2

Galois Theory

Structure

2.1. Introduction.

2.2. Normal Extension.

2.3. F-Automorphism.

2.4. Galois Extension.

2.5. Norms and Traces.

2.6. Check Your Progress.

2.7. Summary.

2.1. Introduction. In this chapter, we shall discuss about normal extensions, fixed fields, Galois extensions, norms, traces and the dependence of all these on normal extensions.

2.1.1. Objective. The objective of these contents is to provide some important results to the reader like:

(i) Normal Extensions.

(ii) Fixed Fields, Galios Groups

(iii) Norms and Traces.

2.1.2. Keywords. Normal Extensions, Galois Group, Fixed Fields.

2.3. Normal Extension. An algebraic extension K of F is said to be normal extension of F if each irreducible polynomial f(x) over F having a root in K splits into linear factors over K, that is, if one root is in K, then all the roots are in K.

If E is the splitting field of f(x) over F such that a root ‘a’ of f(x) is in K, then $E \subseteq K$.

2.3.1. Lemma. Let [K : F] = 2, then K is normal extension of F always.

Proof. Let $g(x) \in F[x]$ be any irreducible polynomial over F. Let α be a root of f(x) and $\alpha \in K$. Now, we have

$$[F(\alpha):F] \leq [K:F] = 2 \quad \Rightarrow \quad [F(\alpha):F] \leq 2 \quad \Rightarrow \quad \deg f(x) \leq 2.$$

If degf(x) = 1, then let

f(x) = ax+b with $a, b \in F, a \neq 0$.

Then, $0 = f(\alpha) = a\alpha + b \quad \Rightarrow \quad \alpha = -\frac{b}{a}, a \neq 0$.

But $-\frac{b}{a} \in F \subseteq K \quad \Rightarrow \quad \alpha \in K$.

If degf(x) = 2, then let f(x) = ax^2+bx+c with $a \neq 0$. If α be a root of f(x), then,

$$f(x) = (x-\alpha)(x+\alpha+\frac{b}{a}), \quad a \in K$$

$\Rightarrow \quad -(\alpha + \frac{b}{a})$ is other root of f(x).

Since $\frac{b}{a} \in F \subseteq K$ and $\alpha \in K \quad \Rightarrow \quad -(\alpha+\frac{b}{a}) \in K$.

Hence K is a normal extension of F.

2.3.2. Theorem. Let K be a finite algebraic extension of a field F then K is a normal extension of F iff K is the splitting field of some non-zero polynomial over F.

Proof. Let K = $F(a_1, a_2, \ldots, a_n)$ be a finite algebraic extension of F. Suppose K is normal extension of F. For each $a_i \in K$, let $f_i(x)$ be the minimal polynomial of a_i over F. Since K is normal extension of F, so $f_i(x)$ splits completely into linear factors over K.

Let f(x) = $f_1(x)f_2(x)\ldots f_n(x)$.

Let 'a' be any root of f(x), then 'a' is also a root of some $f_i(x)$ and hence $a \in K$. Let E be the splitting field of f(x). Then, $E \subseteq K$.

Now, $F(a_i) = \prod_{j=1}^{n} f_j(a_i) = 0$. Therefore, a_i is a root of f(x), that is, $a_i \in E$.

Therefore, $F(a_1, a_2, ..., a_n) \subseteq E \quad \Rightarrow \quad K \subseteq E$.

Thus, K = E.

Hence K is the splitting field of f(x) over F.

Conversely, let K be the splitting field of some non-zero polynomial f(x) over F. Let $a_1, a_2, \ldots, a_n$ be the roots of f(x). Then, K = F($a_1, a_2, \ldots, a_n$).

By definition, $[K:F] \leq n!$.

So, K is finite algebraic extension of F. Let p(x) be any irreducible polynomial over F with a root β in K. p(x) is also a polynomial over K with $(x-\beta)$ as a factor in K[x]. So p(x) is not irreducible over K.

Let L be the splitting field of p(x) over K. We claim that L=K.

Let, if possible, $L \neq K$. Then, there exists a root β' of p(x) in L such that $\beta' \notin K$. As β and β' are conjugates over F, there exists an isomorphism $\sigma : F(\beta) \to F(\beta')$ such that $\sigma(\beta) = \beta'$ and $\sigma(\lambda) = \lambda$ for every λ in F. Now, $F \subseteq F(\beta) \subseteq K$ gives K is a splitting field of f(x) over $F(\beta)$.

Further, $K(\beta') = F(a_1, a_2, ..., a_n)(\beta') = F(\beta')(a_1, a_2, ..., a_n)$ gives $K(\beta')$ is a splitting field of f(x) over $F(\beta')$. Then, there exists an isomorphism $\tau : K \to K(\beta')$ such that

$$\tau(x) = \sigma(x) \text{ for every x in } F(\beta).$$

But then $\tau(\beta) = \sigma(\beta) = \beta'$ and $\tau(\lambda) = \sigma(\lambda) = \lambda$ for every λ in F.

Hence $\tau : K \to K(\beta')$ is an onto isomorphism, such that $\tau(\beta) = \beta'$ and $\tau(\lambda) = \lambda$ for every λ in F. If

$$f(x) = \alpha_0 + \alpha_1 x + ... + \alpha_{n-1} x^{n-1} + \alpha_n x^n$$

in F[x] with $\alpha_n \neq 0$. Then,

$$f(x) = \alpha_n (x - a_1)(x - a_2)...(x - a_n)$$

Let $\tau' : K[x] \to K(\beta')[x]$ be an extension of τ such that

$$\begin{aligned}\tau'(f(x)) &= \tau'(\alpha_0 + \alpha_1 x + ... + \alpha_{n-1} x^{n-1} + \alpha_n x^n) = \tau'(\alpha_0) + \tau'(\alpha_1) x + ... + \tau'(\alpha_{n-1}) x^{n-1} + \tau'(\alpha_n) x^n \\ &= \tau(\alpha_0) + \tau(\alpha_1) x + ... + \tau(\alpha_{n-1}) x^{n-1} + \tau(\alpha_n) x^n = \alpha_0 + \alpha_1 x + ... + \alpha_{n-1} x^{n-1} + \alpha_n x^n \\ &= f(x)\end{aligned}$$

