NOTES ON FIELD THEORY AND GALOIS THEORY

KAEDE

We assume rings to be commutative with unit element, which entails that we require homomorphisms to preserve the unit element.

1. BASIC DEFINITION

Definition 1.1. A ring K is called a field if $K \setminus \{0\}$ foms a group under multiplication.

By our definition, every field contains at least two elements.

Lemma 1.2. A nonzero ring R is a field if and only if it has no proper ideals.

Proof. If R is a field and I is a nonzero ideal. Take $a \in I$ and then $1 = a^{-1}a \in I$, so $I = R$.

Conversely, if R has no proper ideals. Take $a \in R \setminus \{0\}$. We have $(a) = R$ and therefore $ab = 1$ for some $b \in R$. □

As a consequence, homomorphisms of fields are always injective, since 1 never lies in the kernel. This important observation does not trivialize field theory, however

Definition 1.3. We say L/K is a field extension if there is a field homomorphism $K \to L$. If $K' \subset K$ forms a field under operations of K, K' is called a subfield of K.

Remark 1.4. If L/K is a field extension, we can always identify K with its image, which is a subfield of L. However, as we may see later, the way we embed a field into another one is usually various. So we reserve the possibility that K is not a subfield of L.

Definition 1.5. Let L/K be a field extension. A middle field of L/K is a field E which admits extensions L/E and E/K.

We investigate some basic examples.

Example 1.6. (1) Suppose A is an integral domain. Its field of fractions $\mathrm{Frac}(A)$ is a field. In particular, $\mathbb{Q} = \mathrm{Frac}(\mathbb{Z})$ is a field.
(2) Suppose $\mathfrak{m}$ is a maximal ideal in R. Then $R/\mathfrak{m}$ is a field. In particular, $\mathbb{F}_p = \mathbb{Z}/(p)$ is a field for p prime. Also $\mathbb{C} = \mathbb{R}[x]/(x^2+1)$ is constructed in this way.
(3) More generally, for every prime ideal $\mathfrak{p}$ in ring A, $\mathfrak{p}A_\mathfrak{p}$ is maximal in $A_\mathfrak{p}$. We can define the residue field of $\mathfrak{p}$ to be $\kappa(\mathfrak{p}) = A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \simeq \mathrm{Frac}(A/\mathfrak{p})$.

$\mathbb{Q}$ and $\mathbb{F}_p$ for p prime are called prime fields, since they are the smallest field as shown in the following proposition.

Proposition 1.7. Every field contains a prime field.

Proof. Let K be a field and consider the homomorphism of rings

$$\begin{aligned} \mathbb{Z} &\longrightarrow K \\ n &\longmapsto n \cdot 1 \end{aligned}$$

Notice that subring of field is integral, so the kernel is prime. If the kernel is 0, by the universal property of localization, the homomorphism extends to $\mathbb{Q} \to K$. If the kernel is (p) for some p prime, by the universal property of quotient ring, the homomorphism extends to $\mathbb{F}_p \to K$. □

Definition 1.8. Let K be a field and $\mathbb{Z} \to K$ be ring homomorphism as in Proposition 1.6. Then its kernel is (p) with either $p = 0$ or p is a prime. The unique number p is called the characteristic of K, denoted by $\mathrm{char}\, k$.

The characteristic of field, controls the operations on fields in an essential way. If a field K has $\operatorname{char} K = p > 0$, then $pa = (p \cdot 1)a = 0$ for every $a \in K$. It follows that every field contains exactly one prime field.

Proposition 1.9 (freshman's dream)**.** If a field K has $\operatorname{char} K = p > 0$, then $a \mapsto a^p$ is a field endomorphsim.

Proof. Using the binomial theorem

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}$$

It suffices to notice that p divides $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ for $1 \leqslant k \leqslant p-1$. □

Definition 1.10. If a field K has $\operatorname{char} K = p > 0$, then $a \mapsto a^p$ is called the Frobenius endomorphism.

Since field homomorphism is injective, Frobenius endomorphism becomes automorphism when the field is finite.

