Field Theory

Dr. Anuj Jakhar

Lecture 1-4

Indian Institute of Technology Bhilai

anujjakhar@iitbhilai.ac.in

June 14, 2021

- Fields have been used implicitly ever since the discovery of addition, subtraction, multiplication and division. Cardano's formula dating 16th century used $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.
- Lagrange used the field of rational functions in n variables in his study of roots of polynomials in 1770.
- The first truly abstract notion of field is due to Dedekind. In 1877, he gave the following definition: "*I call a system A of numbers (not all zero) a field when the sum, difference, product and quotient of any two numbers in A also belong to A.*"
- This is not completely general for the numbers in this definition are all complex.
- In fact in 1893, his student Weber gave the first fully abstract definition of field which we use today.

Definition. A *binary operation* denoted by '$*$' on a set A is given by a function from $A \times A$ into A mapping (a, b) to $a * b$. A non-empty set G with a binary operation '$*$' is said to be a *group*[1] with respect to '$*$' if the following three conditions are satisfied for all a, b, c belonging to G:

(i) $a * (b * c) = (a * b) * c$ (associativity),

(ii) there exists an element $e \in G$, such that $a * e = a = e * a$ (existence of identity),

(iii) for every $a \in G$, there exists an element $a' \in G$ such that $a * a' = e = a' * a$ (existence of inverse).

Further G is called commutative/abelian[2] if $a * b = b * a$ for all $a, b \in G$.

[1] The abstract form of the definition of a group, which we use today, was built up slowly over the course of 19th century, with suggested definitions by Cayley, Kronecker, Weber, Burnside, and Pierpont. The axioms of associativity, identity element and inverse were first stated in their present form by Pierpont.

[2] The term abelian is derived from the name of Norwegian Mathematician Niels Henrik Abel (1802-1829) who showed the importance of such groups in the theory of equations.

Definition. A set R with two binary operations denoted by '$+$' and '$\cdot$' is said to be a *ring* if

(i) $(R, +)$ is a commutative group,

(ii) Multiplication is associative, i.e., $a.(b.c) = (a.b).c$ for every $a, b, c \in R$,

(iii) Distributive laws hold: $a.(b + c) = a.b + a.c$ and $(b + c).a = b.a + c.a$ for every $a, b, c \in R$.

Definition. A non-empty set F with two binary operations denoted by '$+$' and '$\cdot$' is said to be a *field* if the following axioms are satisfied:
(i) $(F, +)$ is a commutative group (with identity element to be denoted by 0).
(ii) $(F \setminus \{0\}, \cdot)$ is a commutative group (with identity element to be denoted by 1).
(iii) Distributive laws hold, i.e., $a.(b + c) = a.b + a.c$ and $(b + c).a = b.a + c.a$ for every $a, b, c \in F$.

Examples.

(i). $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are fields with respect to ordinary addition and multiplication.

(ii). The set $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ is a field with respect to the usual addition and multiplication.

(iii). Let n be a positive integer. For a, b belonging to $\mathbb{Z}$, we write $a \equiv b \pmod{n}$ and say a is congruent to b modulo n if n divides $a - b$. This is an equivalence relation on $\mathbb{Z}$. The equivalence class of an integer m for this equivalence relation is denoted by $[m]$. The set $\mathbb{Z}/n\mathbb{Z} = \{[m] \mid m = 0, 1, \ldots, n-1\}$ is a ring with respect to the operations $[i] + [j] = [i + j]$ and $[i] \cdot [j] = [ij]$. The ring $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is a prime.

(iv). In what follows, x will stand for an **indeterminate** and $F[x]$ will denote **the set of all polynomials in x with coefficients from F.** It is a ring with respect to the usual addition and multiplication of polynomials. Its quotient field to be denoted by $F(x)$ is the field of rational functions in x over F. Similarly one can define the field of rational functions $F(x_1, x_2, \ldots, x_n)$ in n indeterminates.

Definition. A non-empty subset E of a field F is said to be a subfield of F if E is a field under the induced addition and multiplication operations on F. If a subfield E of F is not equal to F, we shall say that E is a proper subfield of F. If E is a subfield of F, then F is said to be an overfield of E.

Remark. If $\{E_i\}_{i\in I}$ is a family of subfields of a field F, then so is $E = \bigcap\limits_{i\in I} E_i$.

Definition. Let F be a field. By the prime subfield of F we mean the smallest subfield of F. It is the intersection of all subfields of F.

Definition. Let F be a field and K be a field containing F as a subfield. Then K is called an extension of F or K/F is called a field extension. K can be regarded as a vector space over F. A basis of this vector space is called a basis of the extension K/F and its dimension is called the degree of the extension K/F, which will be denoted by $[K : F]$.

Let K/F be a field extension. Then K is said to be finite or infinite extension of F according as the degree of K/F is finite or infinite.

Example. With operations of usual addition and multiplication, $\mathbb{C}$ is an extension of $\mathbb{R}$ of degree two and $\mathbb{R}$ is an infinite extension of $\mathbb{Q}$ because $\mathbb{R}$ is uncountable and $\mathbb{Q}$ is countable.

In 1894, Dedekind developed the theory of field extensions that included the concept of degree. He formulated the proof of Tower theorem stated below.

Tower Theorem. If K is a finite extension of F and L is a finite extension of K, then L is a finite extension of F and $[L : F] = [L : K][K : F]$.

Proof of Tower Theorem.

- Let $\{e_1, e_2, \ldots, e_m\}$ be a basis of K/F and $\{f_1, f_2, \ldots, f_n\}$ be a basis of L/K.
- We claim that $\{e_i f_j \mid 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant n\}$ is a basis of L/F.
- Let α be any element of L. Write $\alpha = \sum\limits_j b_j f_j$, $b_j \in K$ and

  $b_j = \sum\limits_i \lambda_{ij} e_i$, $\lambda_{ij} \in F$.
- Then
$$\alpha = \sum_j \left(\sum_i \lambda_{ij} e_i \right) f_j = \sum_{i,j} \lambda_{ij} e_i f_j.$$
- This shows that the set $\{e_i f_j \mid 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant n\}$ generates the vector space L over F.

Proof Contd....

- To prove its linear independence over F, suppose that $\sum_{i,j} \mu_{ij} e_i f_j = 0$ for some $\mu_{ij} \in F$.
- Then

$$\sum_j \left(\sum_i \mu_{ij} e_i \right) f_j = 0.$$

- As $\{f_1, f_2, \ldots, f_n\}$ is linearly independent over K, it follows that

$$\sum_i \mu_{ij} e_i = 0 \ \text{ for all } \ j.$$

- Since $\{e_1, e_2, \ldots, e_m\}$ is linearly independent over F, $\mu_{ij} = 0$ for all i,j.
- Thus $\{e_i f_j, \ 1 \leqslant i \leqslant m, \ 1 \leqslant j \leqslant n\}$ is a basis of the vector space L over F consisting of mn elements.

