Final Report on Kummer Theory

Junhao Yin, Junkai Qi, Shengan Xu

December 2023

Abstract

In this article, we focus on the Kummer Theory and its application to the Galois Theory. Explicitly, We will answer how to make the Galois Group $G = Gal(K/F)$ of a finite Galois expansion K/F include as many crossed homomorphism groups Z as possible.

Keywords: Kummer expansion, Galois expansion, Crossed homomorphism.

§ 0 Introduction

Throughout this semester's course, Professor Qin has repeatedly emphasized that "the greatest utility of a group lies in its action." This statement is not only pertinent to pure algebra but also carries unique significance in the real world we inhabit.

Indeed, when we observe the real world from a more general perspective, many events can be understood as the group action of a specific group of transformations, such as the passage of time or spatial translations. This naturally introduces the concept of symmetry. Recalling our elementary school days, when we identified geometric shapes like squares and isosceles trapezoids as symmetrical, we often referred to their unchanging shape upon reflection over a line of symmetry. Thus, symmetry essentially describes whether or not something changes under a particular transformation. And since groups are closely related to transformations, mathematicians naturally chose the language of groups to quantitatively describe the abstract concept of symmetry. [1]Seeking the invariant amid constant change has thus become a favored problem for mathematicians and physicists alike, exemplified by the Erlangen program in geometry and Noether's theorem in theoretical mechanics.

Galois theory, as the origin of group theory, is fundamentally based on the symmetry of the roots of equations. In tracing the origins of Galois' brilliant ideas, we see that the early study of the symmetry of equation roots by mathematicians like Lagrange and Vandermonde utilized the important tool of the m-th roots of unity.

These roots inherently possess symmetry (rotations on the unit circle) and often yield surprisingly fruitful outcomes. In abstract algebra, we learn that the structure of extensions over finite fields is clearer and simpler. Delving into the proofs of theorems in this area reveals a significant fact: finite fields inherently contain a group of m-th roots of unity. [2]Extending this scenario to the study of field extensions that include all m-th roots of unity is a natural progression, leading us to Kummer theory, which we will discuss in detail later in this paper.

§ 1 The Character groups of finite Abelian groups

§ 1.1 Definition 1

Suppose A is an finite Abelian group, note the least common multiple of the order of its elements as m, then we note $m = exp(A)$. Suppose the base field K contains m distinct m-th root of unity(which implies when $\chi(F)$ is a prime number, then $\chi(F)$ and m are co-prime). If K/F is a finite Abelian expansion on F and $G = Gal(K/F)$ is its Galois Group, having $\exp(G)|m$, then we call K/F a Kummer m expansion.

A Kummer m expansion K/F would provide us with sufficient homomorphisms from G to multiplicative group F^*, which we shall soon discover.

We would temporarily leave aside the content of Galois expansion and discuss the characters of finite Abelian groups. Suppose G is any Abelian Group with $\exp(G) = m'$, and Field F contains m different roots of unity. We follow the converntion of Group Theory, any homomorphism from G to F^* is called a character form G to F^*, noted χ. If $\chi(\sigma) = 1(\ \forall\sigma \in G)$, then χ is called the trivial character, or principle character, noted $\chi = 1$. Suppose χ_1,χ_2 are two characters from G to F^*. Their multiplication is defined as

$$(\chi_1\chi_2)(\sigma) = \chi_1(\sigma)\chi_2(\sigma), \quad \sigma \in G,$$

thus the inverse of χ_1 is defined as

$$\chi_1^{-1}(\sigma) = \chi_1(\sigma)^{-1}, \quad \sigma \in G.$$

Following from the definition above, it is easy to check that $\chi_1\chi_2$ and χ_1^{-1} are still characters. Therefore, $\hat{G} := \{\chi : \chi$ is a character from G to $F^*\}$ is a group, called the characteristic group of G. The trivial

character is the unit of $\hat{G}$. In order to obtain as many characters as possible, we always assume the $m'|m$, where $m' = \exp(G)$.

§ 1.2 Lemma 1

Suppose Field F contains m different roots of unity, G is a finite Abelian group, $m' = \exp(G)$, $m'|m$. Then $\hat{G}$ satisfies the following properties:

1) $\hat{G} \cong G$;

2) $\bigcap_{\chi \in \hat{G}} = \{1\}$("1" represents the unit of $\hat{G}$)

Proof. 1) Since a finite Abelian group can be written as the direct product of its cyclic subgroups, noted

$$G = G_1 \times G_2 \times ... \times G_r,$$

and $G_i = \langle \sigma_i \rangle$, $\mathrm{ord}(\sigma_i) = m_i, i = 1, ..., r$. Every element σ of G has a unique representation

$$\sigma = \sigma_1^{\nu_1} \sigma_2^{\nu_2} ... \sigma_r^{\nu_r}, \quad 0 \leqslant \nu_i \leq m_i. \tag{1}$$

