Lecture Notes On Abstract Algebra (Week 14)

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

Contents

1 Lecture 26 (Dec 5, 2023): Cyclotomic Fields

A cyclotomic field is obtained by adjoining a root of unity to the rational numbers. It is a splitting field of a polynomial of the form $x^n - 1$. Cyclotomic fields arise naturally in the cyclotomy problem — the division of a circle into equal parts is equivalent to the construction of a primitive root in the complex plane. The structure of cyclotomic fields is "simple", and they therefore provide convenient experimental material in formulating general concepts in number theory. For example, the concept of an algebraic integer and a divisor first arose in the study of cyclotomic fields.

Let n be a positive integer and K a field. If an element ζ in K satisfies $\zeta^n = 1$, then ζ is called an n-th root of unity. An element ζ in K is said to be a **primitive n-th root** of unity if $\zeta^n = 1$ but $\zeta^d \neq 1$ for any $d < n$, i.e., if ζ is an element of order n in $K^\times = K^*$. For example, all n-th roots of unity in $\mathbb{C}$ are complex numbers

$$e^{\frac{2\pi i m}{n}},\ 0 \leq m \leq n-1.$$

Among them, only $e^{\frac{2\pi i m}{n}}$ with $(m, n) = 1$ are primitive.

If $(n, \mathrm{char}(K)) = 1$, then all n-th roots of unity form a cyclic multiplicative group of order n in the algebraic closure $\overline{K}$. That is,

$$\{\zeta \in \overline{K} \mid \zeta^n = 1\} \cong (\mathbb{Z}/n\mathbb{Z}, +).$$

Basic facts on primitive roots of unity

(1) Let ζ be a primitive n-th root of unity. Then ζ^m is again a primitive n-th root of unity if and only if m is relatively prime to n.

(2) The conjugates of ζ are precisely those primitive n-th roots of unity.

The extension $\mathbb{Q}(\zeta_n)$ is called the **n-th cyclotomic field** (分圆域), where $\zeta_n = e^{\frac{2\pi i}{n}} \in \mathbb{C}$ is a primitive n-th root of unity. For example, $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$ are cyclotomic fields.

In general, if n is a positive integer coprome to $\mathrm{char}(F))$ and ζ is a primitive n-th root of unity, then $F(\zeta)$ is called a **cyclotomic extension** over F. Actually $F(\zeta)$ is a splitting field of $x^n - 1$ over F. In other words,

a cyclotomic extension over F is a splitting field of $x^n - 1$ over F for some positive integer n.

Cyclotomic extensions over $\mathbb{Q}$ are cyclotomic fields. Cyclotomic extensions have the same properties as cyclotomic fields.

Basic facts on cyclotomic fields

(1) If $m \mid n$, then $\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_n)$.

(2) The **cyclotomic polynomial** Φ_n is defined to be

$$\Phi_n(x) = \prod_{\substack{(m,n)=1 \\ 0 \le m \le n-1}} (x - \zeta_n^m).$$

It is the minimal polynomial of ζ_n over $\mathbb{Q}$. In particular, $\Phi_n(x) \in \mathbb{Z}[x]$ is irreducible and $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, the Euler totient function.

(3) For any m and n,

$$\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_{[m,n]})$$

and

$$\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{(m,n)}).$$

In particular, if $(m, n) = 1$, then

$$\mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_{mn}), \quad \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}.$$

(4) If $m < n$ and $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_n)$, then m is odd and $n = 2m$. In particular, if $m, n \not\equiv 2 (\mathrm{mod}\ 4)$, then $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_n)$ if and only if $m = n$.