Definition. Let F and F' be fields.

- A mapping f from F to F' is called an isomorphism (of fields) if (i) f is 1-1, (ii) $f(a+b) = f(a) + f(b)$, $f(ab) = f(a)f(b)$ for all $a, b \in F$.
- Two fields F and F' are said to be isomorphic if there exists an isomorphism from one onto the other.
- An isomorphism from F onto itself is called an *automorphism* of F.
- It can be easily checked that if F_0 is the prime subfield of a field F, then F_0 is isomorphic to either $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$ for some prime p.
- A field with p elements will be denoted by F_p.

Definition. The characteristic of a field F is defined to be 0 or p according as the prime subfield of F is isomorphic to $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$, where p is a prime.

Remark. Let F and F' be fields.

- If F is a finite field of characteristic p, then F can be regarded as an extension of $F_p = \mathbb{Z}/p\mathbb{Z}$ and if $\{w_1, \dots, w_m\}$ is a basis of the extension F/F_p, then clearly F has exactly p^m elements, because each element of F can be uniquely writtten as $a_1 w_1 + \cdots + a_m w_m$ with a_i's in F_p.
- We shall prove later that given a prime p and any number $m \geq 1$, there exists a finite field with p^m elements which is “unique" in some sense.

Definition. Let K/F be an extension of fields and $S \subseteq K$. The smallest subfield of K containing $F \bigcup S$ is called the subfield generated by S over F and is denoted by $F(S)$.
In fact $F(S)$ is the intersection of all the subfields of K containing $F \bigcup S$.
If $S = \{\alpha_1 \dots, \alpha_n\}$ is a finite set, then we say that $F(S)$ is finitely generated over F and write $F(S)$ as $F(\alpha_1, \dots, \alpha_n)$.

Definition. An extension K/F is called a *simple* extension if K/F is generated by a single element, i.e., $K = F(\alpha)$ for some $\alpha \in K$; such an element α is called a primitive element for the extension K/F.

Example. Any extension of prime degree is a simple extension.

Definition. Let K/F be an extension of fields and $\{\alpha_1 \ldots, \alpha_n\}$ be a subset of K. The smallest subring of K containing F and $\alpha_1, \ldots, \alpha_n$ will be denoted by $F[\alpha_1, \ldots, \alpha_n]$.

It consists of all polynomial expressions in $\alpha_1, \ldots, \alpha_n$ with coefficients from F.

Note that $F(\alpha_1, \ldots, \alpha_n)$ is quotient field of $F[\alpha_1, \ldots, \alpha_n]$.

Given a field extension K/F and elements $\alpha_1 = \alpha, \ldots, \alpha_n$ in K, it would be interesting to know when is $F(\alpha) = F[\alpha]$ or more generally when is $F(\alpha_1, \ldots, \alpha_n) = F[\alpha_1, \ldots, \alpha_n]$. These questions are related to algebraic extensions introduced below.

Definition. Let K/F be a field extension.

- An element $\alpha \in K$ is called algebraic over F if it satisfies a non-zero polynomial with coefficients from F.
- An element of K which is not algebraic over F is called transcendental over F.
- If every element of K is algebraic over F, then we say that K/F is an algebraic extension.
- An extension which is not algebraic is called a transcendental extension.

- A complex number α is called an algebraic number if it is algebraic over $\mathbb{Q}$, otherwise it is called a transcendental number.
- It was in 1853 that the existence of transcendental numbers was proved by Joseph Liouville.
- Charles Hermite proved that e is a transcendental number in 1873 and Lindemann showed that π is a transcendental number in 1882.
- To this day, it is not known whether $e + \pi$ is transcendental or not. It is difficult to prove that a given complex number is transcendental, it is easy that the set of all transcendental numbers is uncountable.

Definition. Let K/F be an extension of fields.

- If α belonging to K is algebraic over F, then the monic polynomial $g(x)$ of smallest degree over F satisfied by α is called the minimal polynomial of α over F.
- It can be easily seen that $g(x)$ is irreducible over F.

Examples.

- The minimal polynomial of $1+\sqrt{3}$ over $\mathbb{Q}$ is x^2-2x-2.
- The minimal polynomial of $20^{1/3}$ over $\mathbb{Q}$ is x^3-20 in view of Eisenstein irreducibility criterion.

Proposition 1. Let K/F be an extension of fields. Suppose $\alpha \in K$ is algebraic over F with minimal polynomial $g(x)$ over F of degree n. Then $F(\alpha)$ is an extension of degree n of F. Indeed we have

$$F(\alpha) = \{a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} \mid a_i \in F \text{ for } 0 \leq i \leq n-1\} = F[\alpha].$$

Note.

- It may be pointed out that Abel was the first to notice that $F(\alpha) = F[\alpha]$ when α is algebraic over F.
- The converse of this result is also true because if $F(\alpha) = F[\alpha]$, then $1/\alpha = g(\alpha)$ for some polynomial $g(x) \in F[x]$. So α satisfies the non-zero polynomial $xg(x) - 1$ and hence α is algebraic over F.

Corollary 2. If $F(\alpha_1, \alpha_2, \ldots, \alpha_r)$ is a finitely generated extension of F with each α_i algebraic over F, then $F(\alpha_1, \alpha_2, \ldots, \alpha_r)/F$ is a finite extension and $F(\alpha_1, \alpha_2, \ldots, \alpha_r) = F[\alpha_1, \alpha_2, \ldots, \alpha_r]$.

Proposition 3. Every finite extension is algebraic.

Proof.

- uppose that K/F is a finite extension of degree n.
- Let $\alpha \in K$. Then the $n+1$ elements $1, \alpha, \ldots, \alpha^n$ are linearly dependent over F as $[K : F] = n$.
- Hence there exist $a_0, a_1, \ldots, a_n \in F$, not all zero such that $a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0$.
- This implies that α is algebraic over F.

Remark.

- Converse of the above proposition is not true.
- Let $\mathbb{A}$ denote the set of all complex numbers which are algebraic over $\mathbb{Q}$. Then $\mathbb{A}$ is a subfield of $\mathbb{C}$ in view of Theorem 5.
- Using Eisenstein irreducibility criterion, one can verify that $\mathbb{A}/\mathbb{Q}$ is an infinite extension.

Theorem 4. (Transitive property of algebraic extensions) If K/F and L/K are algebraic extensions, then so is L/F.

Theorem 5. Let K/F be an extension of fields. The set E of all elements of K which are algebraic over F is a subfield of K containing F.

