3

Galois Fields

Structure

3.1. Introduction. In this chapter, we shall discuss about finite fields, cyclic and cyclotomic extensions. Also it will be derived that a field of composite order does not exist. Further, the relation between finite division rings and finite fields is obtained.

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

(i) Normal bases.

(ii) Cyclic and Cyclotomic Extensions.

(iii) Cyclotomic Polynomials.

3.1.2. Keywords. Galois Field, Normal Extensions, Splitting Fields.

3.2. Galois Field. A field is said to be Galois field if it is finite.

3.2.1. Theorem. Let F be a field having q elements and ch.F = p, where p is a prime number. Then, q = p^n for some integer $n \geq 1$.

Proof. Let P be the prime subfield of F. Now, we know that upto isomorphism there are only two prime fields, one is Q and other is Z_p. Since P is finite prime field. So, P must be isomorphic to Z_p. Hence P must have p elements. Now, F is a finite field and $P \subseteq F$ so F is a finite dimensional vector space over P.

Let [F : P] = n(say) and let $\{a_1, a_2, \ldots, a_n\}$ be a basis of F over P. Then, each element of F can be written uniquely as

$$\lambda_1 a_1 + \lambda_2 a_2 + ... + \lambda_n a_n \text{ where } \lambda_i \in P .$$

As each λ_i can be choosen in p ways, the total number of elements of F is p^n.

So, we have q = p^n for some integer $n \geq 1$.

Remark. In the other direction of above theorem, we shall show that for every prime p and integer $n \geq 1$, there exists a field having p^n elements. First we prove a lemma:

3.2.2. Lemma. If a field F has q elements, then F is the splitting field of $f(x) = x^q - x \in P[x]$, where P is the prime subfield of F.

Proof. We know that the set of all non-zero elements of a field form an abelian group w.r.t. multiplication. So, F* = F – {0} is a multiplicative abelian group. Now, we are given that o(F) = q. Therefore, o(F*) = q-1.

Now, let λ be an arbitrary element of F*. Then,

$$\lambda^{q-1} = 1$$

where 1 is the multiplicative identity of F. Thus,

$$\lambda\lambda^{q-1} = \lambda \quad \Rightarrow \quad \lambda^q = \lambda \quad \Rightarrow \quad \lambda^q - \lambda = 0$$

That is, λ satisfies the polynomial $f(x) = x^q - x$. Therefore, all the elements of F* are root of $f(x) = x^q - x$. Also, f(0) = 0 and so

$$f(\lambda) = 0 \quad \text{for all } \lambda \in \text{F}$$

Since f(x) is of degree q, so it cannot have more than q roots in any extension of P. Thus, F is the smallest extension of P containing all the roots of f(x).

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

Remark. In above lemma, we have proved that every finite field is splitting field of some non-zero polynomial.

3.2.3. Theorem. For every prime p and integer $n \geq 1$, there exists a field having p^n elements.

Proof. Since p is a prime number. Therefore, Z_p = {0, 1, …, p-1} is a field w.r.t. $+_p$ and x_p and is also a prime field. Consider the polynomial

$$f(x) = x^{p^n} - x \in Z_p[x]$$

Let K be the splitting field of f(x). Then, K contain all the roots of f(x).

Since degree of f(x) is p^n, so f(x) has p^n roots in K. Let these roots be $a_1, a_2, ..., a_{p^n}$. Then, we can write

$$x^{p^n} - x = \prod_{i=1}^{p^n}(x - a_i) \qquad \text{where } a_i \in K.$$

Let $T = \{a \in K : a^{p^n} = a\}$. Then, $T \neq 0$, because $0 \in T$ as $0^{p^n} = 0$ and $0 \in K$.

Now, $1 \in K$ and $1^{p^n} = 1 \quad \Rightarrow \quad 1 \in T$.

Let $k \in Z_p$ be any arbitrary element. Then, k = 1+1+…+1 (k-times). Therefore,

$$k^{p^n} = (1+1+...+1)^{p^n} = 1^{p^n} + 1^{p^n} + ... + 1^{p^n} = 1+1+...+1 = k \qquad [ch.F = p]$$

$$\Rightarrow \quad k \in T$$

So, every element of Z_p is in T, that is, T contains prime field Z_p of K. Further, consider a_i any root of f(x). Then,

$$f(a_i) = 0 \;\Rightarrow\; a_i^{p^n} - a_i = 0 \;\Rightarrow\; a_i^{p^n} = a_i \;\Rightarrow\; a_i \in T$$

Thus, T also contains all the roots of f(x).

We claim that T is a subfield of f(x).

Let $\alpha, \beta \in T$. Then, $\alpha^{p^n} = \alpha$ and $\beta^{p^n} = \beta$. Now,

$$(\alpha - \beta)^{p^n} = \alpha^{p^n} - \beta^{p^n} - 0 = \alpha - \beta \quad \Rightarrow \quad \alpha - \beta \in T$$

and $\quad (\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta \quad \Rightarrow \quad \alpha\beta \in T$.

