Lecture Notes On Abstract Algebra (Week 12)

Guohua PENG (彭国华)
email: peng@scu.edu.cn

Contents

1 Lecture 22 (Nov 21, 2023): Separable Extensions

Let $\tau : F \to F'$ be an embedding from a field F to F', $f(x) \in F[x]$ be of degree $n \geq 1$, $\tau^*(f(x))$ the corresponding polynomial in $F'[x]$ (under the embedding which extends τ and maps $x \to x$), and let α be a root of $f(x)$, $\overline{E'}$ be an algebraic closure E'. Then τ can be extended to an embedding from $F(\alpha)$ into $\overline{E'}$. Moreover, the number of such extensions is $\leq n$ and it is precisely n if $\tau^*(f(x))$ has distinct roots in $\overline{E'}$. It then follows that $|\mathrm{Gal}(E/F)| \leq [E : F]$ for a finite extension $[E : F]$.

When does $|\mathrm{Gal}(E/F)| = [E : F]$ hold? We will see that this happens if and only if E is a splitting field of some separable polynomial over F.

Definition 1.1. *A polynomial $f(x) \in F[x]$ is called* **separable** (可分的) *over F if every irreducible divisor of $f(x)$ has no multiple roots. Otherwise, $f(x)$ is is called* **inseparable** (不可分) *over F.*

Remark 1.1. A separable polynomial may have multiple roots. For example, $(x - 2023)^2$ is separable over $\mathbb{Q}$, but $x = 2023$ is a double root.

Example 1.1.
1. Every polynomial over $\mathbb{Q}$ is separable.
2. Let p be a prime integer, then $x^p - t$ is inseparable over the rational function field $\mathbb{F}_p(t)$. Here $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is a finite field with p elements.

Let p be a prime integer and $\mathrm{char}(F) = p$. Then
- the prime field $\mathbb{F}_p$ is a subfield of F;
- $(a + b)^p = a^p + b^p$ holds for all $a, b \in F$ (Freshman's Dream);
- $\sigma_p(\alpha) = \alpha^p$ is an $\mathbb{F}_p$-endomorphism.

Let $f(x) \in F[x]$ with $\deg f(x) \geq 1$. Recall that

$$\boxed{f(x) \text{ has no multiple roots if and only if } (f(x), f'(x)) = 1,}$$

where $f'(x)$ denotes the formal derivative of $f(x)$. If $f(x)$ is irreducible we have either $\gcd(f, f') = 1$ or $f \mid f'$, and $f \mid f'$ implies $f' = 0$.

Proposition 1.1. *A irreducible polynomial $f(x) \in F[x]$ is inseparable over F if and only if $f'(x)$ is the zero polynomial.*

If $\mathrm{char}(F) = 0$, $f'(x) = 0$ never happens, since $\deg f' = \deg f - 1$. Hence inseparable polynomials exist only when $\mathrm{char}(F) = p$ is a prime. In other words, every polynomial over a field of characteristic 0 is always separable.

If $\mathrm{char}(F) = p$ is a prime and $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in F[x]$ is an inseparable irreducible polynomial, then $f \mid f'$, which forces $f'(x) = 0$. Notice that

$$f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + 2a_2 x + a_1.$$

Hence the polynomial $f'(x) = 0$ if and only if $a_i = 0$ holds for all i that is relatively prime to p, $1 \leq i \leq n$. If follows that $f(x) = g(x^p)$ for some $g(x) \in F[x]$. In particular, $p \mid \deg f(x)$. If $g(x)$ is inseparable, there will be a polynomial $g_1(x)$ such that $g(x) = g_1(x^p)$ and then $f(x) = g_1(x^{p^2})$. Continuing this process, we can find a separable polynomial $h(x) \in F[x]$ such that $f(x) = h(x^{p^m})$ for some positive integer m.