Theorem 6. Let K/F be a finite simple extension with $K = F(\alpha)$ and $g(x)$ be the minimal polynomial of α over F. Let $\langle g(x) \rangle$ denote the ideal generated by $g(x)$ in $F[x]$. Then $F[x]/\langle g(x) \rangle$ is isomorphic to $F(\alpha) = F[\alpha]$.

Proof of Theorem 6.

- Consider the map $\psi : F[x] \to F[\alpha]$ defined by $\psi(h(x)) = h(\alpha)$, $h(x) \in F[x]$.
- Clearly ψ is an onto ring homomorphism with $\ker(\psi) = \langle g(x) \rangle$.
- The theorem now follows from the first isomorphism theorem of rings.

- Cauchy's observation in 1847 that $\mathbb{R}[x]/\langle x^2 + 1 \rangle$ is a field that contains a zero of $x^2 + 1$ paved the way for the next sweeping generalization proved by Kronecker in 1887.

Theorem 7. (Kronecker) If $g(x)$ is a polynomial of degree $n \geqslant 1$ with coefficients in field F and is irreducible over F, then there is an extension K of F with $[K : F] = n$ in which $g(x)$ has a root.

Proof of Theorem 7.

- Since $g(x)$ is irreducible over F, the ideal $I = \langle g(x) \rangle$ in the principal ideal domain $F[x]$ is a maximal ideal and hence $F[x]/I$ is a field.
- Denote $F[x]/I$ by K.
- The mapping from F into K defined by $a \mapsto I + a$ is an isomorphism of F onto its image F' contained in K.
- Identifying F with F', we can consider K as an extension of F.
- Note that the element $I + x$ belonging to K is a root of the polynomial $g(X)$, because $g(I + x) = I + g(x) = I$ as $g(x) \in I$.
- It can be easily checked that $I + 1, I + x, \ldots, I + x^{n-1}$ form a basis of K$=F[x]/I$ over F.
- So $[K : F] = n$.

The corollary stated below follows quickly from Theorem 7.

Corollary 8. If $h(x)$ is a polynomial with coefficients in a field F, then there is a finite extension K of F in which $h(x)$ has a root. Moreover $[K : F] \leqslant \deg h(x)$.

Theorem 9. Let $h(x)$ be a polynomial of degree $n \geqslant 1$ with coefficients in a field F. Then there is an extension K of F of degree at most $n!$ in which $h(x)$ has n roots.

Definition. Let $h(x)$ belonging to $F[x]$ be a polynomial of degree n. An extension K/F is called a splitting field of $h(x)$ over F if K contains n roots $\alpha_1, \alpha_2, \ldots, \alpha_n$ of $h(x)$ and $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

The following corollary is an immediate consequence of Theorem 9.

Corollary 10. Let $h(x)$ be a polynomial of degree $n \geqslant 1$ with coefficients in a field F. Then $h(x)$ has a splitting field L and $[L : F] \leqslant n!$.

Examples.

(i). The splitting field contained in $\mathbb{C}$ of the polynomial $x^3 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(2^{1/3}, \omega)$ where $\omega \neq 1$ is a cube root of unity.

(ii). The splitting field contained in $\mathbb{C}$ of $x^4 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(2^{1/4}, \sqrt{-1})$.

(iii). A splitting field of $x^2 + x + \bar{1}$ over $\mathbb{Z}/2\mathbb{Z}$ consists of $\bar{0}, \bar{1}, \alpha, \bar{1} + \alpha$ where $\alpha^2 + \alpha + \bar{1} = 0$. It provides an example of a field having exactly four elements.

(iv). Let α be a root of the polynomial $x^2 + \bar{1}$ with coefficients in $F_3 = \mathbb{Z}/3\mathbb{Z}$ in an extension of $\mathbb{Z}/3\mathbb{Z}$. Then $K = F_3(\alpha)$ is a splitting field of $x^2 + \bar{1}$. By Proposition **??**, $K = \{a + b\alpha \mid a, b \in F_3\}$ is a field of nine elements.

Definition. Let K and K' be extensions of a field F. A field isomorphism from K into K' which is identity on F is called an F-isomorphism of K into K'. An F-isomorphism of K onto itself is called an F-automorphism of K.

The next theorem tells us that if L_1 and L_2 are splitting fields of a polynomial $h(x)$ over F, then there is an F-isomorphism from L_1 onto L_2.

Theorem 11. Let $\sigma : F \to F'$ be an isomorphism of a field F onto a field F'. Let $h(x) = \sum a_i x^i$ be a polynomial belonging to $F[x]$ and $h^\sigma(x) = \sum \sigma(a_i) x^i$ be its image polynomial. Let K and K' be splitting fields of $h(x)$ and $h^\sigma(x)$ over F, F' respectively. Then there exists an isomorphism $\bar{\sigma}$ from K onto K' such that $\bar{\sigma}|_F = \sigma$.

The following corollary follows immediately from Theorem 11.

Corollary 12. A splitting field of a polynomial over a field F is unique upto F-isomorphism.

Corollary 13. Any two finite fields having the same number of elements are isomorphic.

Proof.

- Let K be a finite field with $q = p^m$ elements.
- Since $K^\times$ is a group of order $q - 1$, for any element $\alpha \in K^\times$, $\alpha^{q-1} = 1$ by Lagrange's theorem for finite groups.
- So each element of K is a root of the polynomial $x^q - x$ which can have at most q roots.
- Thus K is a splitting field of $x^q - x$ over F_p.
- The result now follows from Corollary 12.

Definition. A field F is called algebraically closed if it has no proper algebraic extension, i.e., if K is an algebraic extension of F, then $K = F$.

Remark. In 1799, Gauss at the age of 22, proved that $\mathbb{C}$ is algebraically closed. This result was then considered so important that it was called “The Fundamental Theorem of Algebra". Over a period of fifty years, Gauss gave four different proofs of this theorem.

Example.

- Let $\mathbb{A}$ denote the set of all those complex numbers which are algebraic over $\mathbb{Q}$. In view of Theorem 5, $\mathbb{A}$ is a subfield of $\mathbb{C}$ and is called the field of algebraic numbers. Assuming that $\mathbb{C}$ is algebraically closed we show that $\mathbb{A}$ is algebraically closed. Let ξ be an element of an overfield of $\mathbb{A}$ which is algebraic over $\mathbb{A}$, then ξ being algebraic over $\mathbb{C}$ belongs to $\mathbb{C}$. Since ξ satisfies a polynomial $x^n + a_1x^{n-1} + \cdots + a_n$ for some a_i's belonging to $\mathbb{A}$, it follows that ξ is algebraic over the finite extension $\mathbb{Q}(a_1, a_2, \ldots, a_n)$ of $\mathbb{Q}$ and hence ξ is algebraic over $\mathbb{Q}$ in view of Theorem 4. This proves that ξ belongs to $\mathbb{A}$.