$m_i|m'$ implies $m_i|m$. According to the assumption of F, F contains primitive m_i-th roots of unity, choose one for each i, noted ζ_i. Define the character

$$\chi_i : G \to F^*, \chi_i(\sigma) = \zeta_i^{\nu_i}, \quad i = 1, ..., r.$$

Apparently χ_i is a character. Observe that $\mathrm{ord}(\chi_i) = m_i$. In fact,

$$\chi_i^{m_i} = \zeta_i^{\nu_i m_i} = 1, \quad \forall \sigma \in G,$$

Thus $\chi_i^{m_i} = 1$. If $\chi_i^k = 1$, then $\chi_i^k(\sigma_i) = (\zeta_i)^k = 1$, thus $m_i|k$, which proves that $\mathrm{ord}(\chi_i) = m_i$. Next, we shall prove that $\chi_1, \chi_2, ..., \chi_r$ are independent. Suppose $\chi_1^{k_1} \chi_2^{k_2} ... \chi_r^{k_r} = 1$. Applying the indentity on σ_i:

$$\chi_1^{k_1} \chi_2^{k_2} ... \chi_r^{k_r}(\sigma_i) = 1.$$

The left hand side equals to

$$\chi_1^{k_1}(\sigma_i) \chi_2^{k_2}(\sigma_i) ... \chi_r^{k_r}(\sigma_i) = \chi_i^{k_i}(\sigma_i) = \zeta_i^{k_i},$$

Thus $\zeta_i^{k_i} = 1, m_i | k_i$. So every terms of $\chi_i^{k_i} = 1$, which implies $\chi_1, \chi_2, ..., \chi_r$ are independent. Lastly, we shall prove that every character $\chi : G \to F^*$ can be represented as the product of the powers of $\chi_1, \chi_2, ..., \chi_r$. We know that χ maps σ_i to a m_i-th root of unity, so $\chi(\sigma_i) = \zeta_i^{k_i}$. Hence

$$\begin{aligned}\chi(\sigma) &= \prod_{i=1}^{r} \chi(\sigma_i^{\nu_i}) = \prod_{i=1}^{r} \zeta_i^{\nu_i k_i} = \prod_{i=1}^{r} \chi_i^{k_i}(\sigma_i^{\nu_i}) \\ &= \prod_{i=1}^{r} \chi_i^{k_i}(\sigma) = \left(\prod_{i=1}^{r} \chi_i^{k_i} \right)(\sigma), \quad \forall \sigma \in G.\end{aligned}$$

So we conclude that

$$\chi = \chi_1^{k_1} \chi_2^{k_2} \cdots \chi_r^{k_r}.$$

Let $\hat{G}_i = \langle \chi_i \rangle$, we know that $\hat{G}$ is the direct product of its cyclic subgroup $\hat{G}_i$, and that $|\hat{G}_i| = m_i$. Finally we conclude that $G \cong \hat{G}$.

2) Suppose

$$\sigma \in \bigcap_{\chi \in \hat{G}} \ker(\chi),$$

we represent σ using equation (1), applying χ_i on σ to get $1 = \chi_i(\sigma) = \zeta_i^{\nu_i}$, it follows that $m_i | \nu_i (i = 1, ..., r)$, so $\sigma = 1$, which is

$$\bigcap_{\chi \in \hat{G}} \ker(\chi) = \{1\}.$$

Q.E.D

From Lemma 1, we already know finite Abelian group G is isomorphic to its characteristic group $\hat{G}$. We could furtherly caluclate the characteristic group of $\hat{G}$, noted $\hat{\hat{G}}$, and obvioulsy $G \cong \hat{G} \cong \hat{\hat{G}}$, which appears to possess no further implications. However, it is worthwhile to consider how to construct the isomorphism from G to $\hat{\hat{G}}$ in a natural way. We write $\chi(\sigma)$, the character of G, in the symmetric form:

$$\chi(\sigma) = (\chi, \sigma),$$

which satisfies the following arithmetic:

$$(\chi_1 \chi_2, \sigma) = (\chi_1, \sigma)(\chi_2, \sigma) \tag{2}$$

and

$$(\chi, \sigma\tau) = (\chi, \sigma)(\chi, \tau) \tag{3}$$

The equation (3) suggests that $\chi : G \to F^*$ is a character, while the equation (2) implies σ induces a character $\hat{\sigma} : \hat{\hat{G}} \to F^*$. Using the notation of functions, we write:

$$\hat{\sigma}(\chi) = \chi(\sigma).$$

We compute:

$$\widehat{\sigma\tau}(\chi) = \chi(\sigma\tau) = \chi(\sigma)\chi(\tau) = \hat{\sigma}(\chi)\hat{\tau}(\chi) = \hat{\sigma}\hat{\tau}(\chi), \quad \forall \chi \in \hat{G}.$$

This implies $\widehat{\sigma\tau} = \hat{\sigma}\hat{\tau}$. It yields that the mapping $\sigma \to \hat{\sigma}$ is a homomorphism from G to $\hat{\hat{G}}$. Obviously, it is an injection. In fact, if $\hat{\sigma} = \hat{\tau}$, then $\hat{\sigma}(\chi) = \hat{\tau}(\chi), \quad \forall \chi \in \hat{G}$, so $\chi(\sigma) = \chi(\tau)$, $\chi(\sigma\tau^{-1}) = 1$, thus

$$\sigma\tau^{-1} \in \bigcap_{\chi \in \hat{G}} \ker(\chi).$$

It follows from Lemma 1 that $\sigma\tau^{-1} = 1, \sigma = \tau$. Then we obtain:

§ 1.3 Lemma 2

F, G are inherited from Lemma 1, $\forall \sigma \in G$ induces a character $\hat{\sigma}$ of $\hat{G}$:

$$\hat{\sigma}(\chi) = \chi(\sigma), \quad \chi \in \hat{G}.$$

Therefore, the mapping $\sigma \to \hat{\sigma}$ gives a standard isomorphism from G to $\hat{\hat{G}}$.