If $f(x)$ is an inseparable irreducible polynomial over F, then $\mathrm{char}(F) = p \neq 0$ and there exist a positive integer m and a separable polynomial $g(x)$ such that $f(x) = g(x^{p^m})$.

Example 1.2. Let $F = \mathbb{F}_p(t)$, the field of rational functions over finite field $\mathbb{F}_p$ with p elements (p is a prime). Then $f(x) = x^p - t \in F[x]$ is irreducible. But $f(x)$ is not separable, since $f(x)$ has only one roots in its splitting field. One can see that $f'(x) = 0$ and $f(x) = g(x^p)$, where $g(x) = x - t \in F[x]$.

Let F be a finite field with characteristic p. Then $F^\times = F \setminus \{0\}$ is a (cyclic) group of order $p^n - 1$, where $n = [F : \mathbb{F}_p]$ (see the following lecture on finite fields). Hence every element in F can be written as α^p for some $\alpha \in F$. And a polynomial $g(x^p) \in F[x]$ can be expressed as $h(x)^p$ for some $h(x) \in F[x]$. It follows that a polynomial of the form $g(x^p)$ can not be irreducible.

$$\boxed{\text{If } \mathrm{char}(F) = 0 \text{ or } F \text{ is a finite field, then every polynomial over } F \text{ is separable.}}$$

Definition 1.2. *A field F is said to be* **perfect** (完全域) *if every irreducible polynomial over F is separable. Otherwise, F is called* imperfect.

Theorem 1.1. *Finite fields and fields of characteristic 0 are perfect fields.*

Definition 1.3. *Let K/F be an algebraic extension.*

1. *We say that $\alpha \in K$ is* **separable** (可分元) *over F if its minimal polynomial $f_\alpha(x) \in F[x]$ is separable. Otherwise, it is called* **inseparable element** (不可分元).
2. *If all elements of K are separable over F, then K/F is called a* **separable extension** (可分扩张). *Otherwise, K/F is called an* **inseparable extension**.
3. *If every element $\alpha \in K \setminus F$ is inseparable over F, then K/F is called* **purely inseparable** (纯不可分). *In this case, any element $\alpha \in K \setminus F$ is called a* **purely inseparable element** (纯不可分元).

It follows from Theorem 1.1 that

$\boxed{\text{every algebraic extension of a finite field or a field of characteristic 0 is separable.}}$

Corollary 1.1. *If K/F is separable and M is an intermediate field, then K/M and M/F are also separable.*

This follows directly from the definition of separable extension.

Example 1.3. Take $F = \mathbb{F}_p(t^p)$ and $K = \mathbb{F}_p(t)$.

$$\begin{array}{c} \mathbb{F}_p(t) \\ | \\ \mathbb{F}_p(t^p) \end{array}$$

The field extension K/F is inseparable, since the minimal polynomial of t over F is $x^p - t^p \in F[x]$. The polynomial $x^p - t^p$ splits completely as $x^p - t^p = (x-t)^p$ in $K[x]$ and so $x^p - t^p$ is inseparable. Actually $\mathbb{F}_p(t)/\mathbb{F}_p(t^p)$ is purely inseparable.

Remark 1.2. A purely inseparable element is inseparable, but the converse in not true.

- "Inseparable" only occurs in the case of characteristic p, a prime number.
- If $f(x) \in F[x]$ is irreducible and inseparable, then there exist some positive integer n and separable polynomial $g(x)$ such that

  $$f(x) = g(x^{p^n}),$$

  where $p = \mathrm{char}(F)$.
- If α is inseparable over F, then there exists a positive integer n such that α^{p^n} is separable over F.
- The minimal polynomial of a purely inseparable element over F must be of the form $x^{p^n} - a$.

An element may be neither separable nor purely inseparable Let $\mathrm{char}(F) = p \neq 0$ and let $a \in F$ be nonzero. Let t be transcendental over F and set

$$s = \frac{t^{p^2}}{t^p + a}.$$

Then t is neither separable nor purely inseparable over $F(s)$.