Definition. An extension $\hat{F}$ of a field F is called an algebraic closure of F if $\hat{F}/F$ is an algebraic extension and $\hat{F}$ is an algebraically closed field.

Example. The field $\mathbb{A}$ of algebraic numbers is an algebraic closure of $\mathbb{Q}$.

Remark. In 1910, Ernst Steinitz proved that every field F has an algebraic closure which is unique upto F-isomorphism, i.e., if $\hat{F}_1$ and $\hat{F}_2$ are two algebraic closures of F, then there exists an isomorphism from $\hat{F}_1$ onto $\hat{F}_2$ which is identity on F.

Separable Extensions.

Definition. Let $g(x)$ belonging to $F[x]$ be an irreducible polynomial. $g(x)$ is called a separable polynomial if all its roots in its splitting field are distinct, otherwise it is called inseparable.

Definition.

- Let K/F be an extension of fields. An element $\alpha \in K$ is called *separable* over F if it is algebraic over F and its minimal polynomial over F is a separable polynomial, otherwise α is called *inseparable* over F.
- An extension K/F is called separable if it is algebraic and every $\alpha \in K$ is separable over F.

Examples.

(i). $3^{1/5}$ is separable over $\mathbb{Q}$. In fact $a^{1/n}$ is separable over $\mathbb{Q}$ for any integer a.

(ii). Let $F = F_p(t)$ where t is an indeterminate. Then $\alpha = t^{1/p}$ is not separable over F.

Using Taylor's expansion of a polynomial, the following proposition can be easily proved.

Proposition 14. Let $h(x)$ belonging to $F[x]$ be a non-constant polynomial. A root α of $h(x)$ in some extension field is a repeated root of $h(x)$ if and only if $h'(\alpha) = 0$.

Proposition 15. A monic irreducible polynomial $g(x)$ over a field F has a repeated root if and only if $g'(x)$ is the zero polynomial.

Proof. If $g(x)$ has a repeated root, say α in an extension of F, then by the above proposition $g'(\alpha) = 0$.

- But $g(x)$ being the minimal polynomial of α over F divides every other polynomial $h(x) \in F[x]$ with $h(\alpha) = 0$.
- So in particular $g(x)$ divides $g'(x)$.
- Since $\deg g'(x) < \deg g(x)$, we conclude that $g'(x)$ is identically zero.
- Conversely suppose that $g'(x)$ is the zero polynomial. Then by Proposition 14, every root of $g(x)$ is a repeated root.

Corollary 16. Each irreducible polynomial over a field of characteristic zero is separable.

Corollary 17. An irreducible polynomial $g(x) \in F[x]$ is inseparable if and only if the field F is of characteristic $p > 0$ and $g(x)$ is a polynomial in x^p.

Proof.

- In view of Proposition 15, a monic irreducible polynomial $g(x)$ belonging to $F[x]$ is inseparable if and only if $g'(x)$ is the zero polynomial.
- On writing $g(x)$ as $g(x) = \sum a_i x^i$, we see that $g'(x)$ is the zero polynomial if and only if characteristic of F is a prime p and $a_i = 0$ for each index i not divisible by p, i.e., $g(x) = a_0 + a_p x^p + a_{2p} x^{2p} + \dots$.

Definition. A field F is called perfect if all finite extensions of F are separable.

Note.

- It is immediate from Corollary 16 that every field of characteristic zero is a perfect field.
- Note that if F is a field of characteristic $p > 0$, then $F^p = \{a^p \mid a \in F\}$ is a subfield of F.
- The following theorem asserts that $F^p = F$ if and only if F is perfect.

Theorem 18.

Let F be a field of characteristic $p > 0$. Then F is perfect if and only if every element of F has a pth root in F, i.e., for every $a \in F$, there exists $b \in F$ with $b^p = a$.

Corollary 19. Any finite field is perfect.

Proof.

- Let F be a finite field of characteristic $p > 0$.
- The mapping $a \mapsto a^p$ defined from F into F is 1-1 and hence onto.
- Therefore the corollary follows from Theorem 18.

Definition.

Let K_1, K_2 be subfields of a field L. The smallest subfield of L containing K_1 and K_2 is called the compositum (composite) of K_1 and K_2 and is denoted by $K_1 K_2$ or by $K_1 \cdot K_2$.

Note.

- If K_1, K_2 are algebraic extensions of field F which are subfields of a field L, then we show that the compositum K_1K_2 consists of all finite sums of the type $\sum \alpha_i\beta_i$ where α_i's $\in K_1,\ \beta_i$'s $\in K_2$.
- This is so because the inverse of an element of the type $\sum\limits_{i=1}^{k} \alpha_i\beta_i$ with α_i's $\in K_1,\ \beta_i$'s $\in K_2$, belongs to the subfield $F(\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_k)$ which equals the subring $F[\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_k]$ in view of Corollary 2.
- In particular if K is an algebraic extension of a field F of characteristic $p > 0$, then F, K^p are algebraic extensions of the field F^p and hence the compositum FK^p consists of all finite sums of the type $\sum b_iy_i^p$ with $b_i \in F$, $y_i \in K$.

The following theorem gives a necessary and sufficient condition for a finite extension to be separable.

Theorem 20. Suppose F is a field of characteristic $p > 0$. A finite extension K/F is separable if and only if $K = FK^p$.

The following corollary is an immediate consequence of the above theorem.

Corollary 21. Let α be algebraic over a field F of characteristic $p > 0$. Then $F(\alpha)/F$ is separable if and only if $F(\alpha^p) = F(\alpha)$.

Corollary 22. If α is separable over a field F, then $F(\alpha)/F$ is a separable extension.

Proof.

- Since every finite extension of a field of characteristic zero is separable, it is enough to prove the corollary when characteristic of F is $p > 0$.
- Check that $F(\alpha) = F(\alpha^p)$.
- Hence by the above corollary, $F(\alpha)$ is a separable extension of F.

Theorem 23. (Transitive property of separable extensions) If L/K and K/F are separable extensions, then so is the extension L/F.

Corollary 24. Let K/F be an extension of fields. The set F^S of all elements of K which are separable over F forms a subfield of K.

Proof.

- Let $\alpha, \beta \in K$ be separable over F.
- It is to be shown that $\alpha \pm \beta$, $\alpha\beta$ and α/β are separable over F.
- Now $F(\alpha)/F$ is separable by Corollary 22.
- Also $F(\alpha, \beta)/F(\alpha)$ is separable by the same corollary.
- Therefore by the transitive property of separable extensions, $F(\alpha, \beta)/F$ is separable.

