Galois Theory of Cyclotomic Extensions

Winter School 2014, IISER Bhopal

Romie Banerjee, Prahlad Vaidyanathan

I. Introduction

1. Course Description

The goal of the course is to provide an introduction to algebraic number theory, which is essentially concerned with understanding algebraic field extensions of the field of rational numbers, $\mathbb{Q}$.

We will begin by reviewing Galois theory:

1.1. Rings and Ideals, Field Extensions

1.2. Galois Groups, Galois Correspondence

1.3. Cyclotomic extensions

We then discuss Ramification theory:

1.1. Dedekind Domains

1.2. Inertia groups

1.3. Ramification in Cyclotomic Extensions

1.4. Valuations

This will finally lead to a proof of the Kronecker-Weber Theorem, which states that *If* $\mathbb{Q} \subset L$ *is a finite Galois extension whose Galois group is abelian, then* $\exists n \in \mathbb{N}$ *such that* $L \subset \mathbb{Q}(\zeta_n)$*, where* ζ_n *denotes a primitive* n^{th} *root of unity*

2. Pre-requisites

A first course in Galois theory. Some useful books are :

2.1. Ian Stewart, *Galois Theory (3rd Ed.)*, Chapman & Hall (2004)

2.2. D.J.H. Garling, *A Course in Galois Theory*, Camridge University Press (1986)

2.3. D.S. Dummit, R.M. Foote, *Abstract Algebra (2nd Ed.)*, John Wiley and Sons (2002)

3. Reference Material

3.1. M.J. Greenberg, *An Elementary Proof of the Kronecker-Weber Theorem*, The American Mathematical Monthly, Vol. 81, No. 6 (Jun.-Jul. 1974), pp. 601-607.

3.2. S. Lang, *Algebraic Number Theory*, Addison-Wesley, Reading, Mass. (1970)

3.3. J. Neukrich, *Algebraic Number Theory*, Springer (1999)

4. Pre-requisites

4.1. Definition:

(i) Rings

(ii) Commutative Ring

(iii) Units in a ring

(iv) Field

4.2. Examples:

(i) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$

(ii) $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ for $p \in \mathbb{Z}$ prime

(iii) Definition: Let k be a field

(a) A polynomial over k

(b) Polynomial ring $k[x]$

(c) Degree of a polynomial

4.3. (Euclidean Division): Let k be a field. If $f, g \in k[x]$ with $g \neq 0, \exists t, r \in k[x]$ such that $f = tg + r$ and $\deg(r) < \deg(g)$

4.4. $k[x]$ is a principal ideal domain (PID).

4.5. Definition: Let k be a field.

(i) $f \mid g$ in $k[x]$

(ii) GCD of f and g.

4.6. Theorem: Let k be a field. If $f, g \in k[x]$, then the GCD d of f and g exists in $k[x]$. Furthermore, $\exists s, t \in k[x]$ such that $d = sf + tg$. We write $d = (f, g)$

4.7. Definition:

(i) Ideal in a ring

(ii) Maximal ideal

(iii) Irreducible polynomial $f \in k[x]$

4.8. Theorem: For $f \in k[x]$, the following are equivalent:

(i) f is irreducible in $k[x]$

(ii) The ideal (f) is a maximal ideal

(iii) $k[x]/(f)$ is a field

4.9. Examples:

(i) Polynomials of degree 1 are automatically irreducible

(ii) $x^2 - 2$ is irreducible in $\mathbb{Q}[x]$, but not $\mathbb{R}[x]$

(iii) Polynomial of degree 2 or 3 is irreducible in $k[x]$ iff it does not contain a root in k (Exercise)

4.10. (Gauss Lemma): Let $f \in \mathbb{Z}[x]$ be monic, then f is irreducible in $\mathbb{Z}[x]$ iff it is irreducible in $\mathbb{Q}[x]$

4.11. (Rational Root theorem): Let $f(x) = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Z}[x]$ have a root $p/q \in \mathbb{Q}$ where $(p, q) = 1$. Then

(i) $p \mid a_0$ and $q \mid a_n$

(ii) In particular, if f is monic, then every rational root of f must be an integer.

4.12. (Eisenstein's Criterion): Let $f(x) = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Z}[x]$. Suppose $\exists p \in \mathbb{Z}$ prime such that

(i) $p \mid a_i$ for all $i \in \{0, 1, \ldots, n-1\}$

(ii) $p \nmid a_n$

(iii) $p^2 \nmid a_0$

Then f is irreducible in $\mathbb{Q}[x]$

4.13. (Reduction (mod p)): Let $f(x) = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Z}[x]$ and $p \in \mathbb{Z}$ prime such that $p \nmid a_n$. If $\overline{f}$ is irreducible in $\mathbb{Z}_p[x]$, then f is irreducible in $\mathbb{Q}[x]$.

(The converse is not true: $f(x) = x^4 + 1 \in \mathbb{Z}[x]$ is reducible in $\mathbb{Z}_2[x]$)

4.14. (Fundamental Theorem of Algebra): For any non-constant $f \in \mathbb{C}[x], \exists \alpha \in \mathbb{C}$ such that $f(\alpha) = 0$

II. Field Extensions

1. Simple Extensions

1.1. Remark: In this course, we will consider two kinds of fields :

(i) Finite fields, such as $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}, p \in \mathbb{Z}$ prime

(ii) Subfields of $\mathbb{C}$ (which are necessarily infinite), such as $\mathbb{Q}, \mathbb{R}, \mathbb{C}$

We will begin by only considering subfields of $\mathbb{C}$, and discuss finite fields later.

1.2. Definition:

(i) Field extension $k \subset L$

(ii) Smallest field $k(X)$ generated by a field $k \subset \mathbb{C}$ and a set $X \subset \mathbb{C}$.

(iii) A field extension $k \subset L$ is called simple if $\exists \alpha \in L$ such that $L = k(\alpha)$. α is called a primitive element of the field extension. Note: The primitive element may not be unique (See Example 1.3(ii))

1.3. Examples:

(i) $\mathbb{Q} \subset \mathbb{R}, \mathbb{Q} \subset \mathbb{C}$ are field extensions, but neither are simple. (Proof later)

(ii) $\mathbb{R} \subset \mathbb{C}$ is a simple extension. $\mathbb{C} = \mathbb{R}(i)$. Note that $\mathbb{C} = \mathbb{R}(i+1)$ as well, so the primitive element may not be unique.

(iii) Every subfield $k \subset \mathbb{C}$ contains $\mathbb{Q}$. So $\mathbb{Q} \subset k$ is a field extension. (Exercise)

(iv) Let $F = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, then

(a) F is a field

(b) Hence, $\mathbb{Q} \subset F$ is a field extension

(c) Note that $F = \mathbb{Q}(\sqrt{2})$

(v) Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, then $K = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ and is hence a simple extension

(vi) Let k be a field and $f \in k[x]$ be irreducible. Set $L = k[x]/(f)$, then $k \subset L$ is a field extension.

1.4. Definition/Remark: Let $k \subset \mathbb{C}$ be a field and $\alpha \in \mathbb{C}$

(i) α is said to be algebraic over k if $\exists 0 \neq f \in k[x]$ such that $f(\alpha) = 0$.

(ii) α is said to be transcendental over k if it is not algebraic.

1.5. Examples:

(i) If $\alpha \in k$, then α is algebraic over k

(ii) $\sqrt{2}$ is algebraic over $\mathbb{Q}$

(iii) π is transcendental over $\mathbb{Q}$ (without proof)

(iv) π is algebraic over $\mathbb{R}$

1.6. Theorem: Let $k \subset L$ be a field extension and $\alpha \in L$ be algebraic over k. Then $\exists$ unique polynomial $f \in k[x]$ such that

(i) f is monic and irreducible

(ii) $f(\alpha) = 0$

Furthermore, if $g \in k[x]$ is any polynomial, then $g(\alpha) = 0$ iff $f \mid g$ in $k[x]$. This is called the minimal polynomial of α over k and is denoted by $m_\alpha := m_{\alpha,k}$.

Proof. Let

$$I = \{g \in k[x] : g(\alpha) = 0\}$$

Then by hypothesis, $I \neq \{0\}$. Also, I is clearly an ideal in $k[x]$. Since $k[x]$ is a PID, $\exists f \in I$ such that

$$I = (f)$$

By dividing by the leading coefficient, we may assume f is monic.