Thus, T is a subfield of K. So, $T \subseteq K$.

So, we have T is a field which contains all the roots of f(x). But K is splitting field of f(x). So, $K \subseteq T$. Thus, we have K = T.

Now, if $\lambda \in T$, then $\lambda^{p^n} = \lambda \;\Rightarrow\; \lambda^{p^n} - \lambda = 0 \;\Rightarrow\; f(\lambda) = 0$

Thus, every element of T is a root of f(x).

Therefore, $T = \{a_1, a_2, ..., a_{p^n}\}$.

Now, we claim that all these elements are distinct.

We have $f(x) = x^{p^n} - x$. Any root a_i of f(x) is a multiple root of $f(x)$ iff a_i is a root of $f'(x)$. But

$$f'(x) = p^n x^{p^n - 1} - 1 = -1 \qquad \because ch.Z_p = p$$

So, a_i is not a root of $f'(x)$. Therefore, no root of f(x) is a multiple root. So, all elements of T are distinct. Hence

$$o(T) = p^n = o(K).$$

Thus, we have obtained a field of order p^n.

3.2.4. Theorem. Finite fields having same number of elements are isomorphic.

Proof. Let K_1 and K_2 be finite fields such that $o(K_1) = o(K_2)$.

Let $ch.K_1 = p_1$ and $ch.K_2 = p_2$, where p_1 and p_2 are primes. Then, we have

Then, we have $o(K_1) = p_1^{n_1}$ and $o(K_2) = p_2^{n_2}$ for some integers n_1 and n_2. So, we have

$$p_1^{n_1} = p_2^{n_2} \quad \Rightarrow \quad p_1 = p_2 = p(\text{say}) \text{ and } n_1 = n_2 = n(\text{say})$$

Let P_1 and P_2 are prime subfields of K_1 and K_2 respectively. Then,

$$P_1 \cong Z/{<p>} \cong P_2. \text{ So, } P_1 \cong P_2$$

By previous lemma, K_1 is the splitting field of the polynomial $f(x) = x^{p^n} - x \in P_1[x]$.

Now, $P_1 \cong P_2$ so $P_1[x] \cong P_2[x]$.

Let $f'(t)$ be the corresponding polynomial of f(x) and $f'(t) = t^{p^n} - t \in P_2[t]$.

Again, by previous lemma, K_2 is the splitting field of the polynomial $f'(t) \in P_2[t]$.

But $P_1 \cong P_2$. Therefore, splitting field will also be isomorphic, that is, $K_1 \cong K_2$.

3.2.5. Theorem. A field is finite iff $F^* = F - \{0\}$ is a multiplicative cyclic group.

Proof. Let F be a finite field with q elements. Then, $F^* = F - \{0\}$ is a multiplicative group with (q – 1) elements.

We claim that F* contains elements having order (q - 1).

Since F* is a finite group, so if $\lambda \in F^*$, then by Lagrange's theorem

$$\lambda^{o(F^*)} = 1 \quad \text{for all } \lambda \in F^*$$

That is, multiplicative order of each element is finite, so let 'n' be the least positive integer such that

$$\lambda^n = 1 \quad \text{for all } \lambda \in F^*$$

Then, $n \le q - 1$.

Now, consider the polynomial $f(x) = x^n - 1$.

Then, $f(\lambda)=\lambda^n-1=0 \Rightarrow \lambda$ satisfies f(x) for all $\lambda \in F^*$.

But f(x) is of degree n, it can have atmost n roots. Also, all elements of F* are roots of f(x). Therefore, $o(F^*) \le n \Rightarrow q-1 \le n$.

Hence there exists atleast one element $\lambda \in F^*$ such that $o(\lambda)=o(F^*)=q-1$.

Therefore, F* is cyclic.

Conversely, suppose that F* is cyclic. Let F* = < a >.

If a = 1, then o(F*) = o(a) = o(1) = 1. So, F = {0, 1} is finite.

So, let us assume that $a \ne 1$.

Case I. $ch.F = 0$

Since $1 \in F^* \Rightarrow -1 \in F^*$. Therefore, $-1=a^n$ for some integer n.

W.L.O.G., let $n \ge 1$, then

$a^{2n}=1 \Rightarrow o(a) \le 2n \Rightarrow o(a)$ is finite $\Rightarrow o(F^*)$ is finite $\Rightarrow o(F)$ is finite.

Since Ch.F = 0, then prime subfield P of F is such that $P \subseteq F$ and $P \cong Q$, a contradiction, as $o(Q)=\infty$ and $o(P)<\infty$.

Hence this case is not possible.

Case II. $ch.F \ne 0$

Then, we must have ch.F = p for some prime p.

Let P be the subfield of F, then $P \cong Z_p$ and o(P) = p. Since $a \ne 1,\ a-1 \in F$

$\Rightarrow a-1 \in F^* = <a> \Rightarrow a-1=a^n$ for some integer n $\Rightarrow a^n-a+1=0$.

Thus, 'a' satisfies the polynomial f(x) = $x^n - x - 1$ over P[x] and hence 'a' is algebraic over P.