Also,

$$\begin{aligned}\tau'(f(x)) &= \tau'(\alpha_n (x - a_1)(x - a_2)...(x - a_n)) = \tau'(\alpha_n) \tau'(x - a_1) \tau'(x - a_2)...\tau'(x - a_n) \\ &= \alpha_n (x - \tau(a_1))(x - \tau(a_2))...(x - \tau(a_n))\end{aligned}$$

We get that $\tau(a_1), \tau(a_2), ..., \tau(a_n)$ are also roots of f(x). Since τ is one-one, so

$$\{\tau(a_1), \tau(a_2), ..., \tau(a_n)\} = \{a_1, a_2, ..., a_n\}$$

It implies τ permutes the roots of f(x). Therefore,

$$K = F(a_1, a_2, ..., a_n) = F(\tau(a_1), \tau(a_2), ..., \tau(a_n))$$

However,

$$K(\beta') = \tau(K) = \tau\left(F(a_1, a_2, ..., a_n)\right) = F(\tau(a_1), \tau(a_2), ..., \tau(a_n)) = F(a_1, a_2, ..., a_n) = K$$

It implies $\beta' \in K$, which is a contradiction.

Thus, L = K, so p(x) splits completely over K. Hence K is a normal extension of F.

2.3.3. Corollary. Let K be a finite normal extension of F. If E be any subfield of K such that $F \subseteq E \subseteq K$, then K is normal extension of E.

Proof. Since *K* is a finite normal extension of *F*, so there exist a polynomial *f*(*x*) over *F* such that *K* is splitting field of *f*(*x*) over *F*. Then *K* is also a splitting field of *f*(*x*) over *E*. Hence by above theorem *K* is normal extension of *E*.

2.3.4. Corollary. Let K be finite normal extension of F. If α_1 and α_2 be any two elements in K conjugate over F, then there exists an F automorphism σ of K such that $\sigma(\alpha_1) = \alpha_2$.

Proof. Let *K* be the splitting field of the non-zero polynomial *f*(*x*) over *F*. Since α_1, α_2 are conjugates over *F* there exist an isomorphism σ such that $\sigma : F(\alpha_1) \to F(\alpha_2)$ defined by

$$\sigma(\alpha_1) = (\alpha_2) \text{ and } \sigma(\lambda) = \lambda \text{ for all } \lambda \in F.$$

Now $[F(\alpha_1) : F] = [F(\alpha_2) : F]$ = degree of minimal polynomial of α_1 (or α_2).

Now , $f(x) \in F[x] \subseteq F(\alpha_1)[x]$ and $f(x) \in F[x] \subseteq F(\alpha_2)[x]$

Therefore, *K* is splitting field of $f(x)$ over $F(\alpha_1)$ as well as $F(\alpha_2)$.

Then there exists $\Psi : K \to K$ s.t. $\Psi(\alpha) = \sigma(\alpha)$ for all $\alpha \in F(\alpha_1)$ and $\Psi(\lambda) = \sigma(\lambda) = \lambda$ for all $\lambda \in F$. Then $\Psi(\alpha_1) = \sigma(\alpha_1) = \alpha_2$. Hence Ψ is an *F*-automorphism of *K* such that $\Psi(\alpha_1) = \alpha_2$.

Remark. Converse of Corollary 1 need not be true, for if $F = Q, E = Q(\sqrt{2})$ and $K = Q(\sqrt[4]{2})$. Then K is normal extension of E, E is normal extension of F but K is not a normal extension of F.

2.3.5. M(S, K). Let K be any field and S be any non-empty set.The set of all mappings from S to K is denoted by M(S, K).

2.3.6. Theorem. If $\sigma_1, \sigma_2, ..., \sigma_n$ be any n monomorphisms in M(E, K), then these are always L.I., where E and K are fields.

Proof. If n = 1, then consider σ_1 and let, for $a_1 \in K$

$$a_1\sigma_1 = \bar{0} \quad \Rightarrow \quad a_1\sigma_1(\alpha) = 0 \text{ for all } \alpha \in \mathrm{E}$$

Since $a_1\sigma_1$ is a homomorphism from E to K and

$$a_1\sigma_1(\alpha) = 0 \text{ for all } \alpha \in \mathrm{E}$$

In particular, $\left(a_1\sigma_1\right)(1) = 0$ where $1 \in \mathrm{E} \quad \Rightarrow \quad \left(a_1\right)\sigma_1(1) = 0$.

Since σ_1 is a monomorphism so $\sigma_1(1) \neq 0$, then $a_1 = 0$.

Hence σ_1 is linearly independent.

Now, let us assume, as our induction hypothesis, that $\sigma_1, \sigma_2, ..., \sigma_{n-1}$ are L.I.

We have to prove that $\sigma_1, \sigma_2, ..., \sigma_n$ are L.I.

Let $\lambda_1, \lambda_2, ..., \lambda_n$ are scalars such that

$$\lambda_1\sigma_1 + \lambda_2\sigma_2 + ... + \lambda_n\sigma_n = \bar{0} \qquad ...(1)$$

If any of λ_i is zero, then the above relation reduces to a combination of (n - 1) σ_i's and by induction hypothesis, all λ_i's are zero. Hence we assume that $\lambda_1, \lambda_2, ..., \lambda_n$ are all non-zero.

So, let W.L.O.G., $\lambda_n \neq 0$. Then dividing (1) by λ_n, we have

$$b_1\sigma_1 + b_2\sigma_2 + ... + b_{n-1}\sigma_{n-1} + \sigma_n = \bar{0} \qquad ...(2)$$

where $b_i = \dfrac{\lambda_i}{\lambda_n} = \lambda_i \lambda_n^{-1}$.

Since σ_1 and σ_n are distinct, so there exists an element $x_1 \in E$ such that

$$\sigma_1(x_1) \neq \sigma_n(x_1)$$

Then, clearly $x_1 \neq 0$, since image of 0 is 0 for any homomorphism.