(5) The extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois and

$$\mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right) = \{\sigma_a \mid 1 \le a \le n, (a, n) = 1\} \cong \left(\mathbb{Z}/n\mathbb{Z}\right)^\times,$$

where the automorphism σ_a is given by

$$\begin{aligned} \sigma_a : \quad & \mathbb{Q}(\zeta_n) \to \mathbb{Q}(\zeta_n), \\ & \zeta_n \mapsto \zeta_n^a. \end{aligned}$$

Remark 1.1. 1. The first few cyclotomic polynomials are

$$\begin{aligned} \Phi_1(x) &= x - 1, \\ \Phi_2(x) &= x + 1, \\ \Phi_3(x) &= x^2 + x + 1, \\ \Phi_4(x) &= x^2 + 1, \\ \Phi_5(x) &= x^4 + x^3 + x^2 + x + 1, \\ \Phi_6(x) &= x^2 - x + 1, \\ \Phi_7(x) &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, \end{aligned}$$

$$\Phi_8(x) = x^4 + 1,$$
$$\Phi_9(x) = x^6 + x^3 + 1,$$
$$\Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1,$$
$$\Phi_{11}(x) = x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,$$
$$\Phi_{12}(x) = x^4 - x^2 - 1$$

If p is a prime, then

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

2. The cyclotomic polynomials may be approached in another way. If we set

$$\Phi_d(x) = \prod_{\zeta}(x - \zeta),$$

where ζ runs over all primitive d-th root of unity, then

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

By *Mobius inversion formula* (莫比乌斯反演公式),

$$\Phi_n(x) = \prod_{d|n}(x^d - 1)^{\mu(\frac{n}{d})} \in \mathbb{Q}[x],$$

where $\mu(n)$ is the *Mobius function* given by

$$\mu(n) = \begin{cases} 1, & \text{if } n = 1; \\ (-1)^k, & \text{if } n = p_1 p_2 \cdots p_k \text{ is a product of } k \text{ distinct primes;} \\ 0, & \text{otherwise.} \end{cases}$$

Notice that all roots of $\Phi_n(x)$ are algebraic integers. We then have $\Phi_n(x) \in \mathbb{Z}[x]$. One can prove that $\Phi_n(x)$ is irreducible over $\mathbb{Z}$. Therefore $\Phi_n(x)$ is the minimal polynomial of ζ_n.

Mobius Inversion Formula (addition form) Let $f(n)$ and $g(n)$ be two functions defined over positive integers. If

$$f(n) = \sum_{d|n} g(d),$$

then

$$g(n) = \sum_{d|n} \mu(d) f(\frac{n}{d}).$$

Mobius Inversion Formula (multiplication form) Let $f(n)$ and $g(n)$ be two functions defined over positive integers. If

$$f(n) = \prod_{d|n} g(d),$$

then

$$g(n) = \prod_{d|n} f(\frac{n}{d})^{\mu(d)}.$$

We list a theorem on the structure of the multiplicative group of $\mathbb{Z}/n\mathbb{Z}$.

Theorem 1.1. *Let n be a positive integer. Then $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic if and only if $n = 2, 4, p^m, 2p^m$, where p is an odd prime.*

$$(\mathbb{Z}/n\mathbb{Z})^\times \text{ is cyclic} \iff n = 2, 4, p^m, 2p^m, \text{ where } p = \text{odd prime.}$$

Corollary 1.1. *Let n be a positive integer such that $n \not\equiv 2 (\mathrm{mod}\ 4)$. Then the extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is cyclic if and only if $n = 4$ or p^m, where p is an odd prime.*

- The cyclotomic extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois.
- The Galois group

$$\mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right) = \{\sigma_k \mid 1 \le k \le n, (k,n) = 1\} \cong (\mathbb{Z}/n\mathbb{Z})^\times,$$

  where $\sigma_k(\zeta_n) = \zeta_n^k,\ (k,n) = 1$.
- The extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is cyclic $\iff n = 2, 4, p^m, 2p^m$ for some odd primes p.

The *Kronecker-Weber Theorem*[1] states that every finite abelian extension of the rational number field is a subfield of some cyclotomic field. Consequently, for a finite abelian group G, there is a finite Galois extension K over $\mathbb{Q}$ such that $\mathrm{Gal}(K/\mathbb{Q}) = G$. Equivalently, for every finite abelian group G, there is an irreducible polynomial $f(x) \in \mathbb{Q}[x]$ whose Galois group is G.

Kronecker-Weber Theorem was first stated by Leopold Kronecker (1853) though his argument was not complete for extensions of degree a power of 2. Heinrich Martin Weber (1886) published a proof, but this had some gaps and errors that were pointed out and corrected by Olaf Neumann (1981). The first complete proof was given by David Hilbert (1896).