§ 1.4 Corollary

If the $\hat{H}$ is a subgroup of $\hat{g}$, satisfying $\bigcap_{\chi\in\hat{H}} \ker(\chi) = \{1\}$, then $\hat{H} = \hat{G}$.

Proof. Suppose n =ord(G), for ditinct $\sigma, \tau \in G$, we shall prove $\hat{\sigma}|_{\hat{H}}$ and $\hat{\tau}|_{\hat{H}}$ are not identical. Otherwise, $\hat{\sigma}(\chi) = \hat{\tau}(\chi), \quad \forall\chi \in \hat{H}$. Hence, $\chi(\sigma) = \chi(\tau)$, $\chi(\sigma\tau^{-1}) = 1$, $\forall\chi \in \hat{H}$. As a result

$$\sigma\tau^{-1} \in \bigcap_{\chi\in\hat{H}} \ker(\chi),$$

which is $\sigma\tau^{-1} \in \{1\}$. So $\sigma\tau^{-1} = 1$, $\sigma = \tau$, a contradiction! Consequently, $\hat{\sigma}|_{\hat{H}}$ induces n distinct characters of $\hat{H}$. Lemma 1 yields that $|\hat{H}| \geqslant n$. On the other hand, $\hat{H} \subset \hat{G}$, $|\hat{H}| \leqslant |\hat{G}| = n$. Hence $|\hat{H}| = n$, $\hat{H} = \hat{G}$.

Q.E.D

Next, we will investigate the Kummer expansion. Suppose the base field F contains m distinct m-th roots of unity, K/F is a finite Kummer m expansion, $G = Gal(K/F)$, $\hat{G}$ is characteristic group of G. For each $\chi \in \hat{G}$, according to Theorem 22 from chapter 8[3],$\exists\theta_\chi \in K^*$, s.t.

$$\chi(\sigma) = \theta_\chi^{\sigma-1}, \quad \sigma \in G \tag{4}$$

Because K/F is a Kummer m expansion, m' =ord(G)=ord$(\hat{G})$, $m'|m$. Hence $\chi^m = 1$. According to Lemma 4 from section 8, chapter 8[3]. Any θ_χ that satisfies equation (4), then $\theta_\chi^m \in F^*$. We immediately discover that the inverse is also true. Then we define a subgroup of K:

$$M_K = \{\theta \in K^* | \theta^m \in F^*\}.$$

Obviously $F^* \subset M_K$, and M_K includes all the solutions $\theta_\chi$to equation (4) (χ enumerates $\hat{G}$). Contrary to equation (4), we shall establish a mapping $\eta : M_K \to \hat{G}$: for each $\theta \in M_K$, $\theta^m = a \in F^*$, for any $\sigma \in G$, θ^σ and θ satisfies the equation $x^m = a$. Hence $\theta^\sigma = \zeta_\sigma\theta$, where ζ_σ is a m-th root of unity. By assumption, $\zeta_\sigma \in f^*(\forall\sigma \in G)$. Thus, the mapping $\sigma \to \theta^{\sigma-1} = \zeta_\sigma$ is not only a crossed homomorphism from G to K^*, but also a character from G to F^*, noted χ_θ. χ_θ is defined as

$$\chi_\theta(\sigma) = \theta^{\sigma-1}, \quad \theta \in M_K \tag{5}$$

Apparently, $\eta : \theta \mapsto \chi_\theta$ is a surjective homomorphism from M_K to $\hat{G}$, $\ker(\eta) = F^*$. This proves part of the following lemma.

§ 2 Base field containing all m-th roots of unity

§ 2.1 Lemma 3

Define M_K as previously defined. Then we have the following properties:

1) $M_K/F^* \cong G$, this isomorphism is implemented by the group homomorphism specified in (5) i.e. $\eta : \theta \mapsto \xi^\theta$, with $\ker(\eta) = F^*$.

2) If $x_1, \ldots, x_r$ generate G, then we can generate M_K/F^* using the cosets represented by $\theta_1, \ldots, \theta_r$ as specified in (4), that is, generate M_K using $\theta_1, \ldots, \theta_r$ and F^*.

3) Let $N_K = \{\theta^m | \theta \in M_K\}$ be denoted as M_K^m, then

$$M_K/F^* = N_K/F^{*m}$$

This isomorphism can be realized by the power mapping $\lambda : \theta \to \theta^m$, where $\theta \in M_K$.

Proof. 1) The conclusion can be obtained by applying the above results.

2) Directly follows from 1).