The following corollary is an immediate consequence of the above corollary.

Corollary 25. If elements $\alpha_1, \alpha_2, \dots, \alpha_n$ of an extension of a field F are separable over F, then $F(\alpha_1, \alpha_2, \dots, \alpha_n)/F$ is a separable extension.

Definition. The set F^S given in Corollary 24 is called the separable closure of F in K and the degree $[F^S : F]$ is called the separable degree of the extension K/F. The degree of K/F^S is called the inseparable degree of K/F.

Finite separable extensions have a special property which is given by the following theorem.

Theorem 26. (Primitive Element Theorem) Every finite *separable* extension is simple. More generally if $K = F(\theta_1, \theta_2, \ldots, \theta_n)$ is a finite extension of a field F and if at least $n-1$ of the elements $\theta_1, \ldots, \theta_n$ are separable over F, then K is a simple extension of F.

Definition. Let K/F be an extension of fields of characteristic $p > 0$. An element α of K is said to be purely inseparable over F if the minimal polynomial of α over F has only one root. The extension K/F is said to purely inseparable if every element of K is purely inseparable over F.

Note that an element α of K is both separable and inseparable over F if and only if $\alpha \in F$.

Theorem 27. Let K/F be an algebraic extension of fields of characteristic $p > 0$. Let F^S denote the separable closure of F in K. Then K/F^S is a purely inseparable extension. In particular every algebraic extension can be written as a separable extension followed by a purely inseparable extension.

Proof.

- Let α be any element of K.
- To prove the theorem, it is enough to show that there exists $e \geqslant 0$ such that $\alpha^{p^e} \in F^S$;
- because this will prove that α is purely inseparable over F^S as it will satisfy the polynomial $x^{p^e} - \alpha^{p^e} = (x-\alpha)^{p^e}$ over F^S.
- Let $g(x)$ be the minimal polynomial of α over F.
- If α is separable over F, then $\alpha \in F^S$. If not, then by Corollary 17, $g(x)$ is a polynomial in x^p, say $g(x) = g_1(x^p)$, $g_1(x) \in F[x]$.

Proof Contd....

- Note that $g_1(x)$ being irreducible over F is the minimal polynomial of α^p over F.
- If α^p is separable over F, then $\alpha^p \in F^S$.
- If not, then by Corollary 17, $g_1(x) = g_2(x^p)$ for some $g_2(x) \in F[x]$.
- Note that $g_2(x)$ is the minimal polynomial of α^{p^2} over F and $\deg g_2(x) = \frac{\deg g_1(x)}{p} = \frac{\deg g(x)}{p^2}$.
- Repeating the above argument, we see that there exists e such that α^{p^e} must be separable over F.

Normal Extensions.

Definition. An algebraic extension K/F is called a normal extension if whenever an irreducible polynomial $g(x) \in F[x]$ has one root in K, then it has all roots in K.

Examples.

(i) Any extension K/F of degree two is normal because if an irreducible polynomial $g(x) = ax^2 + bx + c$ has one root β in K, then its other root namely $-\beta - b/a$ also belongs to K.

(ii) If K/F is a normal extension, then the separable closure F^S of F in K is also a normal extension of F.

(iii) Let θ be a root of the polynomial $x^4 - 2$, then $\mathbb{Q}(\theta)/\mathbb{Q}$ is not a normal extension.

Definition. Two elements α and α' lying in an extension of a field F and both algebraic over F are said to be *conjugates* over F or F*-conjugates* if they have the same minimal polynomial over F.

Proposition 28. Let α and α' be algebraic over a field F. Then α and α' are conjugates over F if and only if there exists an F-isomorphism σ from $F(\alpha)$ onto $F(\alpha')$ with $\sigma(\alpha) = \alpha'$.

Proof.

- Suppose first that α and α' are the roots of the same monic irreducible polynomial $g(x)$ belonging to $F[x]$.
- By Proposition 1, $F(\alpha) = F[\alpha]$ and $F(\alpha') = F[\alpha']$.
- Let $h(\alpha)$ be any element of $F(\alpha)$, $h(x) \in F[x]$.
- We define $\sigma(h(\alpha)) = h(\alpha')$.
- Then σ is well defined because if $h(\alpha) = h_1(\alpha)$ with $h_1(x) \in F[x]$, then $g(x)$ divides $h(x) - h_1(x)$ and hence $h(\alpha') = h_1(\alpha')$.
- It can be easily seen that σ is F-isomorphism of $F(\alpha)$ onto $F(\alpha')$.

Proof Contd....

- Conversely, assume that there exists an F-isomorphism σ from $F(\alpha)$ onto $F(\alpha')$ with $\sigma(\alpha) = \alpha'$.
- Let $g(x)$ denote the minimal polynomial of α over F.
- Now $g(\alpha) = 0$ implies that $\sigma(g(\alpha)) = g(\sigma(\alpha)) = g(\alpha') = 0$.
- Therefore α and α' have the same minimal polynomial $g(x)$ over F.

Remark.

- If $g(x)$ is an irreducible polynomial over a field F having a root α and L is an extension of F containing a splitting field of $g(x)$ over F, then arguing as in the proof of above proposition, it can be easily seen that the number of F-isomorphisms of $F(\alpha)$ into L is the number of distinct roots of $g(x)$.
- In fact each of these F-isomorphisms is defined by mapping α onto a root of $g(x)$.
- In particular, if K/F is a finite separable extension of degree n, then by Theorem 26, K/F is a simple extension and hence there are exactly n F-isomorphisms of K into a normal extension of F containing K.

The following two results will be used to give two more equivalent definitions of a finite normal extension.

Proposition 29. Let K be a splitting field of a polynomial $h(x) \in F[x]$ over a field F. If σ is an F-isomorphism from K into an extension of K, then $\sigma(K) = K$.

Proof. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the roots of $h(x)$ in K so that $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

- Let σ is an F-isomorphism from K into an extension of K.
- Write $h(x) = \prod_{i=1}^{n}(x - \alpha_i)$.
- Applying σ, we obtain $h(x) = \prod_{i=1}^{n}(x - \sigma(\alpha_i))$.
- So $\sigma(\alpha_1), \sigma(\alpha_2), \ldots, \sigma(\alpha_n)$ is a permutation of $\alpha_1, \alpha_2, \ldots, \alpha_n$.
- Therefore

$$\begin{aligned}\sigma(K) = \sigma(F(\alpha_1, \alpha_2, \ldots, \alpha_n)) &= F(\sigma(\alpha_1), \sigma(\alpha_2), \ldots, \sigma(\alpha_n)) \\ &= F(\alpha_1, \alpha_2, \ldots, \alpha_n) = K.\end{aligned}$$

Theorem 30. Let K/F be a finite extension of fields. Then the extension K/F is normal if and only if K is a splitting field over F of some polynomial in $F[x]$.