Now, let $x \in E$ be any element then $xx_1 \in E$ also. Compute

$$\left(b_1\sigma_1 + b_2\sigma_2 + ... + b_{n-1}\sigma_{n-1} + \sigma_n\right)\left(xx_1\right) = \bar{0}\left(xx_1\right) = 0$$

$$\Rightarrow \quad b_1\sigma_1\left(xx_1\right) + b_2\sigma_2\left(xx_1\right) + ... + b_{n-1}\sigma_{n-1}\left(xx_1\right) + \sigma_n\left(xx_1\right) = 0$$

$$\Rightarrow \quad b_1\sigma_1\left(x\right)\sigma_1\left(x_1\right) + b_2\sigma_2\left(x\right)\sigma_2\left(x_1\right) + ... + b_{n-1}\sigma_{n-1}\left(x\right)\sigma_{n-1}\left(x_1\right) + \sigma_n\left(x\right)\sigma_n\left(x_1\right) = 0$$

Since $\sigma_n(x_1) \neq 0$, so dividing above equation by $\sigma_n(x_1)$.

$$b_1\frac{\sigma_1\left(x_1\right)}{\sigma_n\left(x_1\right)}\sigma_1\left(x\right) + b_2\frac{\sigma_2\left(x_1\right)}{\sigma_n\left(x_1\right)}\sigma_2\left(x\right) + ... + b_{n-1}\frac{\sigma_{n-1}\left(x_1\right)}{\sigma_n\left(x_1\right)}\sigma_{n-1}\left(x\right) + \sigma_n\left(x\right) = 0 \qquad ...(*)$$

From (2), we also have

$$b_1\sigma_1(x) + b_2\sigma_2(x) + ... + b_{n-1}\sigma_{n-1}(x) + \sigma_n(x) = 0 \qquad ...(**)$$

Subtracting (**) from (*), we get

$$b_1\left(\frac{\sigma_1(x_1)}{\sigma_n(x_1)}-1\right)\sigma_1(x)+b_2\left(\frac{\sigma_2(x_1)}{\sigma_n(x_1)}-1\right)\sigma_2(x)+\ldots+b_{n-1}\left(\frac{\sigma_{n-1}(x_1)}{\sigma_n(x_1)}-1\right)\sigma_{n-1}(x)=0 \quad \ldots(3)$$

Since $\sigma_1(x_1)\neq\sigma_n(x_1) \Rightarrow \dfrac{\sigma_1(x_1)}{\sigma_n(x_1)}\neq 1 \Rightarrow \dfrac{\sigma_1(x_1)}{\sigma_n(x_1)}-1\neq 0$

Now as above equation (3) holds for every $x\in E$, so

$$b_1\left(\frac{\sigma_1(x_1)}{\sigma_n(x_1)}-1\right)\sigma_1+b_2\left(\frac{\sigma_2(x_1)}{\sigma_n(x_1)}-1\right)\sigma_2+\ldots+b_{n-1}\left(\frac{\sigma_{n-1}(x_1)}{\sigma_n(x_1)}-1\right)\sigma_{n-1}=0$$

which is a combination of (n-1) σ_i 's. So, we get

$$b_1\left(\frac{\sigma_1(x_1)}{\sigma_n(x_1)}-1\right)=b_2\left(\frac{\sigma_2(x_1)}{\sigma_n(x_1)}-1\right)=\ldots=b_{n-1}\left(\frac{\sigma_{n-1}(x_1)}{\sigma_n(x_1)}-1\right)=0$$

Now, as $\dfrac{\sigma_1(x_1)}{\sigma_n(x_1)}-1\neq 0$, so $b_1 = 0$ and so $\dfrac{\lambda_1}{\lambda_n}=0$, which implies $\lambda_1=0$, a contradiction.

Hence any set of n monomorphism is linearly independent.

2.3.7. Definition. Let K be any field, then the set of all automorphisms on K is denoted by AutK.

2.3.8. Corollary. AutKconsists of linearly independent elements.

Take E = K in above theorem, the result follows.

2.3.9. Exercise. The set of all automorphisms of K form a group under composition of mappings.

2.4. F-Automorphisms. Let F be any field and K be any extension of F. An automorphism $\sigma: K\to K$ is called F-automorphism of K if

$$\sigma(x)=x \text{ for all } x\in F.$$

Notation. G(K, F) will denote the group of all F-automorphisms of K. G(K, F) is called Galio's group of K over F and known as group of automorphisms from K to K which fixes F.

2.4.1. Exercise. Prove that G(K, F) is a subfield of AutK.

2.4.2. Theorem. If P is a prime subfield of K, then prove that AutK = G(K, P), that is every automorphism on K fixes P.

Proof. Let $\sigma \in \text{Aut}(K)$ then $\sigma(0) = 0$ and $\sigma(1) = 1$

Case 1. Char$K = P$ for some prime p.

Then $P \cong Z_p = \{0, 1, \ldots\ldots, p-1\}$. If $\alpha \in Z_p$ then $\alpha = 1+1+\ldots\ldots+1$ (α times)

$$\sigma(\alpha) = \sigma(1+1+\ldots\ldots+1) = \sigma(1)+\sigma(1)+\ldots\ldots+\sigma(1) = 1+1+\ldots\ldots+1 = \alpha$$

$\Rightarrow \quad \sigma(\alpha) = \alpha$ for all $\alpha \in Z_p$. $\Rightarrow$ σ fixes P.

$\Rightarrow \quad \sigma \in G(K, P) \Rightarrow \text{Aut}\, K \subseteq G(K, P)$.

Case 2. Char$K$ = 0.

Then $P \cong Q = \{mn^{-1} : m\, n \in Z\}$ and

$$\sigma(mn^{-1}) = \sigma(m)\,\sigma(n^{-1}) = \sigma(m)\left(\sigma(n)\right)^{-1} = mn^{-1} \text{ for all } mn^{-1} \in Q$$

$\Rightarrow \quad \sigma$ fixes P. $\quad \Rightarrow \quad \sigma \in G(K, P) \quad \Rightarrow \quad$ Aut $K \subseteq G(K, P)$.

So, in both cases, we get Aut $(K) \subseteq G(K, P)$. But $G(K, P) \subseteq$ Aut (K) always.

So Aut $(K) = G(K, P)$.

2.4.3. Theorem. Let K be any extension of F and $\sigma \in G(K,F)$. If 'a' is an element which is algebraic over F then 'a' and '$\sigma(a)$' are conjugates over F.