Exercises

1. Let p be a prime number and n an integer coprime to p. Show that the Galois group of $x^n - 1$ over $\mathbb{F}_p$ is cyclic of order r, where r is the order of p in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$.

2. Let ζ be a primitive n-th root of unity and $K = \mathbb{Q}(\zeta)$. The following exercises provide an approach to prove $[K : \mathbb{Q}] = \varphi(n)$. Let $m(x)$ be the minimal polynomial of ζ over $\mathbb{Q}$.

   (a) Show that $(m(x), x^d - 1) = 1$ for all $1 \le d < n$.

   (b) Show that every root of $m(x)$ must be primitive.

   (c) Let p be a prime and $(p, n) = 1$. Show that ζ^p is a root of $m(x)$. (Hint: taking $m(x)$ modulo p)

   (d) Show that $\deg m(x) = \varphi(n)$ and then $[K : \mathbb{Q}] = \varphi(n)$.

3. Let K be a splitting field of $x^n - 1$ over F, where n is a positive integer which is prime to $\mathrm{char}(F)$ if $\mathrm{char}(F) \neq 0$. Let $G = \{z \in K \mid z^n = 1\}$.

   (a) Show that G is a cyclic subgroup of $K^\times$.

   (b) Show that the automorphism group $\mathrm{Aut}(G)$ is isomorphism to $(\mathbb{Z}/n\mathbb{Z})^\times$.

   (c) For $\sigma \in \mathrm{Gal}(K/F)$, show that the restriction $\sigma|_G$ is an automorphism on G and deduce that the restriction induces an embedding from $\mathrm{Gal}(K/F)$ to $(\mathbb{Z}/n\mathbb{Z})^\times$.

   (d) For the case $F = \mathbb{Q}$, show that $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$.

4. Prove that the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic if and only if $n = 2, 4, p^m, 2p^m$, where p is an odd prime.

[1] Kronecker was a German mathematician who worked on number theory and algebra. He criticized Cantor's work on set theory, and was quoted by Weber (1893) as having said, "God made the integers, all else is the work of man."

2 Lecture 27 (Dec 7, 2023): Artin's Lemma

2.1 Fixed Subfields

Recall that $\mathrm{Aut}(K)$ denotes the automorphism group of a field K. If P is the prime subfield of K (i.e. the smallest subfield of K), then $\mathrm{Aut}(K) = \mathrm{Gal}(K/P)$. In other words, if $\mathrm{char}(K) = 0$, then $\mathrm{Aut}(K) = \mathrm{Gal}(K/\mathbb{Q})$; if $\mathrm{char}(K) = p \neq 0$, then $\mathrm{Aut}(K) = \mathrm{Gal}(K/\mathbb{F}_p)$.

For a field extension K/F, we associate a group $\mathrm{Gal}(K/F)$, the group of automorphism of K/F. If M is an intermediate field of K/F, then $\mathrm{Gal}(K/M)$ is a subgroup of $\mathrm{Gal}(K/F)$, since every M-automorphism on K is obviously an F-automorphism on K.

Conversely, let H be a subgroup of $\mathrm{Aut}(K)$, we can associate it with a subfield defined by

$$K^H = \{x \in K \mid h(x) = x \text{ for all } h \in H\}. \tag{1}$$

It's easy to check that K^H is a subfield of K. We call it the **fixed subfield** (固定子域, 不动域), or *invariant subfield* (不变子域) of H.

$$\begin{array}{c} K \\ | \\ K^H = F \end{array}$$

Remark 2.1.

1. For a subgroup H of $\mathrm{Aut}(K)$, denoted by $H \leq \mathrm{Aut}(K)$, H acts on K via an obvious way: $\sigma \circ x = \sigma(x)$. The fixed field K^H is just the *subset of K fixed by H*.

2. If we put $F = K^H$, then every element in H induces an F-automorphism of K. Hence

$$H \leq \mathrm{Gal}(K/K^H). \tag{2}$$

Example 2.1. Let $K = \mathbb{Q}(\alpha, i)$, where $i = \sqrt{-1}$ and α is the unique positive real root of $x^4 - 2$. Then K is the splitting field of $x^4 - 2$ over $\mathbb{Q}$.