Proof.

- Let K/F be a finite normal extension.
- Write $K = F(\beta_1, \beta_2, \ldots, \beta_m)$.
- Let $g_i(x) \in F[x]$ be the minimal polynomial of β_i over F and define $h(x) = \prod_{i=1}^{m} g_i(x)$.
- Then K contains all roots of $h(x)$ and hence it is a splitting field of $h(x)$ over F.

Proof Contd....

- Conversely let K be a splitting field of a polynomial $h(x) \in F[x]$.
- Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be all the roots of $h(x)$ so that $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$.
- Let $\beta \in K$ be any root of a monic irreducible polynomial $g(x) \in F[x]$.
- Let β' be another root of $g(x)$ in an extension of K.
- We have to prove that $\beta' \in K$. Since β and β' are F-conjugates, there exists an F-isomorphism σ from $F(\beta)$ onto $F(\beta')$ with $\sigma(\beta) = \beta'$ by Proposition 28.
- Note that splitting fields of $h(x)$ over $F(\beta)$ and $F(\beta')$ are respectively $K(\beta) = K$ and $K(\beta') = F(\beta', \alpha_1, \ldots, \alpha_n)$.
- Therefore by Theorem 11, σ can be extended to an F-isomorphism σ_1 from K onto $K(\beta')$.
- By Proposition 29, $\sigma_1(K) = K$, so $\beta' = \sigma_1(\beta)$ belongs to K.
- This proves that K/F is normal.

Definition.

- Let K/F be a finite extension. It can be easily seen that there exists a smallest normal extension L of F such that $K \subseteq L$.
- The field L is called a normal closure of K over F.
- In fact if $K = F(\beta_1, \beta_2, \dots, \beta_m)$ and $g_i(x) \in F[x]$ is the minimal polynomial of β_i over F, then L is a splitting field of $h(x) = \prod_{i=1}^{m} g_i(x)$ over F. So L is unique upto F-isomorphism.

Proposition 31. Let K be a finite normal extension of a field F and E be a subfiled of K containing F. Then every F-isomorphism of E into K can be extended to an F-automorphism of K.

Proof of Proposition 31.

- Let σ be an F-isomorphism of E into K.
- Since K/F is a finite normal extension, K is a splitting field of a polynomial say $h(x) \in F[x]$ over F by Theorem 30.
- So K is also a splitting field of $h(x)$ over E.
- Therefore in view of Theorem 11, σ can be extended to an F-automorphism of K.

Using the above proposition, we prove the following theorem which gives two more equivalent definitions of a finite normal extension.

Theorem 32. The following statements are equivalent for a finite extension K of a field F:

(i) K/F is a normal extension.

(ii) K is a splitting field over F of a polynomial $h(x)$ belonging to $F[x]$.

(iii) Every F-isomorphism of K into any extension of K has image K.

Proof of Theorem 32.

- (i) and (ii) are equivalent in view of Theorem 30.
- (ii) implies (iii) in view of Proposition 29.
- We now prove that (iii) implies (i).
- Let L be a finite normal extension of F containing K.
- Let $\beta \in K$ be any root of a monic irreducible polynomial $g(x) \in F[x]$.
- Let β' be another root of $g(x)$ in the extension L of K.
- We have to prove that $\beta' \in K$.
- Since β and β' are F-conjugates, there exists an F-isomorphism τ from $F(\beta)$ onto $F(\beta')$ with $\tau(\beta) = \beta'$ in view of Proposition 28.
- By Proposition 31, τ can be extended to an F-automorphism $\bar{\tau}$ (say) of L. On restricting $\bar{\tau}$ to K and using assertion (iii), we see that $\bar{\tau}(K) = K$ and hence $\beta' = \bar{\tau}(\beta)$ belongs to K.
- This proves that K/F is normal.

Keeping in mind the above theorem, the following corollary can be easily verified.

Corollary 33. If K_1, K_2 are finite normal extensions of a field F, then so are K_1K_2 and $K_1 \cap K_2$.

We shall quickly deduce the following corollary from Proposition 31 and Theorem 32.

Corollary 34. Let K be a finite normal extension of field F and E be a subfiled of K containing F. Then E/F is a normal extension if and only if $\sigma(E) = E$ for every F-automorphism σ of K.

Proof of Corollary 34.

- It is immediate from Theorem 32 that if E/F is a normal extension, then $\sigma(E) = E$ for every F-automorphism σ of K.
- To prove the converse, assume that $\sigma(E) = E$ for every F-automorphism σ of K.
- Let $g(x) \in F[x]$ be an irreducible polynomial having a root $\beta \in E$ and β' be another root of $g(x)$.
- Since K/F is normal, $\beta' \in K$.
- Let τ be an F-isomorphism from $F(\beta)$ into K defined by $\tau(\beta) = \beta'$.
- By Proposition 31, τ can be extended to an F-automorphism $\bar{\tau}$ (say) of K.
- Then by our assumption $\bar{\tau}(E) = E$ and therefore $\beta' = \bar{\tau}(\beta)$ belongs to E.
- This proves that E/F is a normal extension.

Example. Every finite extension K of a finite field F is normal.

- Because if $|K| = q = p^m$, then as shown in the proof of Corollary 13, K is a splitting field of $X^q - X$ over F_p and hence it is also splitting field of $X^q - X$ over F.
- Therefore K/F is normal by Theorem 32.

In fact every algebraic extension L of a finite field F is normal because whenever L contains a root α of an irreducible polynomial $g(x)$ belonging to $F[x]$, then all roots of $g(x)$ belong to the normal extension $F(\alpha)$ of F.

Remark. Normality is not a transitive relation. For example; consider $K = \mathbb{Q}(\theta)$ where θ is a real root of $x^4 - 2$, then $\mathbb{Q}(\theta)/\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ are normal but $\mathbb{Q}(\theta)/\mathbb{Q}$ is not a normal extension.

Galois extension.

Definition. An extension K/F is called a Galois extension if it is both normal and separable.

Examples.

(i) An extension of degree 2 of a field of characteristic different from 2 is a Galois extension.

(ii) A generator of the cyclic group consisting of all nth roots of unity in $\mathbb{C}$ is called a primitive nth root of unity. If ζ is a primitive nth root of unity in $\mathbb{C}$, then $\mathbb{Q}(\zeta)/\mathbb{Q}$ is a Galois extension being the splitting field of $X^n - 1$ over $\mathbb{Q}$. The field $\mathbb{Q}(\zeta)$ is called nth cyclotomic field. Such extensions of $\mathbb{Q}$ are called cyclotomic extensions.

