $F/K$  is separable and finite, then  $F = K(\alpha)$  for some  $\alpha \in F$ .*

*Proof.* We may assume that  $K$  is infinite. By induction on generators of  $F/K$ , we may assume that  $F = K(\alpha, \beta)$ . Let  $n := [F : K]_s$ , and  $\sigma_1, \dots, \sigma_n$  be the distinct embedding of  $F$  in  $\overline{K}$ . Let

$$P(x) := \prod_{i \neq j} (\sigma_i \alpha + \sigma_i \beta x - \sigma_j \alpha - \sigma_j \beta x).$$

Since  $\deg(P(x)) = n(n-1)$  and there are infinitely many elements in  $K$ , there must be an  $c \in K$  such that  $P(c) \neq 0$ . Thus all  $\sigma_i(\alpha + c\beta)$  are all distinct. This gives  $n$  distinct embedding of  $K(\alpha + c\beta)$ . One has

$$n = [F : K]_s \leq [K(\alpha + c\beta) : K]_s.$$

Since  $F/K$  is separable, so is  $K(\alpha + c\beta)$ . It's easy to see that  $F = K(\alpha + c\beta)$ .  $\square$

**Definition 0.9.** *Let  $F/K$  be an extension. An element  $u \in F$  is purely inseparable over  $K$  if its minimal polynomial  $p(x) \in K[x]$  factors in  $F[x]$  as  $(x - u)^m$ . An extension  $F/K$  is purely inseparable over  $K$  if every element of  $F$  is purely inseparable over  $K$ .*

It's easy to see that an element  $u \in F$  which is both separable and purely inseparable over  $K$  if and only if  $u \in K$ .

Another useful observation is:

**Lemma 0.10.** *Let  $F/K$  be an extension with  $\text{char}(K) = 0 \neq 0$ . If  $u \in F$  is algebraic over  $K$ , then  $u^{p^n}$  is separable over  $K$  for some  $n \geq 0$ .*

*Proof.* The point is that if  $u$  is not separable, then its minimal polynomial  $p(x)$  is of the form  $f(x^p)$ . Then  $f(x)$  is the minimal polynomial of  $u^p$ . By induction on degree of  $u$ , we are done.  $\square$

Being purely inseparable has the following equivalent formulation:

**Theorem 0.11.** *Let  $F/K$  be an algebraic extension with  $\text{char}(K) = p \neq 0$ . The following are equivalent:*

- (1)  $F/K$  is purely inseparable, i.e. every element  $u \in F$  has minimal polynomial of the form  $(x - u)^m$ .
- (2) for all  $u \in F$ , the minimal polynomial is of the form  $x^{p^n} - a \in K[x]$ .
- (3) for all  $u \in F$ ,  $u^{p^n} \in K$  for some  $n \geq 0$ .

- (4)  $S = K$ , that is, the only element of  $F$  which is separable over  $K$  are the elements in  $K$ .  
 (5)  $F/K$  is generated by purely inseparable elements.

*Proof.* Let  $m = p^n r$ .

$$(x - u)^m = (x - u)^{p^n r} = (x^{p^n} - u^{p^n})^r = x^m - r u^{p^n} x^{p^n(r-1)} + \dots \in K[x].$$

Therefore,  $u^{p^n} \in K$ , this proved (1)  $\Rightarrow$  (3).

Moreover,  $p'(x) := x^{p^n} - u^{p^n} \in K[x]$  and  $p'(x)^r$  is the minimal polynomial of  $u$  (hence irreducible). Therefore,  $r = 1$ . This proved (1)  $\Rightarrow$  (2).

(2)  $\Rightarrow$  (3) is trivial.

For (3)  $\Rightarrow$  (1), let  $a = u^{p^n} \in K$ , then  $f(x) := x^{p^n} - a \in K[x]$  and factors in  $F[x]$  as  $(x - u)^{p^n}$ . Hence the minimal polynomial of  $u$  over  $K$  is a factor of  $f(x)$  and factors into  $(x - u)^m$  in  $F[x]$ .

We have seen (1)  $\Rightarrow$  (4) and (5), (4)  $\Rightarrow$  (3) follows from the above Lemma 0.10.

It remains to show that (5)  $\Rightarrow$  (3). To see this, first note that  $F = K(S)$  where  $S$  consists of elements  $u_i$  such that  $u_i^{p^n} \in K$  for some  $n$  (By the proof of (1)  $\Rightarrow$  (3)). For any  $u \in F$ , say  $u = \frac{f(u_1, \dots, u_r)}{g(u_1, \dots, u_r)}$ . Pick  $N$  such that  $u_i^{p^N} \in K, \forall i = 1, \dots, r$ . Then  $u^{p^N} \in K$ .  $\square$

As a corollary, one can show that

$$P := \{u \in F \mid u \text{ is purely inseparable over } K\}$$

is a subfield.

**Theorem 0.12.** *Let  $F/K$  be an algebraic extension. Keep the notation as above for  $S, P$ .*

- (1)  $S/K$  is separable.
- (2)  $P/K$  is purely inseparable.
- (3)  $F/S$  is purely inseparable.
- (4)  $F/P$  is separable if and only if  $F = PS$ .
- (5)  $P \cap S = K$ .
- (6) if  $F/K$  is normal, then  $S/K$  and  $F/P$  are Galois. And  $\text{Gal}_{F/K} = \text{Gal}_{F/P} \cong \text{Gal}_{S/K}$ .