3) The mapping $\lambda : M_K \to N_K$ is clearly a surjective homomorphism, and λ maps F^* onto F^{*m}. Now consider the complete preimage of $\lambda(F^*)$ denoted as $\lambda^{-1}(F^{*m})$, where it is only necessary to prove $\lambda^{-1}(F^{*m}) = F^*$. It is evident that $F^* \subseteq \lambda^{-1}(F^{*m})$. At this point, let $\alpha \in \lambda^{-1}(F^{*m})$, then there exists $b \in F^{*m}$satisfying$\alpha^m = b$. Since $b \in F^{*m}$, there exists an $a \in F^*$ such that $b = a^m$.

Thus, $(\frac{a}{\alpha})^m = 1$, where $\frac{a}{\alpha} = \xi$ is an m-th root of unity. According to previous assumptions, $\xi \in F^*$, hence $\alpha = \xi a \in F^*$. Therefore, $F^* = \lambda^{-1}(F^{*m})$, and from this 3) is obtained.

Q.E.D

For each $a \in N_K$, the roots of the polynomial $x^m - a$ can be expressed as $\sqrt[m]{a}, \sqrt[m]{a}\xi_1, \ldots, \sqrt[m]{a}\xi_{m-1}$, where $\sqrt[m]{a}$ is any root of $x^m - a$,

and $1, \xi, \ldots, \xi^{m-1}$ are the m distinct mth roots of unity in F. Let $N_K^{\frac{1}{m}}$ denote the set of all roots of the polynomials $x^m - a = 0$, where $a \in N_k$. Since $M_K^m = N_K$ and $1, \xi_1, \ldots, \xi_{m-1} \subset M_K$, similarly we have $N_K^{\frac{1}{m}} = M_K$.

§ 2.2 Theorem 1

Let the base field F contain m distinct mth roots of unity, K/F be a finite m-Kummer extension, $G = \mathrm{Gal}(K/F)$, and $\hat{G}, M_K, N_K$ be defined as above. Then:

1) $K = F(M_K)$ is equivalent to $K = F(N_K^{1/m})$. More precisely, if the characters $\chi_1, \ldots, \chi_r$ generate $\hat{G}$, and define $\theta_{\chi_1}, \ldots, \theta_{\chi_r}$ as in (4). Then, $K = F(\theta_{\chi_1}, \ldots, \theta_{\chi_r})$ holds, and vice versa.

2) $\hat{G} \cong N_K/F^{*m}$.

Proof. 1) Let $\theta_{\chi_1}, \ldots, \theta_{\chi_r}$ generate $\hat{G}$. We want to prove that $K = F(\theta_{\chi_1}, \ldots, \theta_{\chi_r})$. Take $\sigma \in G$ and assume it fixes all θ_{χ_i}. Then, $\chi_i(\sigma) = \theta_{\chi_i}^{\sigma-1} = 1$ for $i = 1, \ldots, r$. Since $\chi_1, \ldots, \chi_r$ generate $\hat{G}$, for any $\chi \in \hat{G}$, χ can be expressed as $\chi = \chi_1^{e_1} \ldots \chi_r^{e_r}$. Therefore, $\chi(\sigma) = \prod_{i=1}^r \chi_i(\sigma)^{e_i} = 1$, and thus, $\sigma \in \bigcap_{\chi \in \hat{G}} \ker(\chi)$. By Lemma 1, we conclude that $\sigma = 1$. According to the Galois Fundamental Theorem, $F(\theta_{\chi_1}, \ldots, \theta_{\chi_r}) = K$.

2) This follows from Lemma 3.

Q.E.D

§ 2.3 Theorem 2

Let F contain m distinct mth roots of unity. Consider a subgroup N of the multiplicative group F^* such that $F^{*m} \subset N$ and $[N : F^{*m}]$ is finite. Let $N^{\frac{1}{m}}$ denote the set of all roots of the polynomials $x^m - a$, where $a \in N$. Adding $N^{\frac{1}{m}}$ to F yields an extension field $K = F(N^{\frac{1}{m}})$. Then, K/F is a finite Kummer extension of degree m, and M_K determined by the characteristic subgroup $\hat{G}$ of $G = \mathrm{Gal}(K/F)$ is equal to $N^{\frac{1}{m}}$.

Proof

For each polynomial $x^m - a$, where $a \in N$, arbitrarily choose one of its roots and denote it as $\sqrt[m]{a}$. Adding the set $S = \{ \sqrt[m]{a} \mid a \in N \}$ to F

forms an extension field $F(S)$. Since F contains m distinct mth roots of unity, $F(S)$ contains all the roots of $x^m - a$ for $a \in N$. Therefore, $K = F(\{ \sqrt[m]{a} \mid a \in N\})$, and K/F is separable. Thus, K/F is a Galois extension.

Next, we will prove that $G = \mathrm{Gal}(K/F)$ is a commutative group. Since each $\sigma \in G$ is determined by its action on S, it suffices to show that any two F-automorphisms of K, denoted as σ and τ, commute in their actions on each root $\sqrt[m]{a} \in N$.