(i) f is irreducible: If $f = gh$, then $0 = f(\alpha) = g(\alpha)h(\alpha)$. Since $\mathbb{C}$ is a field, either $g(\alpha) = 0$ or $h(\alpha) = 0$. Assume WLOG that $g(\alpha) = 0$, then $g \in I$ to $f \mid g$. However, $g \mid f$ as well, so $g = cf$ for some constant $c \in k$. Hence, $\deg(h) = 0$, which means that $h \in k$

(ii) Suppose $g \in k[x]$ is irreducible, monic and satisfies $g(\alpha) = 0$. Then, $g \in I$ and so $f \mid g$. But g is irreducible, so $f = cg$ for some $c \in k$. They are both monic, so $c = 1$. Hence we get uniqueness as well.

(iii) Since f is irreducible, I is a maximal ideal, and so $k[x]/I$ is a field. Define

$$\varphi : k[x] \to \mathbb{C} \text{ by } f \mapsto f(\alpha)$$

Then φ is a homomorphism and $I = \ker(\varphi)$. Thus, Image(φ) is a field.

(iv) Clearly, $k \subset \text{Image}(\varphi)$ and $\alpha \in \text{Image}(\varphi)$. So

$$k(\alpha) \subset \text{Image}(\varphi)$$

Conversely, if $\beta \in \text{Image}(\varphi)$, then $\exists f \in k[x]$ such that $\beta = f(\alpha)$. Thus, $\beta \in k(\alpha)$. Hence,

$$\text{Image}(\varphi) = k(\alpha)$$

□

1.7. Examples:

(i) If $\alpha \in k$, then $m_\alpha(x) = x - \alpha$

(ii) If $k = \mathbb{Q}, \alpha = \sqrt{2}$, then $m_\alpha(x) = x^2 - 2$

(iii) If $k = \mathbb{R}, \alpha = \sqrt{2}$, then $m_\alpha(x) = x - \sqrt{2}$

(iv) If $k = \mathbb{Q}, \zeta_p = e^{2\pi i/p}$, where p is a prime, then

$$m_{\zeta_p}(x) = \Phi_p(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$$

1.8. Definition: Let $k \subset L_1$ and $k \subset L_2$ be field extensions

(i) A homomorphism of field extensions is a field homomorphism $\varphi : L_1 \to L_2$ such that $\varphi(\alpha) = \alpha$ for all $\alpha \in k$.

(ii) An isomorphism of field extensions is a bijective homomorphism. If such an isomorphism exists, we write

$$L_1 \cong_k L_2$$

1.9. Theorem: Let $k \subset \mathbb{C}$ be a field and $\alpha \in \mathbb{C}$ be algebraic over k. Then

$$k[x]/(m_\alpha) \cong_k k(\alpha)$$

Proof. Example 1.3.(vi) and Theorem 1.6 □

1.10. Corollary: Let $k \subset L$ be a field extension and $\alpha, \beta \in L$ be algebraic over k with the same minimal polynomial. Then there is an isomorphism of field extensions $k(\alpha) \cong_k k(\beta)$ which sends $\alpha \mapsto \beta$.

Exercises

1.1. Let k be a field and let $f \in k[x]$ be of degree 2 or 3. Prove that f is irreducible in $k[x]$ iff f does not have a root in k.

1.2. (i) Prove that $f(x)$ is irreducible in $\mathbb{Z}[x]$ iff $f(x+1)$ is irreducible.

(ii) Let $p \in \mathbb{Z}$ be a prime, then prove that, for any $1 \leq k \leq p-1$,

$$p \mid \binom{p}{k}$$

(iii) Use (i) and (ii) to prove that

$$\Phi_p(x) := \frac{x^p - 1}{x - 1} = \sum_{i=0}^{p-1} x^i$$

is irreducible in $\mathbb{Z}[x]$

1.3. Let $f(x) = x^4 + 1 \in \mathbb{Z}[x]$. Use Part (i) of the previous problem to prove that f is irreducible in $\mathbb{Z}[x]$

1.4. Let k be a field. Define $\varphi : \mathbb{Z} \to k$ by $n \mapsto n \cdot 1$.

(i) Prove that $\ker(\varphi)$ is either trivial or $\exists p \in \mathbb{Z}$ such that $\ker(\varphi) = p\mathbb{Z}$.

(ii) If $k \subset \mathbb{C}$ is any field, then prove that $\mathbb{Q} \subset k$

(iii) If k is a finite field, then prove that $\exists p \in \mathbb{Z}$ prime such that $\mathbb{Z}_p \subset k$.

Definition: We say a field has <u>characteristic</u> $n \in \mathbb{Z}$ iff $\ker(\varphi) = n\mathbb{Z}$. We write

$$\text{char}(k) = n$$

Note: By the proof of (i), n must either be 0 or a prime. Hence,

(i) If $k \subset \mathbb{C}$, then $\text{char}(k) = 0$

(ii) If k is a finite field, then $\text{char}(k) = p$ for some prime $p \in \mathbb{Z}$

1.5. (i) If $f(x) \in \mathbb{Z}[x]$ is irreducible, then prove that $f(-x) \in \mathbb{Z}[x]$ is irreducible.

(ii) Determine the minimal polynomial of $\alpha = e^{\pi i/5}$ over $\mathbb{Q}$.

1.6. Let $\varphi : \mathbb{Q} \to \mathbb{C}$ be a homomorphism of fields, then prove that $\varphi(x) = x \quad \forall x \in \mathbb{Q}$

Note: Since φ is a field homomorphism, $\varphi(1) = 1$ must hold by definition.

1.7. Determine all possible homomorphisms $\varphi : \mathbb{Q}(\sqrt{2}) \to \mathbb{C}$

[*Hint:* Use the previous problem to prove that any such homomorphism is completely determined by $\varphi(\sqrt{2})$. Now determine the possible values of $\varphi(\sqrt{2})$]

1.8. Let $\omega = e^{2\pi i/3}$. Prove that there is an isomorphism

$$\mathbb{Q}(\sqrt[3]{2}) \cong_{\mathbb{Q}} \mathbb{Q}(\omega\sqrt[3]{2})$$

1.9. Is the set

$$L := \{a + b\pi : a, b \in \mathbb{Q}\}$$

a field?

1.10. (i) Let $k \subset L$ be a field extension, then L is a k-vector space.

(ii) If $k \subset L_1$ and $k \subset L_2$ are two extensions, then a homomorphism $\varphi : L_1 \to L_2$ of $k-$extensions is a k-linear map of vector spaces.

Definition: Let $k \subset L$ be a field extension

(i) The <u>degree</u> of the extension, denoted by $[L : k]$, is the dimension of the k-vector space L.

(ii) The field extension is called <u>finite</u> if $[L : k] < \infty$.

1.11. Prove that

(i) $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ is a finite extension of degree 2.

(ii) $\mathbb{Q} \subset \mathbb{R}$ is not a finite extension. [*Hint:* $\mathbb{Q}$ is countable, and $\mathbb{R}$ is not]

1.12. If k is a finite field, then prove that $\exists p \in \mathbb{N}$ prime and $n \in \mathbb{N}$ such that $|k| = p^n$

1.13. Let $\mathbb{Q} \subset L$ be a field extension of degree 2 with $\mathbb{Q}$-basis $\{1, \alpha\}$.

(i) Prove that α satisfies a polynomial $f \in \mathbb{Q}[x]$ of degree 2.

(ii) Prove that $\exists r \in \mathbb{Q}$ such that $L = \mathbb{Q}(\sqrt{r})$

[*Hint:* Use the quadratic formula]

2. Finite and Algebraic Extensions

2.1. Recall: If $k \subset L$ is a field extension, then

(i) L is a k-vector space

(ii) The dimension of L over k is called the degree of the extension, and is denoted by $[L : k]$

(iii) $k \subset L$ is called a finite extension iff $[L : k] < \infty$

2.2. Theorem: Let $k \subset \mathbb{C}$ be a field and $\alpha \in \mathbb{C}$ be algebraic over k. Let $m_\alpha \in k[x]$ be the minimal polynomial of α over k, and let $n = \deg(m_\alpha)$. Then

(i) $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a basis for $k(\alpha)$ over k

(ii) In particular, $[k(\alpha) : k] = \deg(m_\alpha) < \infty$

Proof. Let $S = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$.

(i) S is linearly independent: Suppose $\exists a_0, a_1, \ldots, a_{n-1} \in k$ not all zero such that

$$\sum_{i=0}^{n-1} a_i \alpha^i = 0$$

Then α satisfies the non-zero polynomial $f(x) = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} \in k[x]$. This contradicts the minimality of $n = \deg(m_\alpha)$.