Actually,

$$m(x) = x^{p^2} - sx^p - sa$$

is irreducible over $F(s)$. Hence $m(x)$ is the minimal polynomial of t over $F(s)$ and then t is not separable over $F(s)$. On the other hand, if t were purely inseparable over $F(s)$, we would have

$$x^{p^2} - sx^p - sa = (x-t)^{p^2}$$

which would imply that $s = 0$, which is not the case.

The following are equivalent (TFAE):

1. A field F is perfect.
2. Every irreducible polynomial over F has distinct roots.
3. Every finite extension of F is separable.
4. Every algebraic extension of F is separable.
5. Either F has characteristic 0, or every element of F is a p-th power if $\operatorname{char}(F) = p > 0$.

We show a property of finite separable extension.

Theorem 1.2 (Primitive Element Theorem)**.** *If K/F is a finite separable extension, then there exists $\gamma \in K$ such that $K = F(\gamma)$.*

Every finite separable extension is a simple extention.

Proof. If F is a finite field, then K is finite and $K = F(\gamma)$, where γ is a generator of the cyclic group $K^{\times}$. Hence we assume F is infinite. Since K/F is a finite extension, we have $K = F(\theta_1, \theta_2, \ldots, \theta_r)$ for some elements $\theta_1, \theta_2, \ldots, \theta_r \in K$. The result follows if the case $r = 2$ is true.

We assume $K = F(\alpha, \beta)$, where α and β are algebraic over F and K/F is separable. Let $f(x)$ and $g(x)$ be the minimum polynomials of α and β over F respectively and let L be a splitting field of the polynomial $f(x)g(x)$. Then $f(x)$ and $g(x)$ both split over L. The separability of K/F ensures that $f(x)$ and $g(x)$ have no multiple roots. Let $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_m$ be all roots of $f(x)$ in L and let $\beta_1 = \beta, \beta_2, \ldots, \beta_n$ be all roots of $g(x)$ in L. Then

$$f(x) = (x - \alpha) \prod_{i=2}^{m} (x - \alpha_i), \ g(x) = (x - \beta) \prod_{j=2}^{n} (x - \beta_j).$$

$$\begin{array}{ccc} F(\alpha, \beta) & & \\ | & & \\ F(\gamma) & & h(x), \ x - \beta = (g(x), h(x)) \\ | & & \\ F & & f(x), \ g(x) \end{array}$$

Let $c \in F^{\times}$ and set $\gamma = \alpha + c\beta, h(x) = f(\gamma - cx)$. Then $h(x) \in F(\gamma)[x]$ is of degree m and the roots of $h(x)$ are

$$\gamma_i = \frac{\gamma - \alpha_i}{c} = \beta + \frac{1}{c}(\alpha - \alpha_i), \ i = 1, 2, \ldots, m.$$

Actually, $\gamma_1 = \beta$,

$$h(x) = (-c)^m (x - \beta) \prod_{i=2}^{m} (x - \gamma_i).$$

Since F is infinite, we can choose $c \in F$ so that $c \neq \frac{\alpha - \alpha_i}{\beta_j - \beta}$ for all i and $j \geq 2$. This forces $\gamma_i \neq \beta_j$ for $i \geq 2, j \geq 1$. Therefore β is the only common root of $g(x)$ and $h(x)$. It follows that $x - \beta$ is the greatest common divisor of $g(x)$ and $h(x)$ over $F(\gamma)$. That is, $x - \beta = \gcd(g(x), h(x)) \in F(\gamma)[x]$, thus $\beta \in F(\gamma)$. Consequently $\alpha \in F(\gamma)$, since $\alpha = \gamma - c\beta$ and $c \in F$. Therefore $K = F(\alpha, \beta) = F(\gamma)$. $\square$

The proof of the above theorem implies the following result.