Definition 1.11. Let L/K be an field extension and $S \subset$. Here we take K as subset of L. The intersection of all subfields of K containing S and K is obviously the smallest subfield of K containing both S and K. We call it the subfield of L generated by S and K, and we denote it by $K(S)$. We say L is finitely generated over K if $L = K(S)$ for some S finite.

Proposition 1.12. Let L/K be a field extension and $S \subset L$. $K[S]$ is the intersection of all the subrings of L containing S and K. Then $K(S) = \operatorname{Frac}(K[S])$.

Proof. Obviously $K(S) \subset \operatorname{Frac}(K[S])$. On the other hand, for every subfield E of L containing S and K, it contains $K[S]$ automatically. By the universal property of localization, we have $\operatorname{Frac}(K[S]) \subset E$. Thus $\operatorname{Frac}(K[S]) \subset K(S)$. □

Example 1.13. (1) $\mathbb{C} = \mathbb{R}(\mathrm{i})$.
(2) $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}[x]/(x^3 - 2)$.
(3) Let k be a field. $k(x) = \operatorname{Frac}(k[x])$, where x is a indeterminate, is the field of rational functions over k. More generally we have $k(x_1, \cdots, x_n) = \operatorname{Frac}(k[x_1, \cdots, x_n])$.

Definition 1.14 (composite field)**.** Let K and K' be subfields of a field L. The intersection of the subfields of L containing K, K' is called the composite field of K, K' (in L), denoted by KK'. Obviously we have $KK' = K(K') = K'(K)$. We can define the composite field for arbitary finite many fields conained in a common field similarly.

Example 1.15. $\mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt{6}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. All fields are taken as subfields of $\mathbb{C}$.

Definition 1.16 (abstract composite field)**.** Let K and K' be fields sharing the same characteristc, so they have the common prime field k. Then K, K' are both k-algebra, which allows us to consider the tensor algebra $KK' = K \otimes_k K'$. It can be checked that KK' is indeed a field containing K, K' as subfields.

Remark 1.17. In general, the composite field and the abstract composite field is NOT isomorphic.

2. algebraic extension

In this section, suppose L/K is a field extension.

Let $\alpha \in L$, we can consider the evaluation homomorphism $K[x] \to L, g(x) \mapsto g(\alpha)$. Denote the kernel of this homomorphism by I. I is prime since the image is an integral domain. $K[x]$ is a PID, so I is either 0 or $(f(x))$ for some $f(x) \in K[x]$ irreducible.

Definition 2.1. $\alpha \in L$ is said to be algebriac over K if the kernel of the evaluation map is nonzero. Otherwise α is said to be transcendental over K.

If there exists $g(x) \in K[x]$ such that $g(\alpha) = 0$, then the kernel of the evaluation homomorphism is nonzero, and α is algebraic over K.

In algebraic number theory, a complex number is said to be algebraic or transcendental according as it is algebraic or transcendental over $\mathbb{Q}$. We are usually familiar with algebraic numbers. However, most complex numbers are transcendental.

Proposition 2.2. The set of algebraic numbers is countable. In particular, $\mathbb{C}/\mathbb{Q}$ is transcendental.

Proof. $\bigoplus_{\mathbb{N}} \mathbb{Q} \mapsto \mathbb{Q}[x], (a_i) \mapsto \sum_{\mathbb{N}} a_i x^i$ is surjective, so $\mathbb{Q}[x]$ is countable. Each polynomial admits finitely many roots in $\mathbb{C}$. Hence algebraic numbers lie in a countable union of finite sets, which is still countabe. □

Definition 2.3. An extension L/K is said to be algebraic if every element in L is algebriac over K. Otherwise L/K is said to be transcendental, or equivalently there exsists $\alpha \in L$ transcendental over K.

Proposition 2.4. Suppose $f(x) \in K[x]$ is monic and $f(\alpha) = 0$. Then the following statements are equivalent.
(1) f divides other $g \in K[x]$ such that $g(\alpha) = 0$.
(2) f is of least degree such that $f(\alpha) = 0$.
(3) $\mathrm{Ker}(K[x] \to L, g(\alpha) \mapsto g(\alpha)) = (f(x))$.