We claim $1, \alpha, \alpha^2, \alpha^3, i, \alpha i, \alpha^2 i, \alpha^3 i$ is a $\mathbb{Q}$-basis for K. Actually, if $a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + b_0 i + b_1\alpha i + b_2\alpha^2 i + b_3\alpha^3 i = 0$ for some $a_0, a_1, a_2, a_3, b_0, b_1, b_2, b_3 \in \mathbb{Q}$, then $a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 = b_0 + b_1\alpha + b_2\alpha^2 + b_3\alpha^3 = 0$. That is, $f(\alpha) = g(\alpha) = 0$, where $f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3$ and $g(x) = b_0 + b_1 x + b_2 x^2 + b_3 x^3$. But $x^4 - 2$ is the minimal polynomial of α over $\mathbb{Q}$. So we have $f(x) = g(x) = 0$, yielding $a_k = b_k = 0$ for $k = 0, 1, 2, 3$. This can be also see from the fact that $K = \mathbb{Q}(\alpha)(i)$ and $\mathbb{Q}(\alpha) = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\alpha^2 + \mathbb{Q}\alpha^3, K = \mathbb{Q}(\alpha) + \mathbb{Q}(\alpha)i$. So

$$K = \left\{ \sum_{j=0}^{3} a_j \alpha^j + \sum_{j=0}^{3} b_j \alpha^j i \;\middle|\; a_0, a_1, a_2, a_3, b_0, b_1, b_2, b_3 \in \mathbb{Q} \right\}.$$

It was shown in last lecture that

$$\mathrm{Gal}\left((x^4 - 2)/\mathbb{Q}\right) = \mathrm{Gal}(K/\mathbb{Q}) = \langle \sigma, \tau \rangle = \{1, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\},$$

where σ and τ are given by

$$\begin{array}{lll} \sigma : K \to K, & \tau : & K \to K, \\ \alpha \mapsto \alpha i & & \alpha \mapsto \alpha \\ i \mapsto i & & i \mapsto -i. \end{array}$$

That is,

$$\begin{aligned} &\sigma\left(a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + b_0 i + b_1\alpha i + b_2\alpha^2 i + b_3\alpha^3 i\right) \\ &= a_0 + a_1\alpha i - a_2\alpha^2 - a_3\alpha^3 i + b_0 i - b_1\alpha - b_2\alpha^2 i + b_3\alpha^3 \end{aligned} \tag{3}$$

$$\begin{aligned}&\tau\left(a_0+a_1\alpha+a_2\alpha^2+a_3\alpha^3+b_0i+b_1\alpha i+b_2\alpha^2 i+b_3\alpha^3 i\right)\\&=a_0+a_1\alpha+a_2\alpha^2+a_3\alpha^3-b_0i-b_1\alpha i-b_2\alpha^2 i-b_3\alpha^3 i.\end{aligned}\tag{4}$$

Take $H_1=\langle\sigma\rangle, H_2=\langle\tau\rangle$. We have

$$\begin{aligned}&\beta=\sum_{j=0}^{3}a_j\alpha^j+\sum_{j=0}^{3}b_j\alpha^j i\in K^{H_1}\\&\iff\sigma(\beta)=\beta\\&\iff a_0=a_0, a_1=-b_1, a_2=-a_2, a_3=b_3, b_0=b_0, b_1=a_1, b_2=-b_2, b_3=-a_3,\\&\iff a_1=b_1=a_2=b_2=a_3=b_3=0, a_0, b_0\in\mathbb{Q}\\&\iff\beta=a_0+b_0i, a_0, b_0\in\mathbb{Q}\\&\iff\beta\in\mathbb{Q}(i).\end{aligned}$$

Hence

$$K^{H_1}=\mathbb{Q}(i).$$

By considering the action of τ on K, we obtain

$$K^{H_2}=\mathbb{Q}(\alpha)$$

likewise.