Let

$$\sigma(\sqrt[m]{a}) = \zeta^r \sqrt[m]{a}, \quad \tau(\sqrt[m]{a}) = \zeta^s \sqrt[m]{a},$$

where ζ is a primitive mth root of unity in F. Then, we have

$$\sigma\tau(\sqrt[m]{a}) = \sigma(\zeta^s \sqrt[m]{a}) = \zeta^s \sigma(\sqrt[m]{a}) = \zeta^s \zeta^r \sqrt[m]{a} = \zeta^{r+s} \sqrt[m]{a}.$$

On the other hand,

$$\tau\sigma(\sqrt[m]{a}) = \tau(\zeta^r \sqrt[m]{a}) = \zeta^r \tau(\sqrt[m]{a}) = \zeta^r \zeta^s \sqrt[m]{a} = \zeta^{r+s} \sqrt[m]{a}.$$

Therefore, $\sigma\tau(\sqrt[m]{a}) = \tau\sigma(\sqrt[m]{a})$ holds for all $a \in N$, implying that $\sigma\tau = \tau\sigma$.

Furthermore, for all $a \in N$, we have

$$\sigma^m(\sqrt[m]{a}) = \sigma^{m-1}(\zeta^r \sqrt[m]{a}) = \cdots = \zeta^{rm} \sqrt[m]{a} = \sqrt[m]{a}.$$

Therefore, $\zeta^m = 1$. Thus, G is a commutative group with an exponent divisible by m. Finally, before establishing the mapping $\eta : N^m \to \hat{G}$, we need to show that $[K : F]$ is finite. Since $[N : F^{*m}]$ is finite, we can decompose N into cosets of F^{*m} as $N = a_1 F^{*m} \cup \cdots \cup a_s F^{*m}$. It is evident that $K = F(\sqrt[m]{a_1}, \ldots, \sqrt[m]{a_s})$. Hence, $[K : F] \leq m^s < \infty$.

Let $N^{\frac{1}{m}}$ be denoted as M. Each element θ in M is a root of some polynomial $x^m - a$, where $a \in N$. Conversely, every root of a polynomial $x^m - a$, $a \in N$, is an element of M, and $F^* \subset M$. Each element θ in M determines a group homomorphism from G to K^* denoted as $\chi_\theta : \sigma \to \theta^{\sigma-1}$, where $\sigma \in G$. Since both θ and θ^σ are roots of $x^m - a$ for some $a \in N$, and $\theta^{\sigma-1}$ is an mth root of unity, χ_θ is a character of G. Now, we can define $\eta : N^m \to \hat{G}$ as follows:

$$\eta(\theta) = \chi_\theta$$

Then, $\eta : N \to G$ is a homomorphism fromN^m to $\hat{G}$ with $\ker(\eta) = F^*$. Finally, we prove that η is surjective. Let $\eta(M) = \hat{H}$, where $\hat{H}$ is a subgroup of $\hat{G}$. To show that $\hat{H} = \hat{G}$, we first assert that $\bigcap_{\chi\in\hat{H}} \ker(\chi) = \{1\}$. Suppose $\sigma \in G$ is an element satisfying $\chi_\theta(\sigma) = 1 \quad \forall\theta \in M$. Then, for all $\theta \in \hat{G}$, we have $\sigma(\theta) = \theta$. This implies that σ is the identity automorphism of K, so $\sigma = 1$. Therefore, $\bigcap_{\chi\in\hat{H}} \ker(\chi) = \{1\}$. According to the corollary of Lemma 2, we have $H = G$. Thus, η is a surjective homomorphism fromN^m to $\hat{G}$ with $\ker(\eta) = F^*$.

It is also shown that if $\chi_1, \ldots, \chi_r$ generate $\hat{G}$, then M is generated by $\theta_{\chi_1}, \ldots, \theta_{\chi_r}$ specified in (4) and F^*.Now M is M_K as in Lemma 3,therefore, $N^{\frac{1}{m}} = M_K$.

Q.E.D

It should be noted that since F contain m distinct mth roots of unity,it is not difficult to find that the selection of different representatives in N/F^* will not affect the results of domain expansion.

§ 2.4 The situation on field of prime characteristic

According to the past learning experience of abstract algebra, the structure of domain expansion is much clearer on the domain characterized by p, so we will discuss it in depth.We will assume that the base field F has character p which is a prime number. Naturally F_p is a subfield of it. Let K/F be a p^n degree abelian extension and $G = \mathrm{Gal}(K/F)$ is an elementary p-group i.e. G is an $(p, p, \ldots, p)$-type abelian group. A homomorphism from G to the additive group F_p^+ is called the characteristic character of G denoted by χ, χ_1, χ_2, etc. Then

$$\chi(\sigma\tau) = \chi(\sigma) + \chi(\tau) \quad \forall\sigma, \tau \in G.$$

The operations are defined as

$$\chi_1 + \chi_2(\sigma) = \chi_1(\sigma) + \chi_2(\sigma).$$

In this way, the set of characteristic characters of G forms a group called the characteristic character group of G, denoted as $\hat{G}$. Lemmas 1 and 2 along with their corollaries remain valid in the current situation. Each characteristic character χ of G satisfies the additive form of the Noether equation. According to Theorem 26 chapter 8[3], there exists an $\theta_x \in K$ such that

$$\chi(\sigma) = \sigma(\theta_x) - \theta_x \quad \forall \sigma \in G. \tag{6}$$