Corollary 1.2. *Let α, β be separable over F and let $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_m$ be all conjugates of α, $\beta_1 = \beta, \beta_2, \ldots, \beta_n$ be all conjugates of β. If $c \in F$ and $c \neq \frac{\alpha - \alpha_i}{\beta_j - \beta}$ for all $i \geq 1$ and $j \geq 2$, then*

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

Remark 1.3. A inseparable extension may not be simple. Let K be the rational field $\mathbb{F}_p(x, y)$ over the finite field $\mathbb{F}_p$ in two variables. We set $F = K^p = \{f(x, y)^p \mid f(x, y) \in K\}$. Then $F = \mathbb{F}_p(x^p, y^p)$ and K/F is inseparable of degree p^2. But K/F is not a simple extension.

Since an F-embedding on $F(\alpha)$ is only decided by the image of α, we immediately obtain

Lemma 1.1. *Let α be an algebraic element over F of degree n. Then α is separable over F if and only if there are exactly n F-embeddings on $F(\alpha)$.*

Theorem 1.3. *Let K/F be a finite extension extension of degree n. Then K/F is separable if and only if there are exactly n F-embeddings on K.*

Proof. For any $\alpha \in K$, there are at most $[F(\alpha) : F]$ F-embeddings on $F(\alpha)$ and there are at most $[K : F(\alpha)]$ extensions to K for each F-embedding from $F(\alpha)$ to $\overline{F}$.

$$\begin{array}{c} K \\ | \\ F(\alpha) \\ | \\ F \end{array}$$

Notice that every F-embeddings on K comes from an F-embeddings on $F(\alpha)$ and $[K : F(\alpha)][F(\alpha) : F] = n$. Then, if there are exactly n F-embeddings on K, then there are exact $[F(\alpha) : F]$ F-embeddings on $F(\alpha)$. Hence α is separable over F by Lemma 1.1 and then K/F is separable.

Conversely, if K/F is separable, then $K = F(\alpha)$ for some separable element α of degree n, by Theorem 1.2. Hence there are exactly n F-embeddings on $K = F(\alpha)$ by Lemma 1.1. □

Combining Lemma 1.1 and Theorem 1.3, we get

Corollary 1.3. *Let α be algebraic over F. Then the extension $F(\alpha)/F$ is separable if and only if α is separable over F.*

Corollary 1.4.

1. *If K/F is a finite extension and there exists an intermediate extension M such that K/M and M/F are separable, then K/F is separable.*
2. *If K_1/F and K_2/F are separable, then the compositum K_1K_2/F is also separable.*

For the first part, notice that every F-embeddings on K is extended from and F-embeddings on M. Then the result follows by applying Theorem 1.3.

The second statement follows easily if K_1, K_2 are finite extensions over F, since K_1K_2/K_1 is separable (why?). To prove the general case, we notice that for every $\gamma \in K_1K_2$, we have $\alpha_1, \alpha_2, \ldots, \alpha_m \in K_1$ and $\beta_1, \beta_2, \ldots, \beta_n \in K_2$ such that $\gamma \in F(\alpha_1, \alpha_2, \ldots, \alpha_m, \beta_1, \beta_2, \ldots, \beta_n)$. We only need to show that $F(\alpha_1, \alpha_2, \ldots, \alpha_m, \beta_1, \beta_2, \ldots, \beta_n)$ is separable over F. Based on the first part, it suffices to prove that $F(\alpha, \beta)/F$ is separable for $\alpha \in K_1, \beta \in K_2$. This is clear since β is separable over $F(\alpha)$.

$$
\begin{tikzcd}[column sep=small]
 & K_1K_2 \arrow[dl, dash] \arrow[dr, dash] & \\
K_1 \arrow[dr, dash] & & K_2 \arrow[dl, dash] \\
 & F &
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
F(\alpha,\beta) \arrow[d, dash] \\
F(\alpha) \arrow[d, dash] \\
F
\end{tikzcd}
$$