Proof. We know that $G(K, F) = \{ \sigma \in \text{Aut } K : \sigma(\lambda) = \lambda \text{ for all } \lambda \in F \}$.

Let $a \in K$ be an algebraic element over F. So let $f(x) = \lambda_0 + \lambda_1 x + ... + x^n$ be the minimal polynomial of 'a' over F and then $0 = f(a) = \lambda_0 + \lambda_1 a + ... + a^n \in K$ also, since $a, \lambda_0, \lambda_1, ... \in K$.

Now, $\quad 0 = \sigma(0) = \sigma\left(f(a)\right) = \sigma(\lambda_0 + \lambda_1 a + ... + a^n)$

$$= \sigma(\lambda_0) + \sigma(\lambda_1)\,\sigma(a) + ... + \sigma(a^n)$$

$$= \lambda_0 + \lambda_1 \sigma(a) + ... + \left(\sigma(a)\right)^n = f\left(\sigma(a)\right)$$

$\Rightarrow \quad f\left(\sigma(a)\right) = 0$, so $\sigma(a)$ is also a root of $f(x)$

$\Rightarrow \quad \sigma(a)$ is conjugate of 'a' over F.

2.4.4. Exercise. Let G be a group of automorphisms of a field K. Then, the set $F_0 = \{x \in K : \sigma(x) = x \text{ for all } \sigma \in G\}$ is a subfield of K.

Also, this subfield is known as **fixed field under G**.

2.4.5. Example. Let $K = Q\left(\sqrt[3]{2}\right)$. The minimal polynomial of $\sqrt[3]{2}$ over Q is $x^3 - 2$. It has only one root, namely, $\sqrt[3]{2}$ in K. Since K is a field of real numbers. Let σ be any Q – automorphisms of K. Then $\sigma\left(\sqrt[3]{2}\right) \in K$ is a root of $x^3 - 2$. So, $\sigma\left(\sqrt[3]{2}\right) = \sqrt[3]{2}$. Let x be any element of K, then x can be expressed as:

$$a + \sqrt[3]{2}b + \left(\sqrt[3]{2}\right)^2 c, \text{ where } a, b, c \in Q.$$

So, $\sigma(x) = \sigma(a) + \sigma(\sqrt[3]{2})\sigma(b) + \sigma\left(\left(\sqrt[3]{2}\right)^2\right)\sigma(c) = a + \sqrt[3]{2}b + \left(\sqrt[3]{2}\right)^2 c = x$

$\Rightarrow \quad \sigma = I$. Thus, AutK = { I }.

Hence in this case K itself is the fixed field under AutK.

2.4.6. Theorem. Let G be a finite subgroup of AutK. If F_0 is fixed subfield under G, that is, $F_0 = \{x \in K : \sigma(x) = x \text{ for all } \sigma \in G\}$. Then, [K : F_0] = o(G).

Proof. Let [K : F_0] = m and o(G) = n.

Let, if possible, m < n.

Let $\sigma_1, \sigma_2, ..., \sigma_n$ are elements of G and let {x_1, x_2, . . . , x_m} be a basis of K over F_0.

Consider a system of m linear homogeneous equations, $1 \le j \le m$

$$\sigma_1(x_j)u_1 + \sigma_2(x_j)u_2 + ... + \sigma_n(x_j)u_n = 0 \qquad \text{...(1)}$$

Note that $\sigma_1(x_j), \sigma_2(x_j), ..., \sigma_n(x_j)$ are elements of K and u_1, u_2, . . . , u_n are variables.

Since the number of equations is less that the number of variables, so the system (1) has a non-trivial solution, say, y_1, y_2, . . . , y_n, here not all y_i's are zero.

$$\sigma_1(x_j)y_1 + \sigma_2(x_j)y_2 + ... + \sigma_n(x_j)y_n = 0 \qquad \text{...(2)}$$

for j = 1, 2, … , m.

Now, if $x \in K$, then

$$x = \alpha_1 x_1 + \alpha_2 x_2 + ... + \alpha_n x_n, \text{ where } \alpha_i \in F_0.$$

Multiplying j[th] equation of (2) by α_j, we get

$$\sigma_1(x_j)y_1\alpha_j + \sigma_2(x_j)y_2\alpha_j + ... + \sigma_n(x_j)y_n\alpha_j = 0$$

$$\Rightarrow \quad \sigma_1(x_j)\ \sigma_1(\alpha_j)y_1 + \sigma_2(x_j)\sigma_2(\alpha_j)y_2 + ... + \sigma_n(x_j)\sigma_n(\alpha_j)y_n = 0$$

because $\alpha_j \in F_0$ and $\sigma_j \in G$ and F_0 is fixed under G.

$$\Rightarrow \quad \sigma_1(\alpha_j x_j)\ y_1 + \sigma_2(\alpha_j x_j)y_2 + ... + \sigma_n(\alpha_j x_j)y_n = 0 \text{ for j = 1, 2, …, m.}$$

Thus, we have the system of equations,

$$\sigma_1(\alpha_1 x_1)\ y_1 + \sigma_2(\alpha_1 x_1)y_2 + ... + \sigma_n(\alpha_1 x_1)y_n = 0$$
$$\sigma_1(\alpha_2 x_2)\ y_1 + \sigma_2(\alpha_2 x_2)y_2 + ... + \sigma_n(\alpha_2 x_2)y_n = 0$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\sigma_1(\alpha_m x_m)\ y_1 + \sigma_2(\alpha_m x_m)y_2 + ... + \sigma_n(\alpha_m x_m)y_n = 0$$

Adding all these equations, we get

$$\sigma_1(\alpha_1 x_1 + \alpha_2 x_2 + ... + \alpha_m x_m)\ y_1 + \sigma_2(\alpha_1 x_1 + \alpha_2 x_2 + ... + \alpha_m x_m)y_2$$
$$+ ... + \sigma_n(\alpha_1 x_1 + \alpha_2 x_2 + ... + \alpha_m x_m)y_n = 0$$

$$\Rightarrow \quad \sigma_1(x)\ y_1 + \sigma_2(x)y_2 + ... + \sigma_n(x)y_n = 0 \qquad \text{for all } x \in E$$

$\Rightarrow \quad (y_1\sigma_1 + y_2\sigma_2 + ... + y_n\sigma_n)(x) = 0 \quad$ for all $x \in E$

$\Rightarrow \quad y_1\sigma_1 + y_2\sigma_2 + ... + y_n\sigma_n = \bar{0}$

where atleast one of $y_j \neq 0$.