*Proof.* We have seen (1), (2), (5). (3) follows from Lemm 0.10. For (4), look at  $P \subset SP \subset F$ . If  $F/P$  is separable, then  $F/SP$  is separable. Look at  $S \subset SP \subset F$  now. We have  $F/K$  is purely inseparable, thus so is  $F/SP$ . Thus  $F = SP$ .

On the other hand, if  $F = SP = P(S)$ , then clearly  $F = P(S)$  is separable over  $P$ .

Lastly, we look at  $G := \text{Gal}_{F/K}$ . We claim that  $G' = P$ , hence  $F/P$  is Galois with Galois group  $\text{Gal}_{F/P} = \text{Gal}_{F/K}$ .

To see the claim, if  $u \in P$ , then it's clear that  $\sigma(u) = u$  for all  $\sigma \in G$ . Therefore,  $P \subset G'$ . On the other hand, if  $u \in G'$  and  $v$  is another root

of  $p(x)$ , the minimal polynomial of  $u$ . There is an  $\sigma$  such that  $\sigma(u) = v$ . Since  $F/K$  is normal, this  $\sigma$  can be extended to  $G$ . But  $u \in G'$ , thus  $v = u$ , in other words,  $p(x) = (x - u)^m$ .

$F$  is Galois over  $P$  because  $P = G'$ . Hence  $F/P$  is separable. By (5),  $F = PS$ .

Lastly, we consider  $\text{Gal}_{F/P} = \text{Gal}_{F/K} \rightarrow \text{Gal}_{S/K}$  by restriction. This is well-defined since  $S$  is stable. More precisely, for  $u \in S$ ,  $\sigma(u) \in S$  for all  $\sigma \in G$  because  $\sigma(u)$  has the same minimal polynomial as  $u$  does. This is surjective by extension theorem. It remains to show the injectivity. If  $\sigma|_S = \tau|_S$ , then for all  $u \in F$  we have  $u^{p^n} \in S$ . Thus,

$$\sigma(u)^{p^n} = \sigma(u^{p^n}) = \tau(u^{p^n}) = \tau(u)^{p^n}.$$

It follows that  $\sigma(u) = \tau(u)$ .

It remains to show that  $S/K$  is Galois. To see this, suppose  $u \in S$  is fixed by all  $\sigma \in G$ , then  $u \in G' = P$ . Hence  $u \in K$ . We are done.  $\square$

If  $\text{char}(K) = p \neq 0$ , we write  $K^p = \{u^p | u \in K\}$ .

**Definition 0.13.**  $K$  is said to be perfect if  $K^p = K$

**Example 0.14.** Finite fields are perfect.

$\mathbb{Z}_p(x)$  is not perfect.

**Corollary 0.15.** Let  $F/K$  be an algebraic extension with  $\text{char}(K) = p \neq 0$ . We have

- (1) If  $F/K$  is separable, then  $F = KF^{p^n}$  for each  $n \geq 1$ .
- (2) If  $F/K$  is finite and  $F = KF^p$ , then  $F/K$  is separable.
- (3) In particular,  $u \in F$  is separable over  $K$  if and only if  $K(u^p) = K(u)$ .

Note that  $F^p$  is not necessarily an extension over  $K$ . So is  $F^{p^n}$ . But we can take  $KF^{p^n}$ , which is an extension over  $K$ .

*Proof.* We first suppose that  $F/K$  is finite, hence finitely generated. Write  $F = K(u_1, \dots, u_r)$ . It's clear that there is  $N \geq 1$  such that  $u_i^{p^N} \in S$ . Hence  $F^{p^N} \subset S$ , therefore,  $KF^{p^N} \subset S$ .

We claim that  $S = KF^{p^N}$ . To see this, one notices that  $F$  is purely inseparable over  $KF^{p^N}$ , so is  $S$  purely inseparable over  $KF^{p^N}$ . And on the other hand,  $S$  is separable over  $K$ , so is over  $KF^{p^N}$ . Hence  $S = KF^{p^N}$ .

For (1), if  $F/K$  is separable and finite, then we have  $F = KF^{p^N}$ . However, in the proof, one can choose  $N$  to be arbitrary large. More precisely, one has  $F = KF^{p^N}$  for all  $N \geq N_0$ . By looking at the inclusion

$$F = KF^{p^N} \subset KF^{p^{N-1}} \subset \dots \subset KF^p \subset F.$$

One has  $F = KF^{p^n}$  for all  $n \geq 1$ .

Suppose now that  $F/K$  is separable but not necessarily finite. For any  $u \in F$ , we consider  $F_0 := K(u)$  which is separable and finite over  $K$ . Thus  $u \in F_0 = KF_0^{p^n} \subset KF^{p^n}$  for all  $n \geq 1$ . This proves (1).

We now prove (2). If  $F = KF^p$ , then  $F = K(KF^p)^p = KF^{p^2}$ . Inductively, one has  $F = KF^{p^n}$  for all  $n \geq 1$ . Since we have shown that  $S = KF^{p^N}$ , it follows that  $F = S$ .

Apply the statement to a single element. We consider  $F = K(u)$ .  $F^p \subset K^p(u^p) \subset K(u^p)$ . Indeed,  $KF^p = K(u^p)$ . By (2), if  $K(u) = K(u^p)$ , then  $u$  is separable. By (1), if  $u$  is separable, then  $K(u) = K(u^p)$ .  $\square$