For any element $a \in F$, $a+\theta_x$ satisfies equation (6) just like θ_x does. That is,

$$\begin{aligned}\sigma(a + \theta_x) - (a + \theta_x) &= \sigma(a) + \sigma(\theta_x) - a - \theta_x \\ &= a + \sigma(\theta_x) - a - \theta_x = \sigma(\theta_x) - \theta_x = \chi(\sigma).\end{aligned}$$

Conversely, suppose θ is any element of K and satisfies

$$\chi(\sigma) = \sigma(\theta) - \theta \quad \forall \sigma \in G. \tag{7}$$

Subtracting (6) from (7) yields

$$0 = \sigma(\theta - \theta_x) - (\theta - \theta_x).$$

Thus,

$$\sigma(\theta - \theta_x) = \theta - \theta_x \quad \forall \sigma \in G.$$

According to the definition of a Galois extension, we have that $\theta - \theta_x = a \in F$, which implies that θ belongs to the coset $\theta_x + F$. Therefore, all solutions to equation (7) are of the form $\theta_x + F$ for a given x.

Next, let's provide another explicit description of the elements in $\theta_x + F$. Since $\chi(\sigma) \in F_p$ we have $\chi(\sigma)^p = \chi(\sigma)$. Raising both sides of equation (7) to the power of p and considering $\chi(F) = p$, we obtain:

$$\chi(\sigma) = \sigma(\theta^p) - \theta^p. \quad (8) \tag{8}$$

(8) - (7) gives

$$\sigma(\theta^p) - \theta = \theta^p - \theta \quad \forall \sigma \in G.$$

Therefore, $\theta^p - \theta = a \in F$. Thus, θ is a root of the polynomial

$$x^p - x - a \quad (a \in F). \quad (9) \tag{9}$$

On the contrary, for any $a \in F$, suppose the polynomial (9) has a root θ in K. Define

$$\chi_\theta(\sigma) = \sigma(\theta) - \theta, \quad \sigma \in G. \quad (10)$$

Certainly, χ_θ is a cross-homomorphism from G to K^+. Not only that, raising (10) to the power of p,

$$\chi_\theta(\sigma)^p = \sigma(\theta^p) - \theta^p,$$

then subtracting (10) yields

$$\chi_\theta(\sigma)^p - \chi_\theta(\sigma) = \sigma(\theta^p - \theta) - (\theta^p - \theta) = \sigma(a) - a = 0$$

Thus $\chi_\theta(\sigma)^p = \chi_\theta(\sigma)$, $\chi_\theta(\sigma) \in F_p$ for all $\sigma \in G$, making χ_θ a character of G. In conclusion, the character χ_θ defined by (10) is a character of G if and only if θ is a root of the polynomial (9).

We now introduce some notations for convenience: use P_θ to represent $\theta^p - \theta$, $\theta \in K$. For a subset $S \subset K$, use $P(S)$ to denote $\{P(\theta)|\theta \in S\}$.The polynomial (9) can be expressed as$P(x) - a$, and $P^{-1}(a)$ denotes any root of the polynomial (9) in K. $P^{-1}(S)$represents the set of all roots of polynomials$x^p - x - a(a \in S)$. Let$M_K = \{\theta \in K \mid P(\theta) \in F\}$,$N_K = P(M_K)$. The first part of the lemma is as follows:

§ 3 Generalization to previous theorems

§ 3.1 Lemma 4

1)For each element θ in M_K, the character χ_θ defined by (10) is a character of G. Conversely, for every element χ_θ in G, all solutions θ of (7) belong to M_K.

2)$M_K/F^+ \cong G$. This isomorphism can be realized by the mapping $\eta : \theta \mapsto \chi_\theta$ defined by (10). Thus, $\chi_1 \cdots \chi_r$ generate $\hat{G}$ if and only if $\theta_{\chi_1} \cdots \theta_{\chi_r}$ and F^+ generate M_K.

3)$M_K/F^+ \cong N_K/P(F^+)$. This isomorphism can be realized by the mapping $P : \theta \mapsto P(\theta), \theta \in M_K$.

Proof. 1)Proven above.

2)The mapping $\eta : \theta \mapsto \chi_\theta$ defined by (10) is proven to be a surjection from M_K to $\hat{G}$ from 1) and from the operations of $\hat{G}$ it is known to be a homomorphism. χ_θ is a zero homomorphism from G to F_p if and only if $\sigma(\theta) = \theta$ (for all $\sigma \in G$) i.e., $\theta \in F$. Hence $\ker(\eta) = F^+$.