Hence $\sigma_1, \sigma_2, ..., \sigma_n$ are L.D. over K, a contradiction.

Thus, $m \nless n$.

Now, if possible, suppose that m > n.

Then, there exist (n + 1) L.I. elements, say $x_1, x_2, \dots, x_{n+1}$ in K over F_0. Consider the system of n linear homogeneous equations in (n+1) variables

$$\sigma_j(x_1)u_1 + \sigma_j(x_2)u_2 + ... + \sigma_j(x_{n+1})u_{n+1} = 0 \qquad \dots(3)$$

for j = 1,2,…n.

Since the number of variables is again greater than the number of equations, so these homogeneous equations have a non-trivial solution. Let $z_1, z_2, \dots, z_{n+1}$ be a non-trivial solution of the system (3). Let r be the smallest non-zero integer such that $z_j = 0$ for all $j \geq r+1$.

Then, the system (3) reduces to

$$\sigma_j(x_1)z_1 + \sigma_j(x_2)z_2 + ... + \sigma_j(x_r)z_r = 0 \qquad \dots(4)$$

Since $z_r \neq 0$ and $z_r \in K$. Consider, $z_i^l = \dfrac{z_i}{z_r}$. Then, from (4), we get

$$\sigma_j(x_1)z_1^l + \sigma_j(x_2)z_2^l + ... + \sigma_j(x_{r-1})z_{r-1}^l + \sigma_j(x_r) = 0 \qquad \dots(5)$$

for j = 1,2,…n.

Let for j = 1, $\sigma_1 = I$, we get from (5), that

$$x_1z_1^l + x_2z_2^l + ... + x_{r-1}z_{r-1}^l + x_r = 0 \qquad \dots(6)$$

If all $z_1^l, z_2^l, ..., z_{r-1}^l$ are in F_0, then from (6), we get that $x_1, x_2, \dots, x_r$ are L.D. over F_0, which is not possible.

Hence atleast one of z_i^l is not in F_0, say $z_1^l \notin F_0$.

Further, we get that $r \neq 1$, because if r = 1, then we get that $z_1^l = 1$ and so $z_1^l \in F_0$.

Since $z_1^l \notin F_0$, so there exists some $\sigma_i \in G$ such that $\sigma_i(z_1^l) \neq z_1^l$.

Applying $\sigma_i \in G$ to (5), to get

$$\sigma_i(\sigma_j(x_1)z_1^l) + \sigma_i(\sigma_j(x_2)z_2^l) + ... + \sigma_i(\sigma_j(x_{r-1})z_{r-1}^l) + \sigma_i(\sigma_j(x_r)) = 0$$

$$\Rightarrow \quad \sigma_i\sigma_j(x_1)\sigma_i(z_1^l) + \sigma_i\sigma_j(x_2)\sigma_i(z_2^l) + ... + \sigma_i\sigma_j(x_{r-1})\sigma_i(z_{r-1}^l) + \sigma_i\sigma_j(x_r) = 0$$

Since G is a group, the set $\{\sigma_i\sigma_1, \sigma_i\sigma_2, ..., \sigma_i\sigma_n\}$ coincide with the set $\{\sigma_1, \sigma_2, ..., \sigma_n\}$, though the order of elements will be different. So, we get

$$\sigma_j(x_1)\sigma_i(z_1^l) + \sigma_j(x_2)\sigma_i(z_2^l) + ... + \sigma_j(x_{r-1})\sigma_i(z_{r-1}^l) + \sigma_j(x_r) = 0 \quad \dots(7)$$

Subtracting (7) from (5), we have

$$\sigma_j(x_1)\left[z_1^l - \sigma_i(z_1^l)\right] + \sigma_j(x_2)\left[z_2^l - \sigma_i(z_2^l)\right] + ... + \sigma_j(x_{r-1})\left[z_{r-1}^l - \sigma_i(z_{r-1}^l)\right] = 0$$

Put $t_k = z_k^l - \sigma_i(z_k^l)$. Then, the above system becomes

$$\sigma_j(x_1)t_1 + \sigma_j(x_2)t_2 + ... + \sigma_j(x_{r-1})t_{r-1} = 0$$

where $t_1 \neq 0$. Thus, $(t_1, t_2, \ldots, t_{r-1}, 0, 0, \ldots, 0)$ is a non-trivial solution of given system, which is a contradiction to the choice of r. Therefore, $n \not< m$

So, m = n. Hence the proof.

2.5. Galois Extension. A finite extension K of a field F is said to be Galoi's extension of F if F is the fixed subfield of K under the group G(K, F) of all F-automorphisms of K i.e. K/F is Galoi's extension if $K_{G(K,F)} = F$.

2.5.1. Simple Extension. An extension K/F is said to be simple extension if K is generated by a single element over F.

2.5.2. Corollary. Let $K = F(\alpha)$ be a simple finite separable extension of F. Then, K is the splitting field of the minimal polynomial of α over F iff F is the fixed field under the group of all F-automorphisms of K, that is K is Galoi's extension of F.

Proof : Let $f(x)$ be the minimal polynomial of α over F and let degree $f(x) = m$.

Then $[K : F] = m$. Let $\alpha_1 = \alpha, \alpha_2, \alpha_3, \ldots, \alpha_r$ be the distinct conjugates of α in K.

Then $K = F(\alpha_i)$ for all $i = 1, 2, \ldots, r$. Since α and α_i are conjugates over F, so $\exists$ an isomorphism, say $\sigma_i : F(\alpha_1) \to F(\alpha_i)$ given by $\sigma_i(\alpha_1) = \alpha_i$ and $\sigma_i(\lambda) = \lambda$ for all $\lambda \in F$. But $K = F(\alpha_i)$ for all i, so we have that

$$\sigma_i : K \to K \text{ s.t. } \sigma_i(\alpha_1) = \alpha_i \text{ and } \sigma_i(\lambda) = \lambda \text{ for all } \lambda \in F.$$

Since α_1 generates K over F, each σ_i is uniquely determined. Further, we know for any F-automorphism σ of K, $\sigma_i(\alpha_1)$ is a conjugate of α_1 and hence $\sigma_i(\alpha_1) = \alpha_i$ for some α_i.