Proof. (1)⇒(2): Apply Euclid's algorithm.
(2)⇒(3): Let $\ker(K[x] \to L, g(x) \mapsto g(\alpha)) = (h(x))$. Since $f(\alpha) = 0$, we have $h|f$. Then $f = ah$ for some $a \in K^\times$ because f has the least degree and $h(\alpha) = 0$. Thus $(h) = (f)$.
(3)⇒(1) is obvious by definition. □

Definition 2.5. For $\alpha \in L$ algebraic over K, the minimal polynomial of α (over K) is the monic polynomial satisfying the equivalent conditions in Proposition 2.4.

Field extension L/K induces a K-algebra structure on L. In particular, L is a K-vector space, which is the starting point of studying finite extension.

Definition 2.6. We define the degree $[L : K]$ to be $\dim_K L$. L/K is said to be finite if $[L : K] < \infty$.

Finite field extension is something we can really compute in field theory, as shown in the following proposition.

Proposition 2.7. Suppose K/E and L/K are both finite field extension. If $\{ x_i \}$ is a K-basis of L and $\{ y_j \}$ is a E-basis of K, then $\{ x_i y_j \}$ is a E-basis of L. In particular, we have

$$[L : E] = [L : K][K : E]$$

Proof. Every $x \in L$ can be writte as

$$x = \sum_i a_i x_i = \sum_i x_i \sum_j b_{ij} y_j = \sum_{i,j} b_{ij} x_i y_j$$

where $a_i \in K$ and $b_{ij} \in L$. Hence L is generated by $x_i y_j$. On the other hand,

$$\sum_{i,j} b_{ij} b_j = \sum_i x_i \sum_j b_{ij} y_j$$

If the sum is 0, $\sum_j b_{ij} y_j$ is forced for every i and then $b_{ij} = 0$ for all i, j. We see that $x_i y_j$ is indeed a E-basis. □

Corollary 2.8. we define a tower of fields to be a sequence

$$K_1 \subset K_2 \subset \cdots \subset K_n$$

of extension fields. K_n/K_1 is finite if and only if each step is finite, in this case we say the tower is finite.

Proposition 2.9. Suppose $L = K(\alpha)$ for some α algebraic over K and $f(x)$ is the minimal polynomial of α. Then $[L : K] = \deg f$ and $L = K[\alpha]$.

Proof. Since $K[x]$ is a PID, $K[\alpha] \cong K[x]/(f(x))$ is a field. Thus $K(\alpha) = \mathrm{Frac}(K[\alpha]) = K[\alpha]$ according to proposition 1.11. Denoting $n = \deg f$ and applying Euclid's algorithm, one can check that $1, \alpha, \cdots, \alpha^{n-1}$ forms a K-basis of $K[\alpha]$. □

Proposition 2.10. L/K is finite if and only if L/K is algebriac and L is finitely generated over K.

Proof. Suppose L/K is finite and Let $n = [L : K]$. Then L is generated by a K-basis, which is finite. Take an arbitary $\alpha \in L$. Since $1, \alpha, \cdots, \alpha^n$ is K-linearly dependent, we get a nonzero polynomial $f(x) \in K[x]$ such that $f(\alpha) = 0$.

Conversely, if L/K is algebriac and L is finitely generated over K, then $L = K(\alpha_1, \cdots, \alpha_n)$ for some $\alpha_i \in L$. L/K can be expressed by

$$K \subset K(\alpha_1) \subset \cdots \subset K(\alpha_1, \cdots, \alpha_n) = L$$

Since α_i is algebriac over K, it is also algebriac over $K(\alpha_1, \cdots, \alpha_{i-1})$. Then $K(\alpha_1, \cdots, \alpha_i) = K(\alpha_1, \cdots, \alpha_{i-1})(\alpha_i)$ is finite extension of $K(\alpha_1, \cdots, \alpha_{i-1})$, according to proposition 2.9. It follows by corollary 2.8 that L/K is finite. □

The study of field theory is greatly motivated by dealing with roots of polynomials.

We still assume L/K is a field extension in this secton.

Proposition 2.11. Let k be a field. The following statements are equivalent.
(1) Every polynomial in $k[x]$ admits a root in k.
(2) Every polynomial in $k[x]$ is a product polynomials of degree 1.
(3) Irreducible polynomials in $k[x]$ are those of degree 1.
(4) Any algebriac extension over k is trivial.