(ii) S spans $k(\alpha)$: Suppose $\beta \in k(\alpha)$, then by Theorem 1.9, $\exists f \in k[x]$ such that $\beta = f(\alpha)$. By Euclidean division, $\exists t, r \in k[x]$ such that

$$f = t m_\alpha + r, \text{ where } \deg(r) < n$$

Clearly, $f(\alpha) = r(\alpha)$, so $\beta = r(\alpha)$ and $\deg(r) < n$. Hence, $\beta \in \text{Span}(S)$.

□

2.3. Examples:

(i) $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ (This agrees with Example 1.3(iv))

(ii) $\mathbb{Q}(\sqrt[3]{2}) = \{a + b2^{1/3} + c2^{2/3} : a, b, c \in \mathbb{Q}\}$

(iii) Let $p \in \mathbb{Z}$ be a prime number and $\zeta_p := e^{2\pi i/p} \in \mathbb{C}$, then

$$[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = \deg(\Phi_p) = p - 1$$

2.4. (Tower Law) If $k \subset F$ and $F \subset L$ are two field extensions, then

$$[L : k] = [L : F][F : k]$$

Proof. Suppose $[F : k]$ is infinite, then $[L : k]$ is infinite. Similarly, if $[L : F]$ is infinite, so is $[L : k]$. Hence, we may assume that the RHS is finite. Suppose

$$S_1 := \{x_1, x_2, \ldots, x_n\}$$

is a k-basis for F, and

$$S_2 := \{y_1, y_2, \ldots, y_m\}$$

is an F-basis for L. We want to show that

$$S := \{x_i y_j : 1 \leq i \leq n, 1 \leq j \leq m\}$$

has nm elements and is a k-basis for L.

(i) S has nm elements : Suppose not, then $x_{i_1} y_{j_1} = x_{i_2} y_{j_2}$. If $y_{j_1} = y_{j_2}$, then $x_{i_1} = x_{i_2}$ and we are done. If not, then

$$x_{i_1} y_{j_1} - x_{i_2} y_{j_2} = 0$$

But $\{y_{j_1}, y_{j_2}\}$ is F-linearly independent, so $x_{i_1} = x_{i_2} = 0$. This contradicts the k-linear independence of $\{x_{i_1}\}$.

(ii) S spans L over k: Suppose $\beta \in L$, then $\exists a_1, a_2, \ldots, a_m \in F$ such that

$$\beta = \sum_{i=1}^{m} a_j y_j$$

But $a_j \in F$ implies that $\exists \alpha_{i,j} \in k$ such that

$$a_j = \sum_{i=1}^{n} \alpha_{i,j} x_i$$

Hence, $\beta = \sum_{i,j} \alpha_{i,j} x_i y_j$

(iii) S is k-linearly independent in L: Suppose $\exists \alpha_{i,j} \in k$ such that

$$\sum_{i,j} \alpha_{i,j} x_i y_j = 0$$

Collect the coefficient of y_j into a_j and write $\sum_{j=1}^{m} a_j y_j = 0$ where $a_j \in F$. However this would imply that $a_j = 0$ for all j. Again, the k-linear independence of $\{x_i\}$ implies that $\alpha_{i,j} = 0$ for all i, j.

□

2.5. Example: Let $f(x) = x^3 + 6x + 2 \in \mathbb{Q}[x]$. Then f is irreducible over $\mathbb{Q}(\sqrt[4]{2})$

Proof. Suppose not, then by Exercise 1.1, f must have a root $\alpha \in \mathbb{Q}(\sqrt[4]{2})$. Hence, we have a tower

$$\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{Q}(\sqrt[4]{2})$$

However, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(m_\alpha)$. But f is irreducible over $\mathbb{Q}$ by Eisenstein, so it must be the minimal polynomial of α. Hence, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, which, by the Tower Law, would imply that $3 \mid 4$. This is a contradiction. □

2.6. Corollary: Let $k \subset F_1$ and $k \subset F_2$ be field extensions (all contained in $\mathbb{C}$). Let L denote the smallest field containing both F_1 and F_2. Then

(i) $[L : F_2] \leq [F_1 : k]$

(ii) $[L : k] \leq [F_1 : k][F_2 : k]$

L is called the compositum of F_1 and F_2 and is denoted by F_1F_2

Proof. (i) Again, assume $[F_1 : k]$ and $[F_2 : k]$ are finite. Suppose $S := \{x_1, x_2, \ldots, x_n\}$ is a k-basis for F_2 which contains 1. Claim:

$$L = \mathrm{Span}_{F_1}(S) = \{\sum_{i=1}^{n} a_i x_i : a_i \in F_1\}$$

Let $F_3 = \mathrm{Span}_{F_1}(S)$

(a) $F_3 \subset L$ since $F_1 \subset L$ and $S \subset L$ and L is a field.

(b) $F_1 \subset F_3$ since $1 \in S$

(c) $F_2 \subset F_3$ since $F_2 = \mathrm{Span}_k(S)$ and $k \subset F_1$

(d) F_3 is a field:

A. F_3 is clearly closed under addition since it is a vector space.

B. If $x = \sum_{i=1}^{n} \alpha_i x_i$ and $y = \sum_{j=1}^{n} \beta_j x_j$ with $\alpha_i, \beta_j \in F_1$, then

$$xy = \sum_{i,j} \alpha_i \beta_j x_i x_j$$

Now, $x_i x_j \in F_2 = \mathrm{Span}_k(S)$. Since $k \subset F_1$ it follows that,

$$xy \in \mathrm{Span}_{F_1}(S)$$

C. If $0 \neq x = \sum_{i=1}^{n} \alpha_i x_i \in F_3$. Then consider the map

$$T : F_3 \to F_3 \text{ given by } y \mapsto xy$$

Then T is clearly F_1-linear, and is injective (why?). Since $[F_3 : F_1] < \infty$, it follows that T is surjective. Hence, $\exists y \in F_3$ such that $xy = 1$.

(e) Since F_3 is a field and F_1 and F_2 are contained in F_3, it follows that $L \subset F_3$. By part (a), we have that

$$L = F_3 = \mathrm{Span}_{F_1}(S)$$

Hence

$$[L : F_2] \leq |S| = [F_1 : k]$$

(ii) Part (ii) follows from (i) and the fact that $[L : k] = [L : F_2][F_2 : k]$

□

2.7. Definition: A field extension $k \subset L$ is said to be algebraic if every $\alpha \in L$ is algebraic over k.

2.8. Theorem:

(i) If $k \subset L$ is finite extension, then it is algebraic.

(ii) If $\alpha \in L$ is algebraic over k, then $k \subset k(\alpha)$ is algebraic.

Proof. (i) Suppose $k \subset L$ is a finite extension of degree n. Let $\alpha \in L$, then the set

$$S = \{1, \alpha, \alpha^2, \ldots, \alpha^n\}$$

has $n+1$ elements and so it must be k-linearly dependent. Hence, $\exists a_0, a_1, \ldots, a_n \in k$ not all zero such that

$$\sum_{i=0}^{n} a_i \alpha^i = 0$$

and so α satisfies the non-zero polynomial $f(x) = \sum_{i=0}^{n} a_i x^i \in k[x]$

(ii) Follows from part (i) and Theorem 2.1

□

2.9. Definition: An extension $k \subset L$ is said to be finitely generated if $\exists \alpha_1, \alpha_2, \ldots \alpha_n \in L$ such that

$$L = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$$

In other words, L is the smallest field containing k and the set $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$.

2.10. Theorem: $k \subset L$ is a finite extension iff it is algebraic and finitely generated.

Proof. (i) Suppose $k \subset L$ is a finite extension, then let S be a k-basis for L. Then

$$L = k(S)$$

and so $k \subset L$ is finitely generated. Also, by Theorem 3.2, $k \subset L$ is algebraic.

(ii) Suppose $k \subset L$ is finitely generated and algebraic, then $\exists \{\alpha_1, \alpha_2, \ldots, \alpha_n\} \subset \mathbb{C}$ such that

$$L = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$$

By hypothesis, α_i is algebraic over k, and so

$$[k(\alpha_i) : k] < \infty$$

By Theorem 2.6(ii) and induction, it follows that

$$[L : k] \leq \prod_{i=1}^{n} [k(\alpha_i) : k] < \infty$$

Hence, $k \subset L$ is finite extension.