(iii) An algebraic extension of a finite field is a Galois extension in view of Corollary 19 and the last example.

(iv) If K/F is a Galois extension and E is a subfield of K containing F, then K/E is also a Galois extension because the minimal polynomial of any element $\beta \in K$ over E divides the minimal polynomial of β over F. On the other hand E/F may fail to be Galois extension. For example: $K = \mathbb{Q}(2^{1/3}, \sqrt{-3})$ being a splitting field of the polynomial $x^3 - 2$, is a Galois extension of $\mathbb{Q}$ but $E = \mathbb{Q}(2^{1/3})$ fails to be a Galois extension of $\mathbb{Q}$.

- Galois extensions are named after the French mathematician Évariste Galois (1811-1832) and are of fundamental importance in field theory.
- Galois gave a complete solution to the problem partially solved by Gauss, Ruffini and Abel of solving a polynomial equation by radicals in 1830 when he submitted a memoir to the Paris Academy of Sciences on the theory of equations.
- In this memoir, he described what is now known as the Galois group of a polynomial and used this group to derive necessary and sufficient conditions for a polynomial to be solvable by radicals.
- For complete details along with the history of this problem, the reader is referred to the interesting book by Jean-Pierre Tignol.

Definition. Let K/F be a Galois extension. The set of all F-automorphisms of K is a group with respect to the composition of maps. This group is called the Galois group[3] of K/F and will be denoted by $\mathrm{Gal}(K/F)$.

Example. Let d, d_1 be distinct squarefree integers. Show that $K = \mathbb{Q}(\sqrt{d}, \sqrt{d_1})$ is a Galois extension of $\mathbb{Q}$ having Galois group isomorphic to Klein's 4-group.

- Since K is the splitting field of the polynomial $(x^2 - d)(x^2 - d_1)$ over $\mathbb{Q}$, it is a normal extension of $\mathbb{Q}$ of degree 4.
- If $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, then $\sigma(\sqrt{d}) = \epsilon\sqrt{d}$, with $\epsilon \in \{1, -1\}$ and so $\sigma^2(\sqrt{d}) = \sqrt{d}$.
- Similarly $\sigma^2(\sqrt{d_1}) = \sqrt{d_1}$ and hence σ^2 is identity.
- Therefore $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to Klein's 4-group.

[3] It may be pointed out that this definition of Galois group is very different from the one given by Galois in his memoir written by him at the age of 19. He only dealt with splitting fields of polynomials and for him, the Galois group consisted of certain permutations of the roots. The modern formulation of Galois Theory is due to Emil Artin who published his own account of Galois Theory in 1938 and 1942.

We shall now compute the degree of the n-th cyclotomic field over $\mathbb{Q}$ as well as its Galois group.

Definition. Let n be a positive integer. The polynomial $\prod_{\eta}(x-\eta)$, where η runs over all primitive n-th roots of unity in $\mathbb{C}$ is called the n-th cyclotomic polynomial and will be denoted by $\Phi_n(x)$. Note that the degree of $\Phi_n(x)$ is $\phi(n)$.

Note that $\Phi_1(x) = x - 1$, $\Phi_2(x) = x + 1$ belong to $\mathbb{Z}[x]$. The following lemma shows that this holds for every n.

Lemma 35. The n-th cyclotomic polynomial $\Phi_n(x)$ is in $\mathbb{Z}[x]$ for every $n \geq 1$.

Proof of Lemma 35.

- The lemma is proved by induction on n. We first show that $\forall n \geq 1$,

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

- The above equality holds because every nth root of unity is a primitive dth root of unity for a unique divisor d of n and the polynomials on either side of (1) do not have any repeated root.
- By induction hypothesis, the polynomial

$$g(x) := \prod_{\substack{d|n \\ d \neq n}} \Phi_d(x)$$

  belongs to $\mathbb{Z}[x]$.
- Since $g(x)$ is monic, it now follows from (1) that the polynomial $\Phi_n(x) = (x^n - 1)/g(x)$ belongs to $\mathbb{Z}[x]$.

Theorem 36. If ζ be a primitive nth root of unity in $\mathbb{C}$, then $[\mathbb{Q}(\zeta):\mathbb{Q}] = \phi(n)$. Equivalently, the cyclotomic polynomial $\Phi_n(x)$ is irreducible over $\mathbb{Q}$.

Corollary 37. Let $K = \mathbb{Q}(\zeta)$ where ζ is a primitive nth root of unity. Then the Galois group G of the extension $K/\mathbb{Q}$ consists of $\phi(n)$ automorphisms σ_r, $1 \leq r \leq n, (r, n) = 1$, defined by $\sigma_r(\zeta) = \zeta^r$ and G is isomorphic to the group $(\mathbb{Z}/n\mathbb{Z})^\times$ of reduced residue classes modulo n.

Proof of Corollary 37.

- By Lemma 35 and Theorem 36, $\Phi_n(x)$ is the minimal polynomial of ζ over $\mathbb{Q}$.
- So the $\mathbb{Q}$-conjugates of ζ are ζ^r, $1 \leq r \leq n, (r, n) = 1$.
- Consequently, we have exactly $\phi(n)$ isomorphisms σ_r from K into K defined by $\sigma_r(\zeta) = \zeta^r$ with r as above; in fact each of these is an automorphism of K because $\sigma_r(K) = \mathbb{Q}(\zeta^r) = \mathbb{Q}(\zeta)$. So the first assertion of the corollary is proved.
- Since ζ^r and hence σ_r depends only upon the residue class $\bar{r}$ of r modulo n, therefore the mapping $\bar{r} \mapsto \sigma_r$ from $(\mathbb{Z}/n\mathbb{Z})^\times$ into G is well defined and bijective.
- It is a group homomorphism, because if $(rs, n) = 1$, then

$$\sigma_{rs}(\zeta) = \zeta^{rs} = \sigma_r(\zeta^s) = \sigma_r(\sigma_s(\zeta)) = \sigma_r \circ \sigma_s(\zeta).$$

This completes the proof of the corollary.

Definition. Let G be a subgroup of the group of all automorphisms of a field K. Then it can be easily seen that the set $\{\alpha \in K \mid \sigma(\alpha) = \alpha \ \forall\ \sigma \in G\}$ is a subfield of K. It is called the *fixed field* of G.

Theorem 38. Let K/F be a Galois extension of degree n. Then the Galois group of K/F is a group of order n and F is the fixed field of $\mathrm{Gal}(K/F)$.

Theorem 39. (Artin's Theorem) Let G be a finite group of automorphisms of a field K and F be the fixed field of G. Then K/F is a Galois extension with $\mathrm{Gal}(K/F) = G$.