Proof. (1)⇒(2),(2)⇒(3) are obvious.

(3)⇒(4): Suppose k'/k is an algebraic extension. For every $\alpha \in k'$, its irreducible polynomial over k is of degree 1, so $\alpha \in k$.

(4)⇒(1): Let $f(x) \in k[x]$ and we may assume f is irreducible. $k[x]/(f(x))$ is an algebraic extension of k, hence $\deg f = [k[x]/(f(x)) : k] = 1$. □

Definition 2.12 (algebraic closure)**.** If a field k satisfies the equivalent conditions of proposition 3.1, then we say k is algebraically closed. The algebriac closure of a field K is a field, denoted by $\overline{K}$, such that $\overline{K}/K$ is algebraic and $\overline{K}$ is algebriaclly closed.

Theorem 2.13 (fundamental theorem of algebra)**.** $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$.

Despite its name, this theorem is in essence about topology. We shall not prove this theorem as its proof can be found in complex analysis or topology.

According to proposition 3.1(4), algebraic closures are isomorphic to each other: If k, k' are both algebraic closures of E, one can check that $k \otimes_E k'/k$ is algebraic. It remains unclear that whether arbitary field has an algebraic closure. The construction of algebraic closure is a work about set theory.

Theorem 2.14. Every field K has an algebraic closure.

Proof. Choose an uncountable set Σ of cardinality greater than that of K and identity K with a subset of Σ. Let S be the set of triples $(E, +, \cdot)$ with $E \subset \Sigma$ and $(+, \cdot)$ is a field structure such that $(E, +, \cdot)$ contains K as a subfield and is algebraic over it. Define $(E, +, \cdot) \leqslant (E', +', \cdot')$ if E is the subfield of E'. This is a partial order in S. Applying Zorn's lemma we get a maximal element $\overline{K}$ in S.

Similar argument as propostion 2.2 shows that $\overline{K}$ and K have the same cardinality, so $\overline{K} \subsetneq \Sigma$. If $\overline{K}$ admits a nontrivial field extension, then there exists $\alpha \notin \overline{K}$ but algebriac over $\overline{K}$. Hence $\overline{K}(\alpha)$ is a finite extension of $\overline{K}$ and we can find $\overline{K} \subsetneq \widetilde{K} \subset \Sigma$ such that $\widetilde{K}$ is identified with $\overline{K}(\alpha)$, which is a contradiction with the maximality of $\overline{K}$. □

Proposition 2.15. Let $K^a = \{\, x \in L \mid x \text{ is algebraic over } L \,\}$. Then K^a is a field algebraic over K. Moreover, if $\alpha \in L$ is algebraic over K^a, then $\alpha \in K^a$.

Proof. Obviously $K \subset K'$. If nonzero elements $\alpha, \beta \in K'$, then $K(\alpha, \beta) = K[\alpha, \beta]$ is a finite extension of K. Thus every element in $K(\alpha, \beta)$ is algebraic over K. In particular, $\alpha + \beta, \alpha\beta$ and α^{-1}, β^{-1} are in K'.

If $\alpha \in L$ is algebraic over K', then α admits a minimal polynomial in $K'[x]$. Suppose the coefficient of this polynomail are $c_1, \cdots, c_n$. Then $K \subset K(c_1, \cdots, c_n) \subset K(c_1, \cdots, c_n, \alpha)$ is a finite tower. □

Corollary 2.16. If L is algebraically closed, then K^a is the algebraic closure of K.

Definition 2.17. K^a defined in proposition 3.5 is called the algebraic closure of K in L. It is the largest field in L algebriac over K.

Remark 2.18. Sometimes the algebraic closure of K in L is also denoted by $\overline{K}$.

Let $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$, which is the algebraic closure of $\mathbb{Q}$. One of the fundamental goals of number theory is to understand algebraic extension $\overline{\mathbb{Q}}/\mathbb{Q}$.

For a prime numebr p, we will discuss $\overline{\mathbb{F}}_p$ in the following section.