□

2.11. Example: Let $k \subset \mathbb{C}$ be a field and set

$$F = \{\alpha \in \mathbb{C} : \alpha \text{ is algebraic over } k\}$$

Then

(i) F is a field

(ii) $k \subset F$ is an algebraic extension

(iii) If $k = \mathbb{Q}$, then $k \subset F$ is infinite

2.12. Theorem: Let $k \subset \mathbb{C}$ be any field and set F to be the field of numbers that are algebraic over k. For every non-constant $f \in F[x], \exists \alpha \in F$ such that $f(\alpha) = 0$.

Proof. Suppose $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in F[x]$ is a non-constant polynomial, then $\exists \alpha \in \mathbb{C}$ such that $f(\alpha) = 0$. But then, α is algebraic over F. We want to show that α is algebraic over k. So consider

$$F_0 = k(a_0, a_1, \ldots, a_n)$$

Each $a_i \in F$, so a_i is algebraic over k. By Theorem 2.10

$$[F_0 : k] < \infty$$

Also, α is algebraic over F_0. So by Theorem 2.2,

$$[F_0(\alpha) : F_0] < \infty$$

So by the Tower Law

$$[F_0(\alpha) : k] < \infty$$

which implies that α is algebraic over k by Theorem 2.1. Hence, $\alpha \in F$ by definition. □

2.13. Remark:

(i) We say that F is algebraically closed.

(ii) F is the smallest field that contains k and is algebraically closed (Why?)

(iii) F is called the algebraic closure of k, and is denoted by $\overline{k}$

(iv) If k is any field (even a finite field), we can construct a field L such that

(a) $k \subset L$ is algebraic

(b) L is algebraically closed

(c) If $k \subset M$ is any field extension satisfying the above two properties, then $\exists$ an injective homomorphism $\sigma : L \to M$.

In other words, L is unique upto isomorphism. This field L is called the algebraic closure of k, and is denoted by $\overline{k}$

Exercises

2.1. Prove that

(i) $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$

(ii) $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$

2.2. If $k \subset L$ is a finite extension such that $[L : k]$ is prime, then

(i) If F is a field such that $k \subset F \subset L$, then prove that either $F = k$ or $F = L$

(ii) Prove that $\exists \alpha \in L$ such that $L = k(\alpha)$ (ie. $k \subset L$ is a simple extension)

2.3. Suppose $k \subset F_1$ and $k \subset F_2$ are two field extensions whose degrees are relatively prime. Then prove that

$$[F_1F_2 : k] = [F_1 : k][F_2 : k]$$

2.4. Let $p \in \mathbb{Z}$ be prime and let $\zeta_p := e^{2\pi i/p}$. Determine $[\mathbb{Q}(2^{1/p}, \zeta_p) : \mathbb{Q}]$

2.5. Let $k \subset \mathbb{C}$ be a field and $\alpha \in \mathbb{C}$ be algebraic over k, and suppose $\varphi : k(\alpha) \to \mathbb{C}$ is a field homomorphism such that $\varphi \mid_k = \mathrm{id}_k$. Let

$$\beta := \varphi(\alpha)$$

Then prove that

(i) For any $f \in k[x]$,

$$\varphi(f(\alpha)) = f(\beta)$$

(ii) β is algebraic over k

(iii) β and α have the same minimal polynomial over k.

2.6. Use the previous problem and Corollary 1.10 to answer the following question: If $\alpha \in \mathbb{C}$ is algebraic over $\mathbb{Q}$, determine the number of homomorphisms

$$\varphi : \mathbb{Q}(\alpha) \to \mathbb{C}$$

2.7. For each $n \in \mathbb{N}$, define

$$A_n := \{f \in \mathbb{Q}[x] : \deg(f) \leq n\}$$

$$B_n := \bigcup_{f \in A_n} \{\alpha \in \mathbb{C} : f(\alpha) = 0\}$$

(i) Prove that A_n is countable.

(ii) Prove that B_n is countable.

(iii) Prove that $\overline{\mathbb{Q}}$ is countable.

Conclude that there exist real numbers that are transcendental.

3. The Galois Group

3.1. Recall: Let $k \subset \mathbb{C}$ be a field, $\alpha \in \mathbb{C}$ algebraic over k

(i) If $k \subset k(\alpha)$ is a finite extension, and

$$k(\alpha) = \left\{ \sum_{i=0}^{n-1} a_i \alpha^i : a_i \in k \right\}$$

where $n = \deg(m_\alpha)$

(ii) If $\varphi : k(\alpha) \to \mathbb{C}$ is a homomorphism such that $\varphi \mid_k = \mathrm{id}_k$, then

$$\varphi(\sum_{i=0}^{n-1} a_i \alpha^i) = \sum_{i=0}^{n-1} a_i \varphi(\alpha)^i$$

So, φ is completely determined by the complex number $\varphi(\alpha)$. By Exercise 2.5, $\varphi(\alpha)$ must be a root of the minimial polynomial m_α of α. Hence, if

$$S = \{k\text{-homomorphisms } \varphi : k(\alpha) \to \mathbb{C}\}, \text{ and}$$
$$T = \{\text{roots of } m_\alpha \text{ in } \mathbb{C}\}$$

Then we have a map $\mu : S \to T$ given by

$$\varphi \mapsto \varphi(\alpha)$$

We have shown above that this function μ is injective.

(iii) By Corollary 1.10, if $\beta \in T$, then $\exists$ an isomorphism $k(\alpha) \cong_k k(\beta)$. In particular, we get a k-homomorphism $\varphi : k(\alpha) \to \mathbb{C}$ such that $\varphi(\alpha) = \beta$. This proves that μ is surjective. Hence,

$$|\{k\text{-homomorphisms } \varphi : k(\alpha) \to \mathbb{C}\}| = |\{\text{roots of } m_\alpha \text{ in } \mathbb{C}\}|$$

3.2. Examples: List all homomorphisms from $k \to \mathbb{C}$:

(i) $k = \mathbb{Q}$: By Exercise 1.6, there is only one map, the inclusion

(ii) $k = \mathbb{Q}(\sqrt{2})$: By Exercise 1.7, there are two maps given by

$$\sigma_1 : \sqrt{2} \mapsto \sqrt{2}$$
$$\sigma_2 : \sqrt{2} \mapsto -\sqrt{2}$$

(iii) $k = \mathbb{Q}(\omega)$: There are two maps given by

$$\sigma_1 : \omega \mapsto \omega$$
$$\sigma_2 : \omega \mapsto \omega^2$$

(iv) $k = \mathbb{Q}(\sqrt[3]{2})$: There are three maps given by

$$\begin{aligned}\sigma_1 &: \sqrt[3]{2} \mapsto \sqrt[3]{2}\\ \sigma_2 &: \sqrt[3]{2} \mapsto \omega\sqrt[3]{2}\\ \sigma_3 &: \sqrt[3]{2} \mapsto \omega^2\sqrt[3]{2}\end{aligned}$$

(v) $k = \mathbb{Q}(\sqrt{2}, \sqrt{3})$: There are atmost 4 maps given by

$$\begin{aligned}\sigma_1 &= \mathrm{id}\\ \sigma_2 &= \sqrt{2} \mapsto -\sqrt{2} \text{ and } \sqrt{3} \mapsto \sqrt{3}\\ \sigma_3 &= \sqrt{2} \mapsto \sqrt{2} \text{ and } \sqrt{3} \mapsto -\sqrt{3}\\ \sigma_4 &= \sqrt{2} \mapsto -\sqrt{2} \text{ and } \sqrt{3} \mapsto -\sqrt{3}\end{aligned}$$

(vi) $k = \mathbb{Q}(\sqrt[3]{2}, \omega)$: There are atmost 6 maps given by

$$\begin{aligned}\sigma_1 &= \mathrm{id}_L\\ \sigma_2 &= \sqrt[3]{2} \mapsto \sqrt[3]{2} \text{ and } \omega \mapsto \omega^2\\ \sigma_3 &= \sqrt[3]{2} \mapsto \omega\sqrt[3]{2} \text{ and } \omega \mapsto \omega\\ \sigma_4 &= \sqrt[3]{2} \mapsto \omega\sqrt[3]{2} \text{ and } \omega \mapsto \omega^2\\ \sigma_5 &= \sqrt[3]{2} \mapsto \omega^2\sqrt[3]{2} \text{ and } \omega \mapsto \omega\\ \sigma_6 &= \sqrt[3]{2} \mapsto \omega^2\sqrt[3]{2} \text{ and } \omega \mapsto \omega^2\end{aligned}$$

3.3. Theorem: Let $f \in k[x]$ be a monic irreducible polynomial, then all the roots of f in $\mathbb{C}$ are distinct (ie. f does not have any multiple roots. We say that such a polynomial is <u>separable</u>)

Proof. Suppose $\beta \in \mathbb{C}$ is a multiple root of f, then $(x-\beta)^2 \mid f$ in $\mathbb{C}[x]$. Hence, $f'(\beta) = 0$, whence $f \mid f'$ in $k[x]$ (since f must be the minimal polynomial of β over k). However, $\deg(f') < \deg(f)$, so this is impossible. □

3.4. (Primitive Element Theorem): Let $k \subset L$ be a finite extension of subfields of $\mathbb{C}$, then it is a simple extension. ie. $\exists \theta \in L$ such that $L = k(\theta)$

3.5. Corollary: Let $k \subset L$ be a finite extension of subfields of $\mathbb{C}$, then

$$\text{the number of } k\text{-homomorphisms } \varphi : L \to \mathbb{C} = [L : k]$$

3.6. Definition: A field extension $k \subset L$ is said to be <u>normal</u> if every k-homomorphism $\varphi : L \to \mathbb{C}$ maps L into itself.