Theorem 1.4. *Let K/F be an algebraic extension and let M be the set of all separable elements in K over F. Then M is a subfield. Moreover, M/F is separable and K/M is purely inseparable.*

Proof. The second part of Corollary 1.4 shows that M is a field and M/F is separable. Now let $\alpha \in K \setminus M$ with minimal polynomial $f(x) \in M[x]$. Then α is inseparable over M. Otherwise, by Corollary 1.3, $M(\alpha)/M$ is separable. Together with separable extension M/F, $M(\alpha)/F$ is separable and hence α is separable over F, contradictory to the assumption $\alpha \notin M$. So K/M is purely inseparable. $\square$

By Corollary 1.4, $\alpha \pm \beta, \alpha\beta, \frac{\alpha}{\beta}$ are separable if α, β are separable elements. The subfield M in Corollary 1.4 is called the **separable closure** (可分闭包) of K/F. The separable closure is exactly the compositum of all intermediate separable extension over F. And Corollary 1.4 shows that every finite extension K/F can be decomposed into two parts: the lower part M/F is separable and the upper part K/M is purely inseparable.

$$
\begin{tikzcd}
K \arrow[d, dash, "\text{purely inseparable extension}"] \\
M \arrow[r, phantom, "\substack{\text{separable closure of } F \text{ in } K,\\ \text{—maximal intermediate field}\\ \text{such that } M/F \text{ is separable}}"] \arrow[d, dash, "\text{separable extension}"] & {} \\
F
\end{tikzcd}
$$

The **separable degree** (可分次数) of the extension K/F is defined by

$$[K : F]_s = [M : F]$$

and the *inseparable degree* (不可分次数) is defined by $[K : F]_i = [K : M] = \frac{[K:F]}{[K:F]_s}$.

The separable degree is transitive by Corollary 1.4. That is, if K/F is a finite extension and $F \subseteq L \subseteq K$, then

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

Exercises

1. Let p be a prime and F a field with characteristic p. Show that $\sigma_p(\alpha) = \alpha^p$ is an $\mathbb{F}_p$-endomorphism.

2. Let $f(x) \in F[x]$ be an inseparable irreducible polynomial over F and $\mathrm{char}(F) = p$. Show that there exist a positive integer n and a separable irreducible polynomial $g(x)$ over F such that $f(x) = g(x^{p^n})$.

3. Show that every algebraically closed field is perfect.

4. Let α be an inseparable algebraic element over F. Show that there exists a positive integer n such that α^{p^n} is separable over F.

5. Let α be purely inseparable over F. Show that the minimal polynomial of α over F must be of the form $x^{p^n} - a$.

6. Show that $F(\alpha)$ is purely inseparable if and only if $\alpha^{p^n} \in F$ for some positive integer n, where $p = \mathrm{char}(F)$.

7. Let $F \subseteq L \subseteq K$ be field extensions such that L/F is purely inseparable and K/L is normal. Show that K/F is normal.

8. Let α be separable over F. Then the extension $F(\alpha)/F$ is separable.

9. Let K/F be separable and L/F be an arbitrary extension. Show that KL/L is separable.

10. Let K/F be a finite extension and $\mathrm{char}(F) = p \neq 0$. Show that the inseparable degree $[K : F]_i$ is a power of p.

11. Let K/F be a field extension. Suppose that $\alpha \in K$ is separable over F and $\beta \in K$ is algebraic over F. Show that $F(\alpha, \beta)/F$ is a simple extension. Moreover, if F is infinite, the extension $F(\alpha, \beta)/F$ has infinitely many primitive elements of the form $a\alpha + b\beta$, where $a, b \in F$.

12. Let $K = F(\theta_1, \theta_2, \dots, \theta_r)$ be a finite separable extension over an infinite field F. Show that $K = F(\gamma)$, where $\gamma = c_1\theta_1 + c_2\theta_2 + \cdots + c_r\theta_r$ for some elements $c_1, c_2, \dots, c_r \in F$.