Example 2.2. Let p be a prime number and let $\overline{\mathbb{F}}_p$ be an algebraic closure of $\mathbb{F}_p$. We know

$$\mathrm{Aut}(\overline{\mathbb{F}}_p)=\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)=\langle\sigma\rangle,$$

where $\sigma(x)=x^p$ is the p-th Frobenius map. For a positive integer n, consider the subgroup

$$H=\langle\sigma^n\rangle.$$

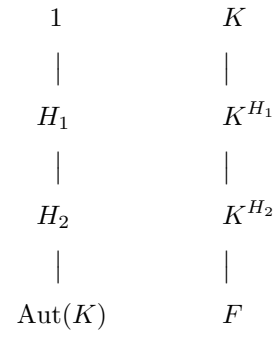
One can check that $[\mathrm{Aut}(\overline{\mathbb{F}}_p):H]=n$ and

$$\overline{\mathbb{F}}_p^H=\{x\in\overline{\mathbb{F}}_p\mid x^{p^n}=x\}=\mathbb{F}_{p^n},$$

the finite field with p^n elements.

Basic Facts on Fixed Subfields

1. Let H be a subgroup of $\mathrm{Aut}(K)$. Then H is a subgroup of $\mathrm{Gal}(K/L)$ for some subfield L if and only if $L\subseteq K^H$. In particular, H is a subgroup of $\mathrm{Gal}(K/K^H)$.
2. Let H_1, H_2 be subgroups of $\mathrm{Aut}(K)$. If $H_1\subseteq H_2$, then $K^{H_1}\supseteq K^{H_2}$.



Exercises

1. Let $K=\mathbb{Q}(\sqrt[4]{2})$ and $H=\mathrm{Gal}(K/\mathbb{Q})$. Determine K^H.
2. Let H be a subgroup of $\mathrm{Aut}(K)$ and F a subfield of K. Prove that $H\leq\mathrm{Gal}(K/F)$ if and only if $F\subseteq K^H$.

3. Let p be a prime and $q = p^f$. Let Ω be an algebraically closed field of characteristic p. Consider the map $\sigma_q : x \mapsto x^q$ on Ω.

   (1) Show that $\sigma_q \in \mathrm{Aut}(\Omega)$.

   (2) Let $H = \langle \sigma_q \rangle$. Show that $H \cong (\mathbb{Z}, +)$ and $\Omega^H \cong \mathbb{F}_q$.

2.2 Artin's Lemma

Let H be a subgroup of $\mathrm{Aut}(K)$. The elements in K that are fixed by H form a subfield of K:

$$K^H = \{x \in K \mid h(x) = x \text{ for all } h \in H\},$$

as is called the fixed subfield of H.

For a finite extension K/F, the fixed field of $H = \mathrm{Gal}(K/F)$ is an extension field of F, but not necessarily F. For example, $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}) = \{1, \theta\}$, where θ is given by

$$\theta(\sqrt[4]{2}) = -\sqrt[4]{2}.$$

But the fixed field of $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q})$ is $\mathbb{Q}(\sqrt{2})$. The following Theorem 2.3 tells when the fixed field of $\mathrm{Gal}(K/F)$ equals F.

We first need Artin's Lemma.

Lemma 2.1 (E. Artin[2]). *Let H be a finite subgroup of $\mathrm{Aut}(K)$. Then $[K : K^H] \le |H|$.*

Proof. Let $F = K^H$ be the fixed subfield of H. Suppose $|H| = n$ and $H = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ with $\sigma_1 = 1$. We only need to prove that $n + 1$ elements in K are always linearly dependent over F.

Let $\alpha_1, \alpha_2, \ldots, \alpha_{n+1} \in K$. Consider the $n \times (n+1)$ matrix over K:

$$A = (\sigma_i(\alpha_j))_{n\times(n+1)} = \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_{n+1}) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_{n+1}) \\ \vdots & \vdots & & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_{n+1}) \end{pmatrix}.$$

Let v_i be the i-th column vector of A. Clearly $r = \mathrm{rank}(A) \le n$, $v_1, v_2, \ldots, v_{n+1}$ are linearly dependent. For simplicity, we assume the first r columns form a maximal linearly independent subset of the column vectors of A. Then $v_1, v_2, \ldots, v_{r+1}$ are linearly dependent and hence there exist unique $a_1, a_2, \ldots, a_r \in K$ such that

$$v_{r+1} = a_1 v_1 + a_2 v_2 + \cdots + a_r v_r. \tag{5}$$

Considering each coordinate of the above vector relation, we have

$$\sigma_i(\alpha_{r+1}) = a_1\sigma_i(\alpha_1) + a_2\sigma_i(\alpha_2) + \cdots + a_r\sigma_i(\alpha_r),\ 1 \le i \le n. \tag{6}$$

It suffices to show that all a_i are actually in F, i.e. a_i is fixed by every element of H.