3.7. Lemma: If $k \subset L$ is a finite normal extension, then, for any k-homomorphism $\varphi : L \to \mathbb{C}$, $\varphi : L \to L$ is bijective.

Proof. Since $k \subset L$ is normal, $\varphi(L) \subset L$. Hence we may consider

$$\varphi : L \to L$$

Note that φ is a k-linear transformation, and it is injective since it is a homomorphism of fields. Since $[L : k] < \infty$, it must be surjective. □

3.8. Definition:

(i) A field extension that is both finite and normal is called a Galois extension.

(ii) If $k \subset L$ is a Galois extension, then we define the Galois group of the extension as

$$\mathrm{Gal}_k(L) = \{k\text{-homomorphisms } \varphi : L \to \mathbb{C}\}$$

Note: $\mathrm{Gal}_k(L)$ is a group under composition.

3.9. Examples:

(i) $\mathrm{Gal}_k(k) = \{\mathrm{id}_k\}$

(ii) $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2})) \cong \mathbb{Z}_2$

(iii) $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\omega)) \cong \mathbb{Z}_2$

(iv) $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}, \sqrt{3})) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

Proof. Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. By Example 3.2, we have atmost 4 maps $\varphi : L \to \mathbb{C}$. By Corollary 3.5, there are exactly 4 maps, so these must be all of them. For each of these maps, $\varphi(\sqrt{2})$ and $\varphi(\sqrt{3})$ belong to $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Hence, by Lemma 3.7, they must be bijective as well. Hence,

$$\mathrm{Gal}_k(L) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$$

Since it is a group of order 4, $\mathrm{Gal}_k(L) \cong \mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$. However,

$$\sigma_i^2 = \mathrm{id}_L \quad \forall i$$

Hence, $\mathrm{Gal}_k(L) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ □

(v) $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}, \omega)) \cong S_3$

Proof. Let $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$. Again, there are exactly 6 homomorphisms $\varphi : L \to \mathbb{C}$ in Example 3.2. Also, for each of these homomorphisms $\varphi(\sqrt[3]{2})$ and $\varphi(\omega)$ belong to L. Hence by Lemma 3.7,

$$\mathrm{Gal}_k(L) = \{\sigma_i : 1 \leq i \leq 6\}$$

It is a group of order 6, so $\mathrm{Gal}_k(L) \cong \mathbb{Z}_6$ or S_3. However,

$$\sigma_3\sigma_2(\sqrt[3]{2}) \neq \sigma_2\sigma_3(\sqrt[3]{2})$$

Hence, $\mathrm{Gal}_k(L)$ is non-abelian, which forces it to be S_3 □

3.10. Lemma: Let $k \subset L$ be a finite normal extension. If F is an intermediate field

$$k \subset F \subset L$$

Then $F \subset L$ is a finite normal extension.

Proof. (i) Clearly, $[L : F] \leq [L : k] < \infty$

(ii) If $\varphi : L \to \mathbb{C}$ is an F-homomorphism, then φ is also a k-homomorphism. Since $k \subset L$ is normal, $\varphi(L) \subset L$.

□

3.11. Definition: Let $k \subset L$ be a field extension and $G := \mathrm{Gal}_k(L)$

(i) If $k \subset F \subset L$ is an intermediate field, then

$$\mathrm{Gal}_F(L) < \mathrm{Gal}_k(L)$$

(ii) If $H < G$, then

$$L^H := \{x \in L : \varphi(x) = x \quad \forall \varphi \in H\} \subset L$$

is called the fixed field of H

Note: L^H is a subfield of L containing k.

(iii) We set

$$\begin{aligned} \mathcal{F} := \{\text{intermediate fields } k \subset F \subset L\} \qquad & \mathcal{G} := \{\text{subgroups } H < G\} \\ \Phi : \mathcal{F} \to \mathcal{G} \qquad & \Psi : \mathcal{G} \to \mathcal{F} \\ F \mapsto \mathrm{Gal}_F(L) \qquad & H \mapsto L^H \end{aligned}$$

3.12. Examples:

(i) If $k \subset L$ is any field extension, and $G = \mathrm{Gal}_k(L)$

(a) If $H = \{e\} < G$, then $L^H = L$

However, L^G may not be equal to k (See below)

(b) If $F = L$, then $\mathrm{Gal}_F(L) = \{e\}$

If $F = k$, then $\mathrm{Gal}_k(L) = G$

(ii) If $k = \mathbb{Q}, L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, then

(a) If $H = \langle \sigma_3 \rangle$ where

$$\sigma_3 : \sqrt{2} \mapsto \sqrt{2} \text{ and } \sqrt{3} \mapsto -\sqrt{3}$$

Then $L^H = \mathbb{Q}(\sqrt{2})$ and $\mathrm{Gal}_{\mathbb{Q}(\sqrt{2})}(L) = H$

(b) If $H = \langle \sigma_4 \rangle$ where

$$\sigma_4 : \sqrt{2} \mapsto -\sqrt{2} \text{ and } \sqrt{3} \mapsto -\sqrt{3}$$

Then $L^H = \mathbb{Q}(\sqrt{6})$

(iii) If $k = \mathbb{Q}, L = \mathbb{Q}(\sqrt[3]{2}, \omega)$, then

(a) If $H = \langle \sigma_2 \rangle$ where

$$\sigma_2 : \sqrt[3]{2} \mapsto \sqrt[3]{2} \text{ and } \omega \mapsto \omega^2$$

Then $L^H = \mathbb{Q}(\sqrt[3]{2})$. Also, $\mathrm{Gal}_{\mathbb{Q}(\sqrt[3]{2})}(L) = H$. Note that $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ is not normal.

3.13. (Fundamental Theorem of Galois Theory - I): Let $k \subset L$ be a Galois extension of subfields of $\mathbb{C}$ with Galois group G. Then

(i) Ψ and Φ are mutual inverses. So there is a one-to-one correspondence

$$\mathcal{F} \leftrightarrow \mathcal{G}$$

(ii) If $F \in \mathcal{F}$ is an intermediate field, then

$$[F : k] = [\mathrm{Gal}_k(L) : \mathrm{Gal}_F(L)]$$

We visualize this by tower diagrams

$$\begin{array}{cc} L & \mathrm{Gal}_k(L) \\ | & \downarrow = \\ F & \mathrm{Gal}_F(L) \\ \downarrow = & | \\ k & \{e\} \end{array}$$

3.14. (Fundamental Theorem of Galois Theory - II): Let $k \subset L$ be a Galois extension of subfields of $\mathbb{C}$ with Galois group G. Then

(i) If $F \in \mathcal{F}$, $k \subset F$ is normal iff $\mathrm{Gal}_F(L) \lhd \mathrm{Gal}_k(L)$.

(ii) In that case, the restriction map

$$\pi : \mathrm{Gal}_k(L) \to \mathrm{Gal}_k(F)$$

is a well-defined, surjective, group homomorphism.

(iii) $\ker(\pi) = \mathrm{Gal}_F(L)$

(iv) Hence,

$$\mathrm{Gal}_k(L)/\mathrm{Gal}_F(L) \cong \mathrm{Gal}_k(F)$$

Exercises

3.1. If $k \subset L$ is a Galois extension with Galois group G.

(i) If F is an intermediate field ($k \subset F \subset L$), then prove that $\mathrm{Gal}_F(L) < G$

(ii) If $H < G$, then prove that L^H is a field such that $k \subset L^H \subset L$.