13. Assume there are finitely many intermediate subfields between F and its extension field K. Show that K/F is a finite simple extension.

14. Let $p_1, p_2, \dots, p_n$ be distinct prime integers and $K = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_n})$. Show that $K/\mathbb{Q}$ is a normal and separable extension.

2 Lecture 23 (Nov 23, 2023): Normals Extensions

2.1 Normal Extensions

An extension of an automorphism may not necessarily be an automorphism, since the extension field may not include all conjugates of its elements. For example, let $\alpha = \sqrt[4]{2}, \beta = \alpha^2 = \sqrt{2}$, the map $\tau(\sum a_k\beta^k) = \sum a_k(-\beta)^k$ gives an automorphism of $F = \mathbb{Q}(\beta)$. The map

$$\sigma : K_1 = \mathbb{Q}(\alpha) \to K_2 = \mathbb{Q}(i\alpha) \hookrightarrow \overline{\mathbb{Q}}$$
$$\sum a_k\alpha^k \mapsto \sum a_k(i\alpha)^k$$

is an extension of τ. But σ is not an automorphism on K_1. The key point is that $K_1 = \mathbb{Q}(\alpha)$ does not contain all conjugates of α over $\mathbb{Q}$.

Recall two roots of an irreducible polynomial over F are called F-conjugate.

Definition 2.1. *An algebraic extension K/F is* **normal** (正规的)*, if K contains all F-conjugates of every element in K.*

In other words, let $\alpha \in K$ and let $m_\alpha(x)$ be the minimal polynomial of α over F. Then K/F is normal if and only if K contains all roots of $m_\alpha(x)$ for all α.

Example 2.1. The extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal since $x^3 - 2$ has a root in $\mathbb{Q}(\sqrt[3]{2})$. But $\sqrt[3]{2}\omega$, another root of $x^3 - 2$ doesn't belong to $\mathbb{Q}(\sqrt[3]{2})$, where $\omega = \frac{-1+\sqrt{-3}}{2}$.

Theorem 2.1. *Let K/F be an algebraic extension. The following four are equivalent.*

1. **The extension K/F is normal.**

2. *If $f(x) \in F[x]$ is irreducible and has a root in K, then all roots of $f(x)$ are in K.*

3. *Every irreducible polynomial in $F[x]$ that has a root in K splits completely over K.*

4. **Every F-embedding on K is essentially an F-automorphism.** *That is, $\sigma(K) = K$ for every F-embedding $\sigma : K \hookrightarrow \overline{F}$.*

Proof. We only need to prove the equivalence of 1 and 4.

Assume K/F is normal and σ is an F-embedding on K. For $\alpha \in K$, let $f(x) \in F[x]$ be its minimal polynomial over F. Noticing that $\sigma|F = \mathrm{id}_F$, $\sigma(\alpha)$ is a root of $\sigma^*(f) = f(x)$. That is, $\sigma(\alpha)$ is a conjugate of α. Hence $\sigma(\alpha) \in K$. This means $\sigma(K) \subseteq K$ and σ is an F-endomorphism of K. Since K/F is algebraic, then $\sigma(K) = K$ (see the following remark).

Conversely, let $\alpha \in K$ and $f(x) \in F[x]$ be its minimal polynomial. Let $\beta \in \overline{F}$ be a conjugate of α. The identity map on F can be extended to an embedding $\tau : F(\alpha) \hookrightarrow \overline{F}$ such that $\tau(\alpha) = \beta$. This embedding can then be extended to an embedding (still denoted by τ) from K to $\overline{F}$. Hence τ must be an F-automorphism and particularly $\tau(K) = K$. It follows $\beta = \tau(\alpha) \in K$. This means K contains every conjugate of α and so K/F is normal. □

$$\boxed{K/F \text{ is normal} \Longleftrightarrow \sigma(K) = K \text{ for every } F\text{-embedding } \sigma : K \hookrightarrow \overline{F}.}$$

Remark 2.1. 1. Let K/F be an algebraic extension. Then every F-endomorphism of K is an F-automorphism (Exercise 9 on page 242 in the textbook).