3. TRANSCENDENTAL EXTENSION

Let L/K be a field extension.

Definition 3.1. A subset S of L is said to be algebraically independent over K if for every nonempty subset $\{ \alpha_1, \cdots, \alpha_n \} \subset S$, there is no nonzero polynomial $f \in K[x_1, \cdots, x_n]$ such that

$$f(\alpha_1, \cdots, \alpha_n) = 0$$

S is said to be algebraically dependent over K if it is not algebraically independent over K.

Definition 3.2. A subset S of L is called a transcendental basis of L/K if S is algebraically independent over K and $L/K(S)$ is algebraic.

Lemma 3.3. Suppose $S \subset L$ is algebraically independent over K. Then $\alpha \in L \backslash K(S)$ is transcendental over $K(S)$ if and only if $S \cup \{ \alpha \}$ is algebraically independent over K.

Proof. Suppose $S \cup \{ \alpha \}$ is algebraically independent over K. If α is algebraic over $K(S)$, then there exists a nonconstant $p \in K(S)[x]$ such that $p(\alpha) = 0$. In particular, $S \cup \{ \alpha \}$ is algebraic dependent over K, a contradiction.

Conversely, assume that α is algebraic over K. Again, by contradiction suppose $S \cup \{ \alpha \}$ is algebraic dependent over K. Since S is already algebraic independent over K, we can pick $\{ \alpha_1, \cdots, \alpha_n \} \subset S$ and $f \in K[x_1, \cdots, x_{n+1}]$ such that

$$f(\alpha_1, \cdots, \alpha_n, \alpha) = \sum_k f_k(\alpha_1, \cdots, \alpha_n)\alpha^k = 0$$

In particular, we can find a nonconstant $p \in K(S)[x]$ such that $p(\alpha) = 0$, a contradiction. □

Corollary 3.4. Suppose L/K is transcendental with $S \subset L$ making $L/K(S)$ algebraic. Then S contains a transcendental basis. By taking $S = L$ we see that every transcendental extension admits a transcendental basis.

Proof. The proof is standard. Let T be the family of subsets of S algebraically independent over K. T is nonempty, with inclusion relation as partial order. By Zorn's lemma we can pick a maximal element $B \in T$. Then $L/K(B)$ is algebraic, otherwise B can be extended by at least one element. □

Theorem 3.5. Any two transcendental bases of L/K have the same cardinality.

Proof. Suppose S, T are transcendental bases of L/K and take $\beta \in T$. Since $L/K(S)$ is algebraic, we can find $\{ \alpha_1, \cdots, \alpha_m \} \subset S$ and nonconstant $f \in K(S)[x]$ such that

$$f(\beta) = \sum_k f_k(\alpha_1, \cdots, \alpha_n)\beta^k = 0$$

Note that $f \notin K[x]$ because S ia algebraically independent over K. Meanwhile, we can take the smallest possible m. After renumbering we may write

$$g(\alpha_1) = (\beta, \alpha_2, \cdots, \alpha_n)\alpha_1^j = 0$$

for some nonconstant $g \in K(\beta, \alpha_2, \cdots, \alpha_n)[x]$. Hence α_1 is algebraic over $K(\beta, \alpha_2, \cdots, \alpha_n)$. On the other hand, by the choice of m we see that $\{\beta, \alpha_2, \cdots, \alpha_m\}$ is algebraically independent over K. □

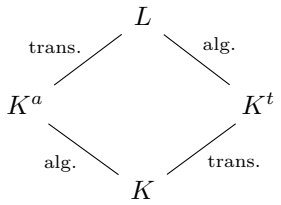
Definition 3.6. The cardinality of transcendental basis of L/K is called the transcendental degree of this field extension.

Definition 3.7. L/K is called a purely transcendental extension if $L = K(S)$ for some transcendental basis S.

Proposition 3.8. Every field extension L/K can be decomposed into extensions L/K^t and K^t/K, with L/K^t algebraic and K^t/K purely transcendental. Moreover, any such K^t are isomorphic to each other.

Definition 3.9. K^t in Proposition 4.8 is called the transcendental closure of K in L.