Letting each $\tau \in H$ acts on both sides of (6), we obtain

$$(\tau\sigma_i)(\alpha_{r+1}) = \tau(a_1)(\tau\sigma_i)(\alpha_1) + \tau(a_2)(\tau\sigma_i)(\alpha_2) + \cdots + \tau(a_r)(\tau\sigma_i)(\alpha_r), 1 \le i \le n. \tag{7}$$

[2]Emil Artin (1898-1962) was among the greatest algebraists of the 20th Century. The modern approach to Galois Theory was formulated by him, together with Irving Kaplanski (1917-2006). Artin and Kaplanski were both members of the Bourbaki group.

Note that $\tau H = H$ holds for $\tau \in H$. This means that $\tau\sigma_i$ ranges over all elements of H when σ_i ranges over all elements of H. Thus the equality (7) gives

$$\sigma_i(\alpha_{r+1}) = \tau(a_1)\sigma_i(\alpha_1) + \tau(a_2)\sigma_i(\alpha_2) + \cdots + \tau(a_r)\sigma_i(\alpha_r), 1 \leq i \leq n,$$

which amounts to

$$v_{r+1} = \tau(a_1)v_1 + \tau(a_2)v_2 + \cdots + \tau(a_r)v_r \tag{8}$$

holds for all $\tau \in H$. Notice that the elements $a_1, a_2, \ldots, a_r \in K$ in (5) are uniquely determined. Comparing (5) and (8), we have $\tau(a_i) = a_i$ holds for all $\tau \in H$ and all i. It follows that $a_1, a_2, \ldots, a_r \in F$. Therefore $\alpha_1, \alpha_2, \ldots, \alpha_{r+1}$ are linearly dependent over F. Consequently $\alpha_1, \alpha_2, \ldots, \alpha_{n+1}$ are linearly dependent over F. □

Actually, Artin's Lemma can be strengthened in the following form.

Theorem 2.1. *Let H be a finite subgroup of* $\mathrm{Aut}(K)$. *Then* $[K : K^H] = |H|$ *and* $\mathrm{Gal}(K/K^H) = H$.

Proof. Set $F = K^H$.

By Artin's Lemma, $[K : F] \leq |H|$, hence K/F is a finite extension. On the other hand, each element of H is essentially an F-automorphism of K, thus $H \subseteq \mathrm{Gal}(K/F)$, yielding $|H| \leq |\mathrm{Gal}(K/F)|$. Now

$$|H| \leq |\mathrm{Gal}(K/F)| \leq [K : F] \leq |H|.$$

This forces $|\mathrm{Gal}(K/F)| = |H| = [K : F]$ and $\mathrm{Gal}(K/F) = H$. □

Remark 2.2. Theorem 2.1 and Artin's Lemma are equivalent.

Recall that a finite extension K/F is separable if and only if there are exactly n F-embeddings on K.

$$\boxed{H \leq \mathrm{Gal}(K/F) \Longleftrightarrow F \subseteq K^H}$$

For a finite extension K/F, recall that

$$\boxed{\begin{aligned} K/F \text{ is Galois} &\Longleftrightarrow K \text{ is a splitting field of some separable polynomial over } F \\ &\Longleftrightarrow |\mathrm{Gal}(K/F)| = [K : F] \end{aligned}}$$

With the help of this result, we immediately have

Theorem 2.2. *For any finite subgroup H of* $\mathrm{Aut}(K)$, *the field extension K/K^H is Galois with Galois group* $\mathrm{Gal}(K/K^H) = H$.