3) According to the definition of N_K the mapping $\theta \mapsto P(\theta)$ from M_K to N_K is a surjection. Moreover, for θ_1, θ_2 we have

$$P(\theta_1 + \theta_2) = (\theta_1 + \theta_2)^p - (\theta_1 + \theta_2) = \theta_1^p + \theta_2^p - \theta_1 - \theta_2 = P(\theta_1) + P(\theta_2)$$

so P is a homomorphism. Clearly, P maps F^+ to $P(F^+)$ i.e., $F^+ \subset P^{-1}(P(F^+))$. Conversely, if $\alpha \in P^{-1}(P(F^+))$ then there exists an $a \in F$ such that $P(\alpha) = P(a)$ i.e., $\alpha^p - \alpha = a^p - a$. Moving terms we have $\alpha - a = b \in F_p$. Since $F_p \subset F$ it follows that $\alpha = a + b \in F^+$. Thus, $P^{-1}(P(F^+)) = F^+$. From this, we get

$$M_K/F^+ \cong N_K/P(F^+)$$

.

Q.E.D

§ 3.2 Theorem 3

Let K/F be an elementary p-group. Define M_K, N_K, P as before. Then

1)

$$K = F(M_K) = F(P^{-1}(N_K)).$$

More precisely, if $\chi_1, \ldots, \chi_r$ are generators of G, then the elements $\theta_{\chi_1}, \ldots, \theta_{\chi_r}$ defined by (6) generate K over F, i.e., $K = F(\theta_{\chi_1}, \ldots, \theta_{\chi_r})$.

2) $G \cong N_K/P(F^+)$.

Proof. 1) Let $\chi_1, \ldots, \chi_r$ be a set of generators for G. We want to prove that

$$K = F(\theta_{\chi_1}, \ldots, \theta_{\chi_r}).$$

Suppose σ is an element of G such that $\sigma(\theta_{\chi_i}) = \theta_{\chi_i}$ for $i = 1, \ldots, r$ which implies $\chi_i(\sigma) = 0$. Since $\chi_1, \ldots, \chi_r$ generate G, any element χ in $\hat{G}$ can be expressed as a linear combination of $\chi_1, \ldots, \chi_r$ with integer coefficients:

$$\chi = e_1\chi_1 + \ldots + e_r\chi_r.$$

Thus,

$$\chi(\sigma) = \sum_{i=1}^{r} e_i\chi_i(\sigma) = 0$$

which implies

$$\sigma = id$$

. Hence, every element of K is fixed by every σ in G that fixes $\theta_{\chi_1}, \ldots, \theta_{\chi_r}$. Since $G = \mathrm{Gal}(K/F)$, it follows that every element of K is in $F(\theta_{\chi_1}, \ldots, \theta_{\chi_r})$, proving the theorem.

2) Follows directly from Lemma 4.

Q.E.D

§ 3.3 Theorem 4

Let F be a field with prime characteristic p. Suppose N is a subgroup of the additive group F^+ containing $P(F^+)$ and $[N : P(F^+)]$ is finite. Denote by K the field obtained by adding the roots of all polynomials $P(x) - a$ $(a \in N)$ to F. Then

1) K is a finite abelian extension of degree p^n and $G = \mathrm{Gal}(K/F)$ is an elementary p-group.

2) $P^{-1}(N)$ is equal to the field M_K determined by the character group G.

Proof. By adding a root θ of $P(x) - a$ to F we include all roots $\theta, \theta + 1, \ldots, \theta + p - 1$ of $P(x) - a$ in the extension $F(\theta)$. Therefore K/F is separable. Choose a set of elements $a_1, \ldots, a_r$ in N such that the cosets $a_1, \ldots, a_r$ generate $N/P(F^+)$. Let θ_i be a root of $P(x) - a_i$ and consider the field $L = F(\theta_1, \ldots, \theta_r)$. Any element a in N can be expressed as:

$$a = k_1 a_1 + \ldots + k_r a_r + b,$$

where $k_i \in F_p, b \in P(F^+)$. The term b can be expressed as $b = c^p - c, c \in F$. Through calculation, it is evident that $\theta = k_1\theta_1 + \ldots + k_r\theta_r + c$ is a root of $P(x) - a$.

$$\begin{aligned} \theta^p - \theta &= (k_1\theta_1 + \ldots + k_r\theta_r + c)^p - (k_1\theta_1 + \ldots + k_r\theta_r + c) \\ &= k_1(\theta_1^p - \theta_1) + \ldots + k_r(\theta_r^p - \theta_r) + c^p - c \\ &= k_1 a_1 + \ldots + k_r a_r + b = a. \end{aligned}$$

Therefore, L also contains a root of each $P(x) - a$ (where $a \in N$) and, of course, includes all of their roots. Consequently, $L = K$. This indicates that K/F is a finite separable normal extension. Next, we prove that $G = \mathrm{Gal}(K/F)$ is a commutative group.

Let σ, τ be any two elements of G. For each $a \in N$, let θ represent a root of $P(x) - a$. The actions of σ and τ on θ are given by:

$$\sigma(\theta) = \theta + j, \quad \tau(\theta) = \theta + k,$$

where $j, k \in F_p$. Then, the actions of $\sigma\tau$ and $\tau\sigma$ on θ are:

$$\sigma\tau(\theta) = \sigma(\tau(\theta)) = \sigma(\theta + k) = \theta + j + k,$$

$$\tau\sigma(\theta) = \tau(\sigma(\theta)) = \tau(\theta + j) = \theta + k + j,$$

thus demonstrating that $\sigma\tau = \tau\sigma$, and hence G is commutative.