2. The above result may be false if the extension K/F is transcendental. Actually, let $F(x)$ be the rational function field in one variable and

$$\begin{aligned} \tau : F(x) &\to F(x) \\ f(x) &\mapsto f(x^2). \end{aligned}$$

Then τ is an F-endomorphism, but not an F-automorphism.

3. Since every polynomial over F splits completely in its algebraic closure, any algebraic closure of F is normal over F.

Corollary 2.1. *1. If K/F is normal and M is an intermediate subfield, then K/M is normal.*

2. Let K/F be an algebraic extension and let K_1, K_2 be two intermediate fields such that K_1/F and K_2/F are normal. Then K_1K_2/F is normal.

$$\begin{tikzcd}[arrows=dash] & K_1K_2 & \\ K_1 \arrow[ur] & & K_2 \arrow[ul] \\ & F \arrow[ul] \arrow[ur] & \end{tikzcd}$$

Proof. 1. Every M-embedding on K is also an F-embedding, hence an automorphism on K.

2. Let σ be an F-embedding on K_1K_2. Then $\sigma\mid_{K_i}$ is an F-embedding on K_i, hence an F-automorphism on K_i, $i=1,2$. Consequently $\sigma|_{K_i}(K_i)=\sigma(K_i)=K_i$. But $\sigma(K_1K_2)=\sigma(K_1)\sigma(K_2)$. Thus $\sigma(K_1K_2)=K_1K_2$ and consequently K_1K_2/F is normal.

$\square$

Corollary 2.1 says that the compositum of normal extensions is still normal. This means, if K/F is algebraic, there will a unique intermediate field E such that E/F is normal and $F\subseteq E'\subseteq K$ with E'/F normal implies $E'\subseteq E$. Such filed E is called the *normal closure of F in K*.

For a finite extension K/F, let $\sigma_1,\sigma_2,\dots,\sigma_n$ be all F-embeddings from K to $\overline{F}$. Set

$$L=\sigma_1(K)\sigma_2(K)\cdots\sigma_n(K).$$

It is the compositum of all conjugates of K. Theorem 2.1 ensures that L/F is normal and the extension field L has the following property: for any subfield $L'\subseteq\overline{F}$ such that $K\subseteq L'$ and L'/F is normal, $L\subseteq L'$. This field is called the **normal closure** (正规闭包) for the extension K/F, or the *normal closure of K over F*. Clearly the normal closure of K/F is the intersection of all normal extension E'/F such that $K\subseteq E'\subseteq\overline{F}$. It is is the smallest extension field of K such that L/F is normal. One can see

$$\text{the normal closure of } K/F=\prod_{\sigma\in\mathrm{Gal}(\overline{F}/F)}\sigma(K).$$

If $K=F(\alpha)$ for some algebraic elements, the normal closure of $F(\alpha)/F$ is just $F(\alpha_1,\alpha_2,\dots,\alpha_n)$, where $\alpha_1,\alpha_2,\dots,\alpha_n$ are all conjugates of α over F. More generally, if $K=F(\beta_1,\dots,\beta_m)$, then the normal closure of K/F is obtained by adjoining all F-conjugates of each β_i to F.

Remark 2.2. The normal closure of F in an extension field K is the maximal intermediate field M such that M/F is normal. While the normal closure of an algebraic extension K/F is the smallest intermediate field M of $\overline{K}/K$ such that M/F is normal.

Example 2.2. The normal closure of $\mathbb{Q}$ in $\mathbb{Q}(\sqrt[3]{2})$ is $\mathbb{Q}$. But the normal closure of the field $\mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[3]{2},\omega)$, where $\omega=\frac{-1+\sqrt{-3}}{2}$ is a 3rd root of unity.