Proof. By Theorem 2.1,

$$|\mathrm{Gal}(K/K^H)| = |H| = [K : K^H].$$

Consequently K/K^H is a Galois extension. □

$$\boxed{H \leq \mathrm{Aut}(K) \text{ and } |H| < \infty \Longrightarrow [K : K^H] = |H|,\ K/K^H \text{ is Galois and } \mathrm{Gal}(K/K^H) = H.}$$

The fixed subfield can be used to described Galois extension.

Theorem 2.3. *Let K/F be a finite extension of fields. Then the extension K/F is Galois if and only if* $F = K^{\mathrm{Gal}(K/F)}$.

Proof.

Let $H = \mathrm{Gal}(K/F)$. Then $F \subseteq K^H$ and Theorem 2.1 shows that $[K : K^H] = |H|$.

$$\begin{array}{c} K \\ | \\ K^H \\ | \\ F \end{array}$$

If $F = K^H$, then $[K : F] = |H| = |\mathrm{Gal}(K/F)|$. Therefore the extension K/F is Galois.

Conversely, if K/F is a Galois extension, then

$$\begin{aligned} |\mathrm{Gal}(K/F)| &= [K : F] \\ &= [K : K^H][K^H : F] \\ &= |H|[K^H : F]. \end{aligned}$$

It follows $[K^H : F] = 1$, hence $F = K^H$.

□

Corollary 2.1. *Let K/F be a finite Galois extension with Galois group G. Then the fixed subfield of G is F. In other words, let $\alpha \in K$, then $\alpha \in F$ if and only if $\sigma(\alpha) = \alpha$ for all $\sigma \in G$.*

Exercises

1. Let q be a prime power and let $\overline{\mathbb{F}}_q$ be an algebraic closure of the finite filed $\mathbb{F}_q$ of q elements. We know that the q-th Frobenius map σ given by $\sigma(x) = x^q$ is an automorphism of $\overline{\mathbb{F}}_q$. For a positive integer n, let $H = \langle \sigma^n \rangle$. Show that $\overline{\mathbb{F}}_q^H = \mathbb{F}_{q^n}$.

2. Let K/F be a Galois extension with Galois group G and $H \lhd G$. Suppose L, T are intermediate subfields such that $F \subseteq L \subseteq T \subseteq K$ and $T = K^H$. Is T/L Galois?

3. Let K/F be Galois with Galois group G. If H and H' are subgroups of G, then $K^{H \cap H'} = K^H K^{H'}$.

4. Let $H \leq \mathrm{Aut}(K)$ and $\sigma \in \mathrm{Gal}(K)$. Show that $K^{\sigma H \sigma^{-1}} = \sigma(K^H)$.

5. Let K/F a finite Galois extension with Galois group G. Assume $G_1, G_2, \ldots, G_n$ are subgroup of G such that $G = G_1 \otimes G_2 \otimes \cdots \otimes G_n$. Show that

$$K = K^{G_1} K^{G_2} \cdots K^{G_n}.$$

6. Let M be an intermediate field of the Galois extension K/F and $H = \{g \in \mathrm{Gal}(K/F) \mid g|_M = \mathrm{id}_M\}$. Show that M is exactly the fixed subfield of H.

7. Let H be a finite subgroup of $\mathrm{Aut}(K)$ and $\alpha \in K$. Suppose that

$$H\alpha = \{h(\alpha) \mid h \in H\} = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}.$$

   Show that $m(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$ is the minimal polynomial of α over K^H.

8. Let $K = \mathbb{C}(x)$ be the field of rational function field in x over $\mathbb{C}$. Define $\sigma, \tau \in \mathrm{Gal}(K/\mathbb{C})$ by

$$\sigma(x) = -x, \tau(x) = ix^{-1}$$

   and $G = \langle \sigma, \tau \rangle$. Show that $|G| = 4$, and the fixed field $F = K^G = \mathbb{C}(y)$, where $y = x^2 - x^{-2}$.

Remark *Lüroth Theorem* asserts that every intermediate field of the extension $\mathbb{C}(x)/\mathbb{C}$ is of the form $\mathbb{C}(u)$ with $u \in \mathbb{C}(x)$.

Homework Exercise 32, 33 on page 244-245. Exercise 11, 12, 17(3), 20, 21, 35(2) on page 315-318. Exercise 10, 11 on page 98 (optional).