From this, it follows that $\sigma = \sigma_i$ for some i.

Hence the group $G(K, F)$ consists of $\sigma_1, \sigma_2, \ldots, \sigma_r$. Let F_0 be the fixed field under $G(K, F)$. Then by theorem 2.4.6.,

$$[K : F_0] = o[G(K, F)] = r.$$

So , $F = F_0$ if and only if $r = m$. Hence F is the fixed field under G if and only iff $f(x)$ has all m roots in K, that is, if and only if K is the splitting field of $f(x)$ over F.

2.5.3. Theorem. Let K be a finite extension of F and ch.F = 0. Then, K is normal extension of F iff the fixed field under G(K, F) is F itself, that is, K is Galoi's extension of F.

Proof. We know that any finite field extension of a field of characteristic zero is simple extension so K/F is a simple extension. So , let $K = F(\alpha)$ for some $\alpha \in K$.

Now, suppose that K is a normal extension of F. Then, by definition, every irreducible polynomial over F having one root in K splits into linear factors over K. Since $[K : F]$ is finite , so α is algebraic over F. Let $f(x)$ be minimal polynomial of α over F and K' be its splitting field over F. Then $K' \subseteq K$. Also, $\alpha \in K'$, $F \subseteq K'$

$$\Rightarrow \quad K \subseteq K'.$$

So $K = K'$ i.e. K is splitting field of $f(x)$ over F. Hence, by corollary 2.5.2., F is itself fixed subfield under $G(K , F)$, that is, K/F is Galois extension.

Conversely, suppose that F is itself the fixed subfield under $G(K, F)$. Again, by corollary 2.5.2., K is the splitting field of the minimal polynomial of α over F. Further we know that if K is a finite algebraic extension of a field F iff K is the splitting field of some non-zero polynomial over F. Hence K is a normal extension of F.

2.5.4. Fundamental Theorem of Galoi's Theory.

Given any subfield E of K containing F and subgroup H of G(K, F)

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

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

(iii) [K : E] = o(G(K, E)) and [E : F] = index of G(K, E) in G(K, F)

(iv) E is a normal extension of F iff G(K, E) is a normal subgroup of G(K, F)

(v) when E is a normal extension of F, then

$$G(E,F) \cong G(K,F)/G(K,E).$$

Proof. (i) Since K is a finite normal extension of F and $F \subseteq E \subseteq K$, we must have that K is a finite normal extension of E. so, by above theorem fixed field under G(K, E) is E itself, that is E = G(K, E).

(ii) By definition, $K_H = \{x \in K : \sigma(x) = x \ \forall \ \sigma \in H\}$, that is each element of K_H remains invariant under every automorphisms of H. So, clearly, we have

$$H \subseteq G(K, K_H)$$

Now, we know that if F_0 is fixed subfield under subgroup G, then $[K : F_0] = o(G)$.

Here K_H is fixed subfield under H, so we must have $[K: K_H] = o(H)$ …(1)

Now, K is normal extension of K_H, so K_H is fixed subfield under G(K, K_H), by above theorem. So again we have

$[K : K_H] = o(G(K, K_H))$ …(2)

By (1) and (2), we obtain

$O(H) = o(G(K, K_H))$

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

(iii) Since K|F and K|E both are finite normal extensions, so by above theorem fixed field under G(K, F) and G(K, E) are F and E respectively.
Hence [K : E] = o(G(K, E)) and [K : F] = o(G(K, F))

Now, [K : F] = [K : E][E : F]

So $[E:F] = \frac{[K:F]}{[K:E]} = \frac{o(G(K:F))}{o(G(K:E))} =$ index of G(K, E) in G(K, F)

(iv) Let E be a normal extension of F. Then, E is algebraic extension of F. Let $a \in E$, then 'a' is algebraic over F. Let p(x) be the minimal polynomial of 'a' over F. Then, E|F being normal and E contains a root of p(x), then all roots of p(x) are in F.
Hence E contains all the conjugates of 'a' over F. Let $\sigma \in G(K, F)$, then $\sigma(a)$ is a conjugate of 'a' and hence $\sigma(a) \in E$.
Let $\eta \in G(K, E)$ then $\eta : K \to K$ such that $\eta(\lambda) = \lambda$ for all $\lambda \in E$. In particular,

$\eta(\sigma(a)) = \sigma(a)$ $[\sigma(a) \in E]$

$\Rightarrow \sigma^{-1}(\eta(\sigma(a))) = \sigma^{-1}\sigma(a) = a \Rightarrow (\sigma^{-1}\eta\sigma)(a) = a \Rightarrow \sigma^{-1}\eta\sigma \in G(K, E)$
Hence $G(K, E) \,\Delta\, G(K, F)$.
Conversely, let $G(K, E) \,\Delta\, G(K, F)$.
We shall prove that E is a normal extension of F.
Let $a \in E \subseteq K \Rightarrow a \in K$ and K is normal extension of F.
Therefore, K contains all the roots of minimal polynomial p(x) of 'a' over F. Equivalently, if L is the splitting field of p(x) over F, then $L \subseteq K$.
Let b be any other root of p(x), then $b \in L \subseteq K$ and b is a conjugate of 'a' over F. Hence there exists an isomorphism $\sigma : K \to K$ such that

$\sigma(a) = b$ and $\sigma(\lambda) = \lambda$ for all $\lambda \in F$

Let $\eta \in G(K, E)$, then $\sigma^{-1}\eta\sigma \in G(K, E)$. Therefore,

$\sigma^{-1}\eta\sigma(a) = a \Rightarrow \eta(\sigma(a)) = \sigma(a) \Rightarrow \eta(b) = b$ for all $\eta \in G(K, E)$

But E is fixed under G(K, E), therefore, we get

$b = \sigma(a) \in E \Rightarrow b \in E \Rightarrow L \subseteq E$

Thus, E is normal extension of F.
(v) Let E be a normal extension of F. Then, E = F(a) for some $a \in E$. For any $\sigma \in G(K, F)$, let σ_E denotes the restriction of σ to E. Since $\sigma(a) \in E$, we get $\sigma(E) \subseteq E$.