Theorem 2.2. A finite extension K/F is normal if and only if K/F is a splitting field of some polynomial over F.

Proof. Suppose K/F is normal and finite. Let $\alpha_1,\alpha_2,\dots,\alpha_n$ be a basis for K over F. Then $K=F(\alpha_1,\alpha_2,\dots,\alpha_n)$, where each α_i is algebraic over F. If $m_i(x)$ is the minimal polynomial of α_i over F, then by assumption $m_i(x)$ splits over F. Hence K is a splitting field of $m(x)=m_1(x)m_2(x)\cdots m_n(x)$ over F.

Conversely, assume K is a splitting field of a polynomial $f(x)$ over F. Then $[K:F]$ is finite and $K=F(\alpha_1,\alpha_2,\dots,\alpha_n)$, where $\alpha_1,\alpha_2,\dots,\alpha_n$ are all roots of a polynomial $f(x)\in F[x]$.

Let τ be an F-embedding on K and let $m_i(x)$ be the minimal polynomial of α_i. It follows that $m_i(x)\mid f(x)$ and $\tau(\alpha_i)$ is a root of $\tau^*(m_i)=m_i(x)$, hence a root of $f(x)$. Thus, $\tau(\alpha_i)=\alpha_j\in K$ for some $1\le j\le n$. This shows that every F-embedding on K is an F-automorphism. So K/F is normal. $\square$

Main results on normal extensions

1. Let $F \subseteq M \subseteq K$ be algebraic extensions of fields. If K/F is normal, then K/M is normal.
2. If $K_1/F, K_2/F$ are normal, then K_1K_2/F is normal.
3. Let K/F be a finite extension. Then K/F is normal $\Longleftrightarrow$ K is a splitting field of some $f(x) \in F[x]$.
4. If $\alpha_1, \dots, \alpha_r$ are algebraic over F, then the normal closure of $F(\alpha_1, \dots, \alpha_r)/F$ is just the splitting field of $m_1(x) \cdots m_r(x)$, where $m_i(x)$ is the minimal polynomial of α_i over F.

Exercises

1. Let α be algebraic over F with minimal polynomial $m(x)$. Show that the normal closure of $F(\alpha)/F$ is a splitting field of $m(x)$ over F.
2. Find the normal closure of $\mathbb{Q}(\alpha)/\mathbb{Q}$ in $\mathbb{C}$, where α is a root of $x^3 - 2x + 2$.
3. Let K/F be a normal extension and M an intermediate subfield. Is the extension M/F normal?
4. Let $\alpha \in \mathbb{C}$ be a root of $x^4 - 2x^2 - 15 = 0$ and $F = \mathbb{Q}(\alpha)$. Determine a normal closure of F over $\mathbb{Q}$
5. Let p be a prime. Show that $x^p - t$ is irreducible over the field $\mathbb{F}_p(t)$ of rational functions, where t is an indeterminate. What's the splitting field of $x^p - t$?
6. Let K/F be a finite extension. Show that $|\mathrm{Gal}(K/F)| = [K : F]$ if and only if K is a splitting field of a separable polynomial over F.

2.2 Quiz 4

1. (5分) 有多少个互不同构的 72 阶交换群?
2. (10分) 设 α 为多项式 $f(x) = x^3 - 3x + 4$ 的一个实根.
   (1) 证明: $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$.
   (2) 将 $\alpha^4, (\alpha - 1)^{-1}$ 表成 $1, \alpha, \alpha^2$ 的 $\mathbb{Q}$-线性组合.
3. (5分) 设 K/F 为域的有限扩张, $\overline{F}$ 为 F 的代数闭包, $\sigma : K \to \overline{F}$ 是一个 F-嵌入. 证明: $\sigma(K)$ 为 $\overline{F}/F$ 的中间域且 $[\sigma(K) : F] = [K : F]$.

Homework Exercise 14, 17, 26, 27, 28, 29, 31, 39, 40 on page 243-245.