Using above two results, we prove the following main result.

Theorem 40. (Fundamental Theorem of Galois Theory) Let K/F be a finite Galois extension. For any subfield T of K which contains F, let $G(K, T)$ denote the subgroup of $G(K, F) = \mathrm{Gal}(K/F)$ consisting of those automorphisms which are identity on T. For any subgroup H of $G(K, F)$, let K_H denote the fixed field of H. Then the mapping $T \mapsto G(K, T)$ sets up a one-to-one correspondence between the set of subfields of K which contain F onto the set of subgroups of $G(K, F)$ such that

(i) $T = K_{G(K,T)}$,

(ii) $H = G(K, K_H)$,

(iii) $[K : T] =$ order of $G(K, T)$ and $[T : F] =$ index of $G(K, T)$ in $G(K, F)$,

(iv) T is a normal extension of F if and only if $G(K, T)$ is a normal subgroup of $G(K, F)$,

(v) when T is a normal extension of F, then $G(T, F) \cong G(K, F)/G(K, T)$.

Proof .

- Note that for any intermediate field T, K/T is a Galois extension, therefore by Theorem 38, T is the fixed field of $G(K, T)$ which proves (i).
- Second assertion follows from Theorem 39 applied to H. Also in view of Theorem 38, we see that $|G(K, F)| = [K : F]$, $|G(K, T)| = [K : T]$. Therefore on dividing, assertion (iii) follows.
- To prove (iv), suppose first that $G(K, T)$ is a normal subgroup of $G(K, F)$. For every $\sigma \in G(K, F)$, $\sigma G(K, T)\sigma^{-1} = G(K, T)$. In particular, their fixed fields are the same. Keeping in mind that the fixed field of $\sigma G(K, T)\sigma^{-1}$ is $\sigma(T)$, we see that $\sigma(T) = T \ \forall \ \sigma \in G(K, F)$. This proves that T/F is a normal extension in view of Corollary 34.

Proof Contd...

- Conversely suppose that T is a normal extension of F. Note that for any $\sigma \in G(K, F)$, $\sigma(T) = T$ in view of Theorem 32.
- Therefore the mapping $\Phi : G(K, F) \to G(T, F)$ given by $\Phi(\sigma) = \sigma|_T$ is clearly a group homomorphism with $\ker(\Phi) = G(K, T)$.
- By virtue of Proposition 31, Φ is onto.
- So by first isomorphism theorem of groups, $G(K, F)/G(K, T) \cong G(T, F)$.
- Therefore $G(K, T)$ is a normal subgroup of $G(K, F)$ and hence the theorem is proved.

Definition. A Galois extension K/F is called cyclic (respectively abelian) if its Galois group is cyclic (respectively abelian[4]).

In view of the fact that a subgroup of an abelian group is normal and a factor group of an abelian (resp. cyclic) group is abelian (resp. cyclic), the corollary stated below follows quickly from assertions (iv), (v) of Theorem 40.

Corollary 41. Let K be a finite Galois extension of a field F which is abelian (resp. cyclic). If E is an intermediate field of the extension K/F, then E/F is a Galois extension and is abelian (resp. cyclic).

[4] The terminology 'abelian extension' seems to have been initiated by Leopold Kronecker who stated and partially proved Kronecker-Weber Theorem which says that every finite abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension.

Keeping in mind that the number of subgroups of a cyclic group of order n is the number of divisors of n, the following corollary is an immediate consequence of Theorem 40.

Corollary 42. Let K be a finite cyclic extension of a field F of degree n. Then the number of intermediate fields of K/F (including K, F) is the number of divisors of n.

Remark.

- An analogue of the fundamental theorem of Galois theory also holds for infinite Galois extensions.
- In fact Krull defined a topology on $\mathrm{Gal}(K/F)$ by taking as a fundamental system of open neighbourhoods of the identity the set of subgroups belonging to finite extensions of F contained in K.
- The closed subgroups are precisely those subgroups which are of the type $\mathrm{Gal}(K/L)$ where L runs over intermediate fields between K and F.

Definition. Let K be a finite extension of a finite field F consisting of q elements. The mapping σ defined on K by $\sigma(\alpha) = \alpha^q$, $\alpha \in K$ is clearly an F-automorphism of K. It is called the Frobenius automorphism of K/F.

With K/F as in the above definition, we shall prove below that its Frobenius automorphism generates the Galois group of K/F.

Proposition 43. Let K/F be an extension of finite fields. Then $\mathrm{Gal}(K/F)$ is a cyclic group generated by the Frobenius automorphism of K/F.

Proof of Proposition 43.

- Let K/F be an extension of degree n with $|F| = q$.
- Then $|\mathrm{Gal}(K/F)| = n$ by the fundamental theorem of Galois theory.
- Consider the map $\sigma : K \longrightarrow K$ defined by $\sigma(\alpha) = \alpha^q$, $\alpha \in K$.
- It is easily checked that σ is an F-automorphism of K.
- Its powers $\sigma^0, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ are distinct because otherwise σ^i is the identity map for some $i,\ 0 < i < n$ and consequently $\alpha^{q^i} = \alpha$ for each α in K which is impossible as the polynomial $x^{q^i} - x$ can't have more roots than its degree.
- Thus $\mathrm{Gal}(K/F)$ is a cyclic group generated by σ.

Definition. Let $g(x)$ be a monic polynomial without repeated roots having coefficients in a field F. Let $\alpha_1, ..., \alpha_m$ be all the roots of $g(x)$ in its splitting field. In view of Corollary 25 and Theorem 30, $F(\alpha_1, ..., \alpha_m)$ is a Galois extension of F. Its Galois group is called the Galois group of $g(x)$ over F. This group is also called the Galois group of the equation $g(x) = 0$ over F.

Example. Let m be an integer with $|m| > 1$ which is not divisible by the cube of any prime number. Then we show that the Galois group of the polynomial $g(x) = x^3 - m$ over $\mathbb{Q}$ is isomorphic to the symmetric group S_3 of degree 3. It can be easily seen that $g(x)$ is irreducible over $\mathbb{Q}$. Note that the splitting field K of $g(x)$ over $\mathbb{Q}$ is $\mathbb{Q}(\theta, \omega)$, where θ is a root of $g(x)$ and $\omega \neq 1$ is a cube root of unity. Hence $[K : \mathbb{Q}] = 6$. So the Galois group of $g(x)$ over $\mathbb{Q}$ is either abelian or isomorphic to S_3. But this group can not be abelian in view of Corollary 41, because the subextension $\mathbb{Q}(\theta)/\mathbb{Q}$ is not normal. Therefore $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to S_3.