But $[\sigma(E):F]=[E:F]$. Therefore, we get $\sigma(E)=E$. Hence σ_E is an F-automorphism of E and so $\sigma_E \in G(E,F)$.

Define a mapping $\lambda : G(K,F) \to G(E,F)$ by setting

$$\lambda(\sigma)=\sigma_E \text{ for all } \sigma \in G(K,F)$$

Clearly, for any $\sigma, \eta \in G(K,F)$, we have

$$\lambda(\sigma\eta)=(\sigma\eta)_E=\sigma_E\eta_E=\lambda(\sigma)\lambda(\eta)$$

Hence λ is a group homomorphism.

Consider any $\gamma \in G(E,F)$. Now, $\gamma(a)$ is a conjugate of 'a' over F. Thus, there exists an F-automorphism σ on K such that $\sigma(a)=\gamma(a)$.

Further, as σ and η are both identity of F and E is generated by 'a' over F. We get

$$\sigma(x)=\gamma(x) \text{ for all } x \in F(a)=E \quad \Rightarrow \quad \gamma=\sigma_E=\lambda(\sigma)$$

This proves λ is onto mapping. Hence

$$G(E,F) \cong G(K,F)/Ker\lambda$$

Now, if $\lambda \in Ker\lambda$ iff σ_E is identity on E iff $\sigma(x)=x$ for all $x \in E$ iff $\sigma \in G(K,E)$.

Hence $Ker\lambda = G(K,E)$ and we obtain

$$G(E,F) \cong G(K,F)/G(K,E).$$

2.5.5. Example. Determining Galois group of splitting field of x^4+1 over Q.

Solution. Roots of x^4+1 over Q are

$$x = e^{\frac{(2m+1)\pi i}{4}}, \quad m = 0, 1, 2, 3$$

$$= e^{\frac{\pi i}{4}}, e^{\frac{3\pi i}{4}}, e^{\frac{5\pi i}{4}}, e^{\frac{7\pi i}{4}}$$

Let $a = e^{\frac{\pi i}{4}}$,

Then roots are $x = a, a^3, a^5, a^7$

Therefore, splitting field K of x^4+1 over Q is given by

$$K = Q(a, a^3, a^5, a^7) = Q(a).$$

Clearly, x^4+1 is irreducible over Q, so it is minimal polynomial of x^4+1 over Q.

Now, $[K : Q] = [Q(a) : Q]$

= degree of minimal polynomial of 'a' over Q

= degree $(x^4+1) = 4$

Since K is splitting field of some non-zero polynomial over Q, so K must be normal extension of Q. Also, char$Q$ = 0, so we must have that the fixed field under the Galois group $G(K, Q)$ is Q itself.

So, we must have $o(G(K,Q)) = [K : Q] = 4$

Now , $K = Q(a)$ and $[K : Q] = 4$

so $\{1, a, a^2, a^3\}$ must be a basis of K over Q. If $y \in K$ be any arbitrary element, then

$$y = \alpha_0.1 + \alpha_1 . a + \alpha_2 . a^2 + \alpha_3 . a^3 \quad , \quad \alpha_i \in Q \, , \quad 0 \le i \le 3.$$

and $$\sigma(y) = \sigma(\alpha_0.1) + \sigma(\alpha_1 . a) + \sigma(\alpha_2 . a^2) + \sigma(\alpha_3 . a^3)$$

$$= \alpha_0 + \alpha_1 \sigma(a) + \alpha_2 (\sigma(a))^2 + \alpha_3 (\sigma(a))^3$$

Hence any $\sigma \in G(K , Q)$ is determined by its effect on 'a'.

Now, $\sigma(a)$ must be a conjugate of 'a' and $G(K, Q)$ contains four elements, so we must have

$G(K , Q) = \{\sigma_1 , \sigma_2 , \sigma_3 , \sigma_4\}$, where $\sigma_1(a) = a$, $\sigma_2(a) = a^3$, $\sigma_3(a) = a^5$, $\sigma_4(a) = a^7$.

Now, $G(K, Q)$ is a group of order four means that either it is a cyclic group of order 4 or it is isomorphic to Klein's group.

We observe that $\sigma_1(a) = a \quad \Rightarrow \quad \sigma_1 = I$ and $\sigma_2^2(a) = \sigma_2(\sigma_2(a)) = a^9 = a$

$$\sigma_3^2(a) = \sigma_3(\sigma_3(a)) = a^{25} = a \quad \text{and} \quad \sigma_4^2(a) = \sigma_4(\sigma_4(a)) = a^{49} = a$$

Hence, $$\sigma_2^2 = \sigma_3^2 = \sigma_4^2 = I.$$

So, the Galois group $G(K, Q)$ contains no element of order 4 which in turn implies that

$G(K, Q)$ is isomorphic to Klein's four group.

2.6. Norms and Traces.

Let E be a finite separable extension of degree n over the subfield F and K be a normal closure of E over F. Then, there are exactly n distinct F-monomorphisms, say, $\tau_i, 1 \le i \le n$, of E into K. Consider the mappings $N_{E/F}$ and $S_{E/F}$ of E into K as:

$$N_{E/F}(x) = \prod_{i=1}^{n} \tau_i(x) , \qquad S_{E/F}(x) = \sum_{i=1}^{n} \tau_i(x) ,$$

for every $x \in E$ and $1 \le i \le n$.

Then, $N_{E/F}(x)$ and $S_{E/F}(x)$ are known as norm and trace respectively of x from E to F.

The next theorem, indicates why to use "of x from E to F" in the definition of norm and trace.

2.6.1. Theorem. Norm, $N_{E/F}(x)$ is a homomorphism of the group $E^* = E - \{0\}$ of the field E into the group $F^* = F - \{0\}$ of the field F. Also, the trace $S_{E/F}$ is a non-zero homomorphism of the additive group E of the field E into the additive group F of F.