3.2. Let $k \subset L$ be a Galois extension with Galois group G

(i) If F_1 and F_2 are intermediate fields such that $F_1 \subset F_2$, then prove that $\mathrm{Gal}_{F_2}(L) \subset \mathrm{Gal}_{F_1}(L)$

(ii) If H_1 and H_2 are subgroups of G such that $H_1 \subset H_2$, then prove that $L^{H_2} \subset L^{H_1}$

3.3. Let $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$, and $G = \mathrm{Gal}_{\mathbb{Q}}(L)$. Let $F = \mathbb{Q}(\sqrt[3]{2})$ and $H = \mathrm{Gal}_F(L)$

(i) List all the elements of H from Example 3.2(vi)

(ii) Prove that H is not normal in G.

3.4. Let $L = \mathbb{Q}(\sqrt{3}, \sqrt{2})$ and let $G = \mathrm{Gal}_{\mathbb{Q}}(L)$

(i) Determine all the subgroups of G

(ii) For each subgroup H from part (i), determine L^H (Use Theorem 3.13(ii))

3.5. Let $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$ and $G = \mathrm{Gal}_{\mathbb{Q}}(L)$.

(i) List all the subgroups of G from Example 3.2(vi)

(ii) For each subgroup H from part (i), determine L^H (Use Theorem 3.13(ii))

3.6. Let $L = \mathbb{Q}(\sqrt[4]{2}, i)$.

(i) Prove that $\mathbb{Q} \subset L$ is a normal extension of degree 8.

(ii) Prove that $\mathrm{Gal}_{\mathbb{Q}}(L)$ has a subgroup H which is not normal.

Note: There is only one group of order 8 which satisfies (ii). This is the dihedral group of order 8, usually denoted by D_4 or D_8.

3.7. Let $n \in \mathbb{N}$, $\zeta_n = e^{2\pi i/n}$ and $L = \mathbb{Q}(\zeta_n)$.

(i) Prove that $\mathbb{Q} \subset L$ is a finite extension of degree $\leq n-1$.

(ii) If $\varphi : L \to \mathbb{C}$ is a homomorphism, then prove that $\exists 1 \leq i \leq n-1$ such that

$$\varphi(\zeta_n) = \zeta_n^i$$

Conclude that $\mathbb{Q} \subset L$ is a normal extension

(iii) Use part (ii) to prove that $\mathrm{Gal}_{\mathbb{Q}}(L)$ is an abelian group.

3.8. Read Theorem 3.14 before attempting this problem: Let $k \subset L$ be a finite normal extension whose Galois group is abelian.

(i) If F is an intermediate field, $k \subset F \subset L$, then prove that $k \subset F$ is a normal extension. (Compare this with Exercise 3.1)

(ii) Prove that $\mathrm{Gal}_k(F)$ is an abelian group.

4. Finite Fields

Note: All fields in this section will be finite of characteristic $p > 0$.

4.1. Remark: If L is a finite field of characteristic $p > 0$, then

(i) $\mathbb{F}_p \hookrightarrow L$. Hence, $|L| = p^n$ for some $n \geq 1$

(ii) We may construct an algebraically closed field, $\overline{\mathbb{F}_p}$ which will play the role that $\mathbb{C}$ played in the earlier discission.

(iii) Note that the only homomorphism $\varphi : \mathbb{F}_p \to \overline{\mathbb{F}_p}$ is the inclusion map, so $\mathbb{F}_p$ will play the role that $\mathbb{Q}$ played in the earlier discussion.

(iv) As before, if k is a finite field and $\alpha \in \overline{\mathbb{F}_p}$, then there is a 1-1 correspondence

$$\{k\text{-homomorphisms } \varphi : k(\alpha) \to \overline{\mathbb{F}_p}\} \leftrightarrow \{\text{roots of } m_\alpha \text{ in } \overline{\mathbb{F}_p}\}$$

(Exercise 2.5 and Corollary 1.10 hold for finite fields without any change in the proof)

4.2. Theorem: If k is a finite field and $f \in k[x]$ is irreducible, then it is separable. (ie. It has no multiple roots in $\overline{\mathbb{F}_p}$)

4.3. Corollary: If k is a finite field and $\alpha \in \overline{\mathbb{F}_p}$, then

$$|\{k\text{-homomorphisms } \varphi : k(\alpha) \to \overline{\mathbb{F}_p}\}| = [k(\alpha) : k]$$

4.4. Theorem: If L is a finite field, then L^* is cyclic (as a multiplicative group)

Proof. By the Fundamental theorem of finite abelian groups, we can write

$$L^* \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \ldots \times \mathbb{Z}_{d_m}$$

such that $d_1 \mid d_2 \mid \ldots \mid d_m$. Let $n = d_m$, then for any $\alpha \in L^*$, we have

$$\alpha^n = 1$$

Hence, α is a root of the polynomial $x^n - 1 \in L[x]$ which has atmost n roots. Hence,

$$d_1 d_2 \ldots d_m = |L^*| \leq n = d_m$$

Hence, $m = 1$ and $L^* \cong \mathbb{Z}_n$ is cyclic. □

4.5. Corollary: If $k \subset L$ is a finite field extension of finite fields, then $k \subset L$ is simple.

Proof. The primitive element may be chosen to be any generator of L^* □

4.6. Corollary: If $k \subset L$ is a finite extension of finite fields, then

$$\text{the number of } k\text{-homomorphisms } \varphi : L \to \overline{\mathbb{F}_p} = [L : k]$$

Proof. Write $L = k(\alpha)$ by Corollary 4.3. Now, as in 3.1,

$$|\{k\text{-homomorphisms } \varphi : L \to \overline{\mathbb{F}_p}\}| = |\{ \text{ roots of } m_\alpha \text{ in } \overline{\mathbb{F}_p}\}|$$

But m_α is separable, so the RHS is $\deg(m_\alpha) = [L : k]$ □

4.7. Theorem: If L is a finite field of characteristic $p > 0$ and cardinality p^n, then

$$L = \{\alpha \in \overline{\mathbb{F}_p} : \alpha^{p^n} = \alpha\}$$

Proof. Let S be the set in the RHS, then S is the set of roots of the polynomial $x^{p^n} - x \in \overline{\mathbb{F}_p}[x]$. Hence,

$$|S| \leq p^n$$

Since $|L| = p^n$, it suffices to prove that $L \subset S$. Now if $\alpha \in L$, then we may assume $\alpha \neq 0$. Now $\alpha \in L^*$, which is a group of order $p^n - 1$. So

$$\alpha^{p^n - 1} = 1 \Rightarrow \alpha^{p^n} = \alpha$$

Hence, $\alpha \in S$, which proves the $L \subset S$ and completes the proof. □

4.8. Corollary: For any prime $p \in \mathbb{N}$ and any $n \in \mathbb{N}$, there is a unique field of cardinality p^n. We denote this field by

$$\mathbb{F}_{p^n}$$

4.9. Definition: As before, we make the following definitions :

(i) A field extension $k \subset L$ of finite fields is called <u>normal</u> if, for every k-homomorphism $\varphi : L \to \overline{\mathbb{F}_p}$, we have $\varphi(L) \subset L$.

(ii) If $k \subset L$ is such an extension, we write

$$\mathrm{Gal}_k(L) = \{k\text{-homomorphisms } \varphi : L \to \overline{\mathbb{F}_p}\}$$

Note: As before, If $k \subset L$ is a finite normal extension, $\mathrm{Gal}_k(L)$ is a group.

4.10. Theorem: If $k \subset L$ is a finite extension of finite fields, then it is normal.

Proof. Suppose $\varphi : L \to \overline{\mathbb{F}_p}$ is a k-homomorphism, and $\beta \in L$, then we want to show that $\varphi(\beta) \in L$. By Theorem 4.7,

$$\beta^{p^n} = \beta \Rightarrow \varphi(\beta)^{p^n} = \varphi(\beta)$$

Hence, $\varphi(\beta) \in \{\alpha \in \overline{\mathbb{F}_p} : \alpha^{p^n} = \alpha\} = L$ □

4.11. Lemma: If L is a field of characteristic $p > 0$, then the map $F : L \to L$ defined by $x \mapsto x^p$ is a homomorphism, called the <u>Frobenius map</u>.

Proof. (i) F is a map from L to $\overline{\mathbb{F}_p}$, but $\mathbb{F}_p \subset L$ is a normal extension by 4.10, so $F(L) = L$.