We have seen that L/K can be decomposed in two ways:



4. EMBEDDING THEORY

In this section, we will assume L/K is algebraic. Obivously L can be embedded into $\overline{K}$, but in how many ways?

For the sake of simplicity, we shall introduce some terminalogies first.

Definition 4.1. Suppose $K' \subset \overline{K}$ is a subfield with an isomorphism $\sigma\colon K \to K'$. Embedding $\tau\colon L \to \overline{K}$ is called the extension of σ if the following diagram commutes

$$\begin{array}{ccc} K & \longrightarrow & L \\ \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \tau} \\ K' & \longrightarrow & \overline{K} \end{array}$$

Definition 4.2. Let $\alpha, \beta \in \overline{K}$. β is called a conjugate of α over K if they are both roots of a irreducible polynomial over K.

Lemma 4.3. Suppose $L/K, L'/K'$ are field extensions and $\sigma\colon K \to K'$ is an isomorphism. Let $f(x)$ be an irreducible polynomial over K with a root $\alpha \in L$. Then there exists an extension $\tau\colon K(\alpha) \to L'$ of σ if and only if $(\sigma f)(x)$ admits a root in L'.

Proof. If $(\sigma f)(x)$ admits a root $\beta \in L'$, we can define

$$\begin{aligned} K[x] &\longrightarrow L' \\ f(x) &\longmapsto (\sigma f)(\beta) \end{aligned}$$

Then we obtain an embedding $K[x]/(f(x)) \to L'$ and we already knows $K[x]/(f(x)) \simeq K(\alpha)$. It is a routine to check the diagram commutes.

Conversely, if there is such an extension τ, $\tau(\alpha)$ happens to be the root of (σf). □

Corollary 4.4. The number of such extensions coincides with the number of roots of (σf) in L'.

Theorem 4.5. Suppose $K' \subset \overline{K}$ is a subfield with an isomorphism $\sigma\colon K \to K'$. If $L = K(\alpha)$ is simple, then the number of extensions of σ is no more than $[L : K]$, with identity holds if and only if the minimal polynomial of α has no multiple root in $\overline{K}$.

Proof. Let f be minimal polynomial of α over K. By Corollary, the number of such extensions is no more than $\mathrm{Root}(f)$. The equality holds if and only if f has no multiple root. □

Definition 4.6. A polynomial $f \in K[x]$ is said to be separable if its every irrducible component in $K[x]$ has no multiple root in $\overline{K}$.

Proposition 4.7. $f(x) \in K[x]$ admits no multiple root if and only if $\gcd(f, f') = 1$

Proof. Let $\alpha \in \overline{K}$ be a root of f and write $f(x) = (x-\alpha)^r g(x)$. Then $f'(x) = (x-\alpha)^r g'(x) + r(x-\alpha)^{r-1} g(x)$ and $(x-\alpha)^{r-1} | \gcd(f, f')$. □

Corollary 4.8. If $f(x) \in K[x]$ is irreducible, then f is separable if and only if $\mathrm{char}K = p > 0$ and $f(x) = g(x^p)$ for some $g(x) \in K[x]$.

Corollary 4.9. Every irreducible polynomial in finite fields is separable.

Proof. Let $\mathbb{F}_q$ be a finite field with $q = p^n$. Since Frobenius endomorphism is isomorphism on finite fields, for every $f(x) = g(x^p)$ we can find $h \in \mathbb{F}_q[x]$ such that $f(x) = (h(x))^p$. □

Example 4.10. If K is characteristic 0 or finite, every irreducible polynomial over K is separable.

Example 4.11. Consider $K = \mathbb{F}_p(t)$ for some prime p and indeterminate t. Then $x^p - t \in \mathbb{F}_p[t]$ is irreducible by Einsenstein criterion, and therefore irreducible over $\mathbb{F}_p(t)$ by Gauss Lemma. However, we see that $(x^p - t)' = 0$. Let α be a root of $x^p - t$ in $\overline{F_p(t)}$. Then $x^p - t = x^p - \alpha^p = (x-\alpha)^p$.

Definition 4.12. $\alpha \in L$ is said to be separable over K if its minimal polynomial over K is separable. L/K is said to be separable if its every element is separable over K.