Proof. For justifying that these mappings are homomorphisms on the said structures, consider $x, y \in E$, then

$$N_{E/F}(xy) = \prod_{i=1}^{n} \tau_i(xy) = \prod_{i=1}^{n} \tau_i(x)\tau_i(y) = \prod_{i=1}^{n} \tau_i(x) \prod_{i=1}^{n} \tau_i(y) = N_{E/F}(x) N_{E/F}(y)$$

and,

$$S_{E/F}(x+y)=\sum_{i=1}^{n}\tau_i(x+y)=\sum_{i=1}^{n}\left(\tau_i(x)+\tau_i(y)\right)=\sum_{i=1}^{n}\tau_i(x)+\sum_{i=1}^{n}\tau_i(y)=S_{E/F}(x)+S_{E/F}(y)$$

Further, if τ is any F-automorphism of K, then, for $x \in E$, the mappings ρ_i, $1 \le i \le n$, of E into K defined by $\rho_i(x)=\tau(\tau_i(x))$ are clearly n distinct F- monomorphisms of E into K and so { $\rho_1,\rho_2,...,\rho_n$ } = { $\tau_1,\tau_2,...,\tau_n$ }, might be with different order. Let x be any arbitrary element of E, then

$$\tau\left(N_{E/F}(x)\right)=\tau\left(\prod_{i=1}^{n}\tau_i(x)\right)=\prod_{i=1}^{n}\tau\tau_i(x)=\prod_{i=1}^{n}\rho_i(x)=N_{E/F}(x)$$

and $$\tau\left(S_{E/F}(x)\right)=\tau\left(\sum_{i=1}^{n}\tau_i(x)\right)=\sum_{i=1}^{n}\tau\tau_i(x)=\sum_{i=1}^{n}\rho_i(x)=S_{E/F}(x).$$

Therefore, norm and trace of x belong to the fixed field under G(K,F). Since K is a normal closure of a seperable extension, so it is finite separable normal extension of F. Hence it follows that the fixed field under G(K,F) is F itself. Hence $N_{E/F}(x), S_{E/F}(x) \in F$.

Now, we only need to prove that $S_{E/F}$ is not the zero homomorphism. On the contrary assume that

$$S_{E/F}(x)=\sum_{i=1}^{n}\tau_i(x)=0, \qquad \text{for all } x \in E$$

However, it concludes that the set $\{\tau_1,\tau_2,...,\tau_n\}$ of distinct monomorphisms of E into K is linearly dependent over K, which in turn contradicts as we already have proved the result "If E and K be any two fields, then every set of distinct monomorphisms of E into K is linearly independent". Hence the proof.

Now consider two possibilities:

1. Let D be a finite separable extension of subfield F and E be a subfield of D, containing F. Then D is a separable extension of E and E is a separable extension of F. Thus if x is any element of D, define the norm $N_{D/E}(x)$ of x from D to E, which is an element of E as obtained in Theorem 1, and then define the norm of $N_{D/E}(x)$ from E to F, which is an element of F.
2. Also, define the norm of x from D to F.

The next theorem shows that these two procedures lead to the same element of F.

2.6.2. Theorem. Let D be a finite separable extension of a subfield F and E be a subfield of D containing F. Then, for every x $\in$ D,

i) $N_{E/F}(N_{D/E}(x)) = N_{D/F}(x)$

ii) $S_{E/F}(S_{D/E}(x)) = S_{D/F}(x)$.

Proof. Let K be a normal closure of D over F and [E : F] = n, [D : E] = m, then due to tower law, [D : F] = mn. Thus, there are exactly n distinct F-monomorphisms $\sigma_1,\ldots,\sigma_n$ (say) of E into K and m distinct E-monomorphisms $\tau_1, \ldots, \tau_m$ (say) of D into K. Extending $\sigma_1,\ldots,\sigma_n$ from E to K, we can obtain n distinct F-automorphisms $\sigma_1', \sigma_2', \ldots, \sigma_n'$ of K which act like $\sigma_1,\ldots,\sigma_n$ on E.

Let $\varphi_{ij}(i = 1,\ldots, n; j = 1,\ldots, m)$ be the mappings of D into K defined by

$$\varphi_{ij}(x) = \sigma_i'(\tau_j(x)) \text{ for all } x \in D.$$

These mn mappings are distinct F-monomorphisms of D into K and hence they form a complete set of F-monomorphisms of D into K. If $x \in D$, then we have

$$N_{D/F}(x) = \prod_{\substack{1\le i\le n \\ 1\le j\le m}} \phi_{ij}(x) = \prod_{\substack{1\le i\le n \\ 1\le j\le m}} \sigma_i'\left(\tau_j(x)\right) = \prod_{1\le i\le n} \sigma_i'\left(\prod_{1\le j\le m} \tau_j(x)\right)$$
$$= \prod_{1\le i\le n} \sigma_i'\left(N_{D/E}(x)\right) = \prod_{1\le i\le n} \sigma_i\left(N_{D/E}(x)\right) = N_{E/F}\left(N_{D/E}(x)\right)$$

Similarly, we can derive the result for traces also.

2.7. Check Your Progress.

1. Consider F = **Q** and E = **Q(i),** define norm and trace for this structure.
2. Find the Galois group of $x^3 - 2$ over Q.

2.8. Summary.

In this chapter, we have derived results related to normal extensions and observed that finite algebraic extension is normal if it becomes splitting field of a non-zero polynomial

Books Suggested:

1. Luther, I.S., Passi, I.B.S., Algebra, Vol. IV-Field Theory, Narosa Publishing House, 2012.
2. Stewart, I., Galios Theory, Chapman and Hall/CRC, 2004.
3. Sahai, V., Bist, V., Algebra, Narosa Publishing House, 1999.
4. Bhattacharya, P.B., Jain, S.K., Nagpaul, S.R., Basic Abstract Algebra (2nd Edition), Cambridge University Press, Indian Edition, 1997.
5. Lang, S., Algebra, 3rd editioin, Addison-Wesley, 1993.
6. Adamson, I. T., Introduction to Field Theory, Cambridge University Press, 1982.
7. Herstein, I.N., Topics in Algebra, Wiley Eastern Ltd., New Delhi, 1975.