(ii) F is clearly multiplicative

(iii) We only need to check that if $\alpha, \beta \in L$, then $(\alpha+\beta)^p = \alpha^p + \beta^p$. However, this follows by the binomial theorem and the fact that

$$p \mid \binom{p}{k} \quad \forall 1 \leq k \leq p-1$$

□

4.12. Theorem: Let $L = \mathbb{F}_{p^n}$, then $\mathrm{Gal}_{\mathbb{F}_p}(L)$ is a cyclic group of order n generated by F

Proof. We know that $F : L \to L$ is a homomorphism, and every homomorphism fixes $\mathbb{F}_p$, so $F \in \mathrm{Gal}_{\mathbb{F}_p}(L)$. Also,

$$|\operatorname{Gal}_{\mathbb{F}_p}(L)| = [L : \mathbb{F}_p] = n$$

So it suffices to prove that $o(F) = n$.

(i) For any $\alpha \in L$,

$$F^n(\alpha) = \alpha^{p^n} = \alpha \Rightarrow o(F) \leq n$$

(ii) Suppose $o(F) = s \leq n$, then $F^s = \mathrm{id}_L$. Then for any $\alpha \in L$,

$$\alpha^{p^s} = \alpha \Rightarrow \alpha \text{ is a root of } x^{p^s} - x$$

Hence,

$$|L| \leq |\{\text{roots of } x^{p^s} - x \text{ in } \overline{\mathbb{F}_p}\}| \leq p^s$$

But $|L| = p^n$, so $n \leq s$, which proves the theorem.

□

4.13. Corollary: If $k \subset L$ is a finite extension of finite fields of characteristic $p > 0$, then $\mathrm{Gal}_k(L)$ is a cyclic group genered by F^j where $j = [k : \mathbb{F}_p]$

Proof. Let $G = \mathrm{Gal}_k(L)$, then $G < \mathrm{Gal}_{\mathbb{F}_p}(L)$, which is a cyclic group generated by F. Hence, $G = \langle F^j \rangle$ for some $1 \leq j \neq n$. Now

$$o(F^j) = |G| = [L : k]$$

Hence, by the Tower Law

$$j = \frac{|\operatorname{Gal}_{\mathbb{F}_p}(L)|}{|G|} = \frac{[L : \mathbb{F}_p]}{[L : k]} = [k : \mathbb{F}_p]$$

□

Exercises

4.1. Let $L = \mathbb{F}_3[x]/(x^2+1)$.

(i) Prove that L is a field of cardinality 9.

(ii) List down all the elements of L

4.2. Let $f(x) = x^3 - 2 \in \mathbb{F}_7[x]$ and $L = \mathbb{F}_7[x]/(f)$

(i) Prove that L is a field of cardinality 7^3

(ii) Determine which elements of L are the roots of f. [*Hint:* $2^3 = 1$ in $\mathbb{F}_7$]

4.3. Construct a field with 4 elements.

4.4. Let k be a finite field and $f \in k[x]$ be an irreducible polynomial.

(i) Prove that $\exists n \in \mathbb{N}$ such that $f \mid (x^{p^n} - x)$ in $k[x]$

[*Hint:* Use Theorem 4.7 on the field $k[x]/(f)$]

(ii) Conclude that f is separable. (This proves Theorem 4.2)

4.5. Fix $n \in \mathbb{N}$ and let

$$L = \{\alpha \in \overline{\mathbb{F}_p} : \alpha^{p^n} = \alpha\}$$

(i) If $d \mid n$, then prove that

$$k = \{\alpha \in \overline{\mathbb{F}_p} : \alpha^{p^d} = \alpha\}$$

is a subfield of L

(ii) Conversely, if $k \subset L$ is a subfield of L, then prove that $\exists d \mid n$ such that k is given as in part (i).

[*Hint:* Consider the tower $\mathbb{F}_p \subset k \subset L$]

(iii) If k is as in part (i), determine $\mathrm{Gal}_k(L)$

4.6. Let L be a finite field. Prove that there is a 1-1 correspondence

$$\{\text{subfields of } L\} \leftrightarrow \{\text{subgroups of } \mathrm{Gal}_{\mathbb{F}_p}(L)\}$$

Note: This proves Theorem 3.13 in the case of finite fields. Theorem 3.14 is not needed since all finite extensions of finite fields are normal.

4.7. Let $k \subset F_1$ and $k \subset F_2$ be Galois extensions of subfields of $\mathbb{C}$. Prove that $k \subset F_1 \cap F_2$ is a Galois extension.

4.8. Let $k \subset F_1$ and $k \subset F_2$ be Galois extensions of subfields of $\mathbb{C}$. Let $L = F_1F_2$, and prove that

(i) $k \subset L$ is a Galois extension (Use the primitive element theorem)

(ii) Define a function

$$\mu : \mathrm{Gal}_k(L) \to \mathrm{Gal}_k(F_1) \times \mathrm{Gal}_k(F_2)$$

by

$$\varphi \mapsto (\varphi\,|_{F_1}, \varphi\,|_{F_2})$$

Prove that μ is well-defined and injective.

5. Cyclotomic Extensions

5.1. Definition: Fix $n \in \mathbb{N}$

(i) $\zeta_n = e^{2\pi i/n}$

(ii) $\mu_n = \{e^{2\pi ik/n} : 0 \leq k \leq n-1\} = \langle \zeta_n \rangle$.

Note: μ_n is a cyclic group of order n.

(iii) Elements of μ_n are called roots of unity. Generators of μ_n are called primitive n^{th} roots of unity.

(iv) $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\mu_n)$ is called the n^{th} cyclotomic field.

Note: $\mathbb{Q} \subset \mathbb{Q}(\mu_n)$ is a normal extension.

(v) If G is a group, then $\mathrm{Aut}(G) = \{\varphi : G \to G : \varphi \text{ is an isomorphism}\}$.

5.2. Theorem: Let $k \subset \mathbb{C}$ be any field, then

(i) $k \subset k(\zeta_n)$ is a finite normal extension.

(ii) The map

$$\Gamma : \mathrm{Gal}_k(k(\zeta_n)) \to \mathrm{Aut}(\mu_n)$$

given by

$$\varphi \mapsto \varphi|_{\mu_n}$$

is a well-defined injective homomorphism.

Proof. (a) If $\varphi \in \mathrm{Gal}_k(k(\zeta_n))$, we want to show that $\varphi|_{\mu_n} \in \mathrm{Aut}(\mu_n)$.

A. Firstly, if $\zeta \in \mu_n$, then $\varphi(\zeta)^n = 1$, so $\varphi(\zeta) \in \mu_n$

B. Now, $\varphi|_{\mu_n}$ is clearly a homomorphism from μ_n to itself.

C. Since φ is injective, $\varphi|_{\mu_n}$ is injective. Since μ_n is finite, it is also surjective.

(b) So Γ is a well-defined function. It is clearly a homomorphism since the operation on both groups is composition.

(c) If $\Gamma(\varphi) = \mathrm{id}_{\mu_n}$, then $\varphi(\zeta_n) = \zeta_n$. Since $\varphi|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$, it would follow that $\varphi = \mathrm{id}_{\mathbb{Q}(\zeta_n)}$

□

5.3. Recall:

(i) If R is a ring, $R^* = \{u \in R : \exists v \in R \text{ such that } uv = 1\}$.

(ii) R^* is a group under multiplication, called the group of units of R.

(iii) If $R = \mathbb{Z}_n$, then

$$R^* = \{\overline{a} \in \mathbb{Z}_n : (a, n) = 1\}$$

Note: $\mathbb{Z}_n^*$ is an abelian group.

5.4. Theorem: $\mathrm{Aut}(\mu_n) \cong \mathbb{Z}_n^*$

Proof. If $a \in \mathbb{Z}$ such that $(a, n) = 1$, then define

$$\sigma_a : \mu_n \to \mu_n \text{ by } \zeta_n \mapsto \zeta_n^a$$

(i) σ_a is clearly a homomorphism of μ_n

(ii) Since $(a, n) = 1, \exists s, t \in \mathbb{Z}$ such that $sa + tn = 1$. Hence,

$$\sigma_a(\zeta^s) = \zeta^{as} = \zeta^{as+tn} = \zeta$$

Hence, σ_a is surjective.

(iii) Since μ_n is finite, this means that σ_a is injective as well. So $\sigma_a \in \mathrm{Aut}(\mu_n)$.