Definition 4.13. $\alpha \in L$ is called a primitive element of L/K if $L = K(\alpha)$.

Theorem 4.14 (primitive element theorem)**.** If L/K is finite and separable, then L/K admits a primitive element. In particular, finite separable extensions are simple.

Proof. □

Corollary 4.15. L/K is separable if and only if $L = K(\alpha)$ with α separable over K.

Using algebraic closure, we easily see that splitting field of any polynomial exists.

Theorem 4.16. If $L = K(\alpha_1, \cdots, \alpha_n)$ is a finite extension of K, then every extension $\tau \colon L \to \overline{K}$ arises in the follwing way:

Denote $E_i = K(\alpha_1, \cdots, \alpha_i)$. We define isomorphisms $\sigma_i \colon E_i \to F_i$ for $i \leqslant n$ by induction. For $i = 1$, we pick a conjugate β_1 of $\sigma_1(\alpha)$ and set $F_1 = K(\beta_1)$. Suppose we have defined σ_i, then we pick a conjugate β_{i+1} of $\sigma_i(\alpha_{i+1})$ and set $F_{i+1} = F_i(\beta_{i+1})$. Finally we let $\tau = \sigma_n$.

Proof. By Lemma 4.2, we can see that $\tau = \sigma_n$ is an extension of σ. Conversely, if τ is an extension of σ, in each step we may take $\beta_i = \tau(\alpha_i)$. □

Corollary 4.17. The number of embeddings of σ is no more than $[L : K]$, with identity holds if and only if L/K is separable.

Proof. In each step the number of embeddings is no more than $[F_{i+1} : F_i]$. If L/K is separable, then $L = K(\alpha)$ for some α separable. Conversely, if L/L is inseparable, then we may take $\alpha \in L$ inseparable. $L/K(\alpha)$ is still finite, so the number of embeddings is less than $[L : K(\alpha)][K(\alpha) : K] = [L : K]$. This is a contradiction. □

Corollary 4.18. Suppose L/K is finite with a middle field E. Then L/K is separable if and only if $L/E, E/K$ are both separable.

Definition 4.19. Suppose $\mathrm{char}K = p > 0$. An element $\alpha \in L$ is said to be purely inseparable over K if $\alpha^q \in K$ for some $q = p^n$. L/K is said to be purely inseparable if every element of L is purely inseparable over K.

By definition purely inseparable extensions are always algebraic. In addition, decomposition of purely inseparable closures are also purely inseparable.

Definition 4.20. The separable closure of L/K is defined as

$$K^{sep} = \{\, \alpha \in L \mid \alpha \text{ is separable over } K \,\}$$

If $\mathrm{char} K > 0$, the purely inseparable closure of L/K is defined as

$$K^{ins} = \{\, \alpha \in L \mid \alpha \text{ is purely inseparable over } K \,\}$$

Lemma 4.21. K^{sep}, K^{ins} are subfields of L.

Proof. Let $\alpha, \beta \in K^{sep}$. By definition, β is separable over K, and therefore separable over $K(\alpha)$. Since $K(\alpha)/K$ is separable, $K(\alpha, \beta)/K$ is separable.

Let $\alpha, \beta \in K^{ins}$. Then $(\alpha + \beta)^q = \alpha^q + \beta^q$ for $q = p^n$, so we can take n sufficiently large. □

Proposition 4.22. If $\mathrm{char}\, K = p > 0$, then L/K^{ins} is separable.

Proof. If $\alpha \in L$ is inseparable over K^{ins}, its minimal polynomial over K^{ins} can be written as $f(x) = g(x^p)$ for some $g \in K^{ins}[x]$. Then $K^{ins}(\alpha^p)$ □

Theorem 4.23. Suppose L/K is algebraic, then L/K^{sep} is purely inseparable and K^{sep}/K is separable.

Proof. Suppose $\alpha \in L$. Since L/K^{sep} is algebraic, α has a minimal polynomial f over K^{sep}. By definition α is inseparable over K^{sep}, so $f = g(x^q)$ for some $q = p^n$ separable polynomial $g \in K^{sep}[x]$. □

5. finite fields

6. Galois theory