Similarly,

$$\tau\sigma(\theta) = \tau(\theta + j) = \theta + k + j$$

. Thus the actions of σ and τ on the roots of $P(x) - a$ commute, implying $\sigma\tau = \tau\sigma$. This proves that G is a commutative group. Now let's calculate the order of σ.

$$\sigma^p(\theta) = \sigma^{p-1}(\theta + j) = \sigma^{p-2}(\theta + 2j) = \cdots = \theta + pj = \theta$$

. The action of σ^p keeps each root of $P(x) - a$ fixed. Thus $\sigma^p = 1$ implying $\sigma = 1$ or the order of σ is p. Therefore G is an elementary p-group.

Let M represent the set of all roots of polynomials $P(x)-a$ $(a \in N)$ then $P(M) = N$ and $F \subset M$. For each $\theta \in M$ using the definition in (7) we define a crossed homomorphism χ_θ from G to K i.e. $\chi_\theta(\sigma) = \sigma(\theta) - \theta$ for all $\sigma \in G$.According to the definition of M, $P(\theta) in N$. Following the proof of the first part of conclusion 1) in Lemma 4, it is known that $\chi_\theta(\sigma) \in F_p$ for all $\sigma \in G$.

Now, we can define $\eta : M \to \hat{G}$ as follows:

$$\eta(\theta) = \chi_\theta$$

Then, $\eta : N \to G$ is a homomorphism fromN^m to $\hat{G}$ with $\ker(\eta) = F^*$. Finally, we prove that η is surjective. Let $\eta(M) = \hat{H}$, where $\hat{H}$ is a subgroup of $\hat{G}$. To show that $\hat{H} = \hat{G}$, we first assert that $\bigcap_{\chi \in \hat{H}} \ker(\chi) = \{1\}$. Suppose $\sigma \in G$ is an element satisfying $\chi_\theta(\sigma) = 1 \quad \forall \theta \in M$. Then, for all $\theta \in \hat{G}$, we have $\sigma(\theta) = \theta$. This implies that σ is the identity automorphism of K, so $\sigma = 1$. Therefore, $\bigcap_{\chi \in \hat{H}} \ker(\chi) = \{1\}$. According to the corollary of Lemma 2, we have $H = G$. Thus, η is a surjective homomorphism fromN^m to $\hat{G}$ with $\ker(\eta) = F^*$.

It is also shown that if $\chi_1, \ldots, \chi_r$ generate $\hat{G}$, then M is generated by $\theta_{\chi_1}, \ldots, \theta_{\chi_r}$ and F^*.According to Lemma 4, it is concluded tha $M = M_K$,i.e. $P^{-1}(N) = M_K$

Q.E.D

References

[1] A. D. Aleksandrov *et al.*, *Mathematics: Its Content, Meaning, and Method*. Science Press, 2001.

[2] Z. Sun, *Modern Algebra*. Nanjing University Press, 2022.

[3] S. Ding and L. Nie, "Introduction to algebra," *Educational Publishing House*, 2000.

[4] J. L. Alperin, *Local Representation Theory: Modular Representations as an Introduction to the Local Representation Theory of Finite Groups*. Cambridge University Press, 1995.

[5] N. Bourbaki, *Algebra II: Chapters 4–7*. Springer, 2003, contains detailed discussions on field theory and extensions relevant to Kummer Theory.

[6] J. Cassels and A. Fröhlich, Eds., *Algebraic Number Theory*. Academic Press, 1967, includes foundational results on Kummer theory.

[7] D. A. Cox, *Galois Theory*. John Wiley & Sons, 2013.

[8] H. M. Edwards, *Galois Theory*. Springer, 1977.

[9] N. Jacobson, *Basic Algebra I and II*. Dover Publications, 2009.

[10] S. Lang, "Cyclotomic fields and modular functions," *Bulletin of the American Mathematical Society*, vol. 25, no. 2, pp. 205–220, 1991.

[11] J. S. Milne, *Algebraic Number Theory*. Cambridge University Press, 2017, available online: https://www.jmilne.org/math/CourseNotes/ant.html.

[12] M. R. Murty, *Problems in Algebraic Number Theory*. Springer, 1999.

[13] J. Neukirch, *Algebraic Number Theory*. Springer, 2013.

[14] J. J. Rotman, *Advanced Modern Algebra*. American Mathematical Society, 2012, comprehensive coverage of Galois Theory and related topics.

[15] J.-P. Serre, *Topics in Galois Theory*. A K Peters/CRC Press, 2008.

[16] R. T. Sharifi, "Kummer theory for fields with additive valuation," *Manuscripta Mathematica*, vol. 123, pp. 245–257, 2007.

[17] L. C. Washington, *Introduction to Cyclotomic Fields*, ser. Graduate Texts in Mathematics. Springer, 1997, vol. 83.

[18] C. Weibel, "Galois cohomology and algebraic cycles," *AMS Contemporary Mathematics*, vol. 750, pp. 1–35, 2019.