(iv) If $a \equiv b$ in $\mathbb{Z}_n^*$, then $n \mid (b - a)$, so

$$\sigma_a(\zeta) = \zeta^a = \zeta^b = \sigma_b(\zeta)$$

Hence, $\sigma_a = \sigma_b$. So we get a well-defined map

$$\Theta : \mathbb{Z}_n^* \to \mathrm{Aut}(\mu_n) \text{ given by } \overline{a} \mapsto \sigma_a$$

(v) Θ is a homomorphism since $\sigma_{ab} = \sigma_a \circ \sigma_b$

(vi) Θ is injective: If $\sigma_a = \mathrm{id}_{\mu_n}$, then

$$\begin{aligned} \zeta^a &= \zeta \\ \Rightarrow \zeta^{a-1} &= 1 \\ \Rightarrow n &\mid (a-1) \\ \Rightarrow \overline{a} &= \overline{1} \text{ in } \mathbb{Z}_n^* \end{aligned}$$

(vii) Θ is surjective: If $\varphi : \mu_n \to \mu_n$ is an automorphism, then $\exists 1 \leq j \leq n$ such that $\varphi(\zeta) = \zeta^j$. Since φ is surjective, $\exists t \in \mathbb{N}$ such that

$$\varphi(\zeta^t) = \zeta \Rightarrow \zeta^{tj} = \zeta^1$$

Hence, $\exists s \in \mathbb{Z}$ such that $tj + sn = 1$. So $(j, n) = 1$ whence $\overline{j} \in \mathbb{Z}_n^*$ and

$$\varphi = \sigma_j = \Theta(\overline{j})$$

□

5.5. Lemma: Let $n \in \mathbb{N}$ and $\zeta \in \mu_n$ be a primitive n^{th} root of unity. ζ^a is a primitive n^{th} root of unity if and only if $(a, n) = 1$

Proof. Suppose $(a, n) = 1$, then $\exists s, t \in \mathbb{Z}$ such that $sa + tn = 1$. Hence

$$\zeta_n = \zeta_n^{sa+tn} = (\zeta_n^a)^s \in \langle \zeta_n^a \rangle$$

Hence, $\langle \zeta_n^a \rangle = \mu_n$. Conversely, if ζ_n^j is a primitive root of unity, then $\exists k \in \mathbb{N}$ such that $\zeta_n^{jk} = \zeta_n$. Hence, $n \mid (jk - 1)$ and so $(j, n) = 1$. □

5.6. Definition: n^{th} Cyclotomic polynomial is defined as

$$\Phi_n(x) = \prod(x - \zeta)$$

where the product is taken over all the primitive roots of unity. By Lemma 5.5,

$$\deg(\Phi_n) = |\mathbb{Z}_n^*|$$

5.7. Theorem: $\Phi_n \in \mathbb{Q}[x]$

Proof. Write

$$\Phi_n(x) = a_0 + a_1 x + \ldots + a_l x^l$$

If $\psi \in \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n))$ and $a \in \mathbb{Z}$ such that $(a, n) = 1$, then $\exists b \in \mathbb{Z}$ such that $(b, n) = 1$ such that

$$\psi(\zeta_n^a) = \zeta_n^{ab}$$

Since $(ab, n) = 1$, we see that ψ permutes the roots of Φ_n. Hence,

$$\psi(\Phi_n(x)) = \prod(x - \psi(\zeta)) = \prod(x - \zeta) = \Phi_n(x)$$

Hence, $\psi(a_i) = a_i$ for all i. Hence, if $G = \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n))$, we have

$$a_i \in \mathbb{Q}(\zeta_n)^G$$

By the Fundamental Theorem of Galois Theory - I, this implies that $a_i \in \mathbb{Q}$. □

5.8. Theorem: Φ_n is irreducible in $\mathbb{Q}[x]$

5.9. Corollary: $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n)) \cong \mathbb{Z}_n^*$

Proof. By 5.2 and 5.4,

$$\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n)) \cong \text{ a subgroup of } \mathbb{Z}_n^*$$

However, Φ_n is in $\mathbb{Q}[x]$, it satisfies ζ_n, and it is both irreducible and monic. Hence, Φ_n is the minimal polynomial of ζ_n over $\mathbb{Q}$, whence

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg(\Phi_n) = |\mathbb{Z}_n^*|$$

Hence, the map Γ from Theorem 5.2 must be surjective as well. □

5.10. Corollary: If $p \in \mathbb{N}$ is a prime, then $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\zeta_p))$ is a cyclic group of order $p - 1$.

5.11. Corollary: If F is an intermediate field $\mathbb{Q} \subset F \subset \mathbb{Q}(\mu_n)$ such that $\mathbb{Q} \subset F$ is Galois, then $\mathrm{Gal}_{\mathbb{Q}}(F)$ is an abelian group.

Proof. Since $\mathbb{Q} \subset F$ is Galois, by Theorem 3.14, $\mathrm{Gal}_F(\mathbb{Q}(\mu_n)) \lhd \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\mu_n))$ and

$$\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\mu_n))/\mathrm{Gal}_F(\mathbb{Q}(\mu_n)) \cong \mathrm{Gal}_{\mathbb{Q}}(F)$$

Hence, $\mathrm{Gal}_{\mathbb{Q}}(F)$ is a quotient of the abelian group $\mathbb{Z}_n^*$, and so it must be abelian. □

5.12. (Kronecker-Weber Theorem) If $\mathbb{Q} \subset F$ is any finite normal extension such that $\mathrm{Gal}_{\mathbb{Q}}(F)$ is abelian, then $\exists n \in \mathbb{N}$ such that $F \subset \mathbb{Q}(\mu_n)$.

The proof of this statement will take up the rest of the course.

Exercises

Read all the previous sections carefully and ask any questions you may have

5.1. If $m, n \in \mathbb{N}$ has lcm l, then

(i) Prove that $\mathbb{Q}(\zeta_n) \subset \mathbb{Q}(\zeta_l)$ and $\mathbb{Q}(\zeta_m) \subset \mathbb{Q}(\zeta_l)$

(ii) Prove that $\exists s, t \in \mathbb{Z}$ such that $\zeta_l = \zeta_m^s \zeta_n^t$

(iii) Conclude that

$$\mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_l)$$

5.2. (i) For any $n \in \mathbb{N}$, prove that

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

(ii) If $p \in \mathbb{N}$ is prime, then prove that

$$\Phi_{2p}(x) = \Phi_p(-x) \qquad \text{(Compare with Exercise 1.5)}$$
$$\Phi_{p^2}(x) = \sum_{k=0}^{p-1} x^{pk}$$

(iii) Determine $\Phi_8(x)$ (Compare with Exercise 1.3)

Recall the following facts:

(i) Chinese Remainder theorem: If $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ is the prime decomposition of n with $\{p_i\}$ all distinct primes, then

$$\mathbb{Z}_n^* \cong (\mathbb{Z}_{p_1^{e_1}})^* \times (\mathbb{Z}_{p_2^{e_2}})^* \times \ldots \times (\mathbb{Z}_{p_k^{e_k}})^*$$

(ii) If $G = G_1 \times G_2$ is the direct product of two finite groups. Then G is cyclic iff both G_1 and G_2 are cyclic and $(|G_1|, |G_2|) = 1$.

5.3. If $p \in \mathbb{N}$ is prime, then prove that $|\mathbb{Z}_{p^e}^*| = p^e - p^{e-1}$

5.4. If $n \in \mathbb{N}$ is such that $\mathbb{Z}_n^*$ is cyclic, then prove that n can be divisible by atmost one odd prime.

5.5. Let $n \geq 3$

(i) List down the element of $\mathbb{Z}_8^*$, and prove that it is not cyclic.

(ii) Prove that there is a surjective map

$$\mathbb{Z}_{2^n}^* \to \mathbb{Z}_{2^{n-1}}^*$$

(iii) Use induction and part (i) to prove that $\mathbb{Z}_{2^n}^*$ is not cyclic

5.6. If $n \in \mathbb{N}$ such that $\mathbb{Z}_n^*$ is cyclic, then prove that either $n = 4$ or $n = 2^i p^j$ for some odd prime p and $i \in \{0, 1\}$ and $j \in \mathbb{N} \cup \{0\}$

Note: The converse to the above statement is also true.

Bibliography

[Stewart] Ian Stewart, *Galois Theory (3rd Ed.)*

[Rotman] J. Rotman, *Galois Theory (2nd Ed.)*

[Garling] DJH Garling, *A Course in Galois Theory*

[E. Artin] Emil Artin and A.N. Milgram, *Galois Theory*

[Greenberg] M.J. Greenberg, *An Elementary Proof of the Kronecker-Weber Theorem*, The American Mathematical Monthly, Vol. 81, No. 6 (Jun.-Jul. 1974), pp. 601-607.

[Lang] S. Lang, *Algebraic Number Theory*, Addison-Wesley, Reading, Mass. (1970)

[Neukrich] J. Neukrich, *Algebraic Number Theory*, Springer (1999)