Then, [P(a) : P] = degree of minimal polynomial of 'a' over P = r (say)

Therefore, P(a) is a vector space over P of dimension r. Thus, $P(a) \cong P^{(r)} = \{(\alpha_1, \alpha_2, ..., \alpha_r) : \alpha_i \in P\}$.

But $o(P)=p \Rightarrow o(P^{(r)})=p^r \Rightarrow o(P(a))=p^r$. Now, F* = < a > and $a \in P(a)$.

$\Rightarrow F^* \subseteq P(a) \Rightarrow \text{o}(F^*) \le o(P(a)) \Rightarrow \text{o}(F^*)<\infty$.

Therefore, o(F*) is finite.

Remark. The above theorem may not be true when a field F is infinite. We give an example of field of rational numbers. Let $Q^* = \{\alpha \in Q : \alpha \ne 0\}$.

We shall prove that the multiplicative group Q* is not cyclic.

Let, if possible, Q* is cyclic. So, let g be its generator, that is, Q* = < g >, where

$$g=\frac{p_1^{\alpha_1}p_2^{\alpha_2}...p_r^{\alpha_r}}{q_1^{\beta_1}q_2^{\beta_2}...q_t^{\beta_t}}$$

where p_i's and q_i's are distinct primes.

Now since $1\in Q^*$, so there must exist a positive integer n such that

$$1=g^n=\left(\frac{p_1^{\alpha_1}p_2^{\alpha_2}...p_r^{\alpha_r}}{q_1^{\beta_1}q_2^{\beta_2}...q_t^{\beta_t}}\right)^n \quad \Rightarrow \quad p_1^{n\alpha_1}p_2^{n\alpha_2}...p_r^{n\alpha_r}=q_1^{n\beta_1}q_2^{n\beta_2}...q_t^{n\beta_t}$$

which is a contradiction, since p_i's and q_i's are distinct primes. Hence Q* is not cyclic.

Remark. In view of the above remark, we can say that R* and C* are not cyclic because every subgroup of a cyclic group is cyclic and Q* is not cyclic.

3.3. Normal Bases. Let K be a finite separable normal extension of a subfield F and

$$G(K,F)=\{\tau_1,\tau_2,...,\tau_n\}$$

be the Galois group of K over F. If $x\in K$, then a basis of the form $\{\tau_1(x),\tau_2(x),...,\tau_n(x)\}$ for K over F is called a normal basis of K over F.

3.3.1. Theorem. Let K be a finite separable normal extension of degree n over a subfield F with Galois group $G(K,F)=\{\tau_1,\tau_2,...,\tau_n\}$. The subset $\{x_1,x_2,...,x_n\}$ of K is a basis for K over F if and only if the matrix

$$\left(\tau_i(x_j)\right)=\begin{pmatrix}\tau_1(x_1) & \tau_1(x_2) & \cdots & \tau_1(x_n)\\ \tau_2(x_1) & \tau_2(x_2) & ... & \tau_2(x_n)\\ \vdots & & \ddots & \vdots\\ \tau_n(x_1) & \tau_n(x_2) & \cdots & \tau_n(x_n)\end{pmatrix}$$

is non-singular.

Proof. Suppose first that the matrix $\left(\tau_i(x_j)\right)$ is non-singular.

Since [K : F] = n, so it is enough to show that the set $\{x_1,x_2,...,x_n\}$ is linearly independent over F. For this, consider

$$a_1x_1+a_2x_2+...+a_nx_n=0$$

where $a_i, 1\le i\le n,$ are elements of F.

Applying the F-automorphisms $\tau_1,\tau_2,...,\tau_n$, to obtain

$$\begin{gathered}a_1\tau_1(x_1)+a_2\tau_1(x_2)+...+a_n\tau_1(x_n)=0\\ a_1\tau_2(x_1)+a_2\tau_2(x_2)+...+a_n\tau_2(x_n)=0\\ . \qquad\qquad . \qquad\qquad .\\ . \qquad\qquad . \qquad\qquad .\\ . \qquad\qquad . \qquad\qquad .\\ a_1\tau_n(x_1)+a_2\tau_n(x_2)+...+a_n\tau_n(x_n)=0,\end{gathered}$$

which is a homogeneous system of equations in unknowns $a_i, 1 \le i \le n,$ with non-singular matrix of coefficients $\left(\tau_i(x_j)\right)$. It follows from the theory of homogeneous linear equations that $a_1 = a_2 = ... = a_n = 0$. Thus $\{x_1, x_2, ..., x_n\}$ is linearly independent and so forms a basis, as required.

Next, suppose that the matrix $\left(\tau_i(x_j)\right)$ is singular.

Again, due to the theory of homogeneous linear equations, it follows that there exist a non-trivial solution for the system

$$\begin{aligned}
&a_1\tau_1(x_1) + a_2\tau_1(x_2) + ... + a_n\tau_1(x_n) = 0\\
&a_1\tau_2(x_1) + a_2\tau_2(x_2) + ... + a_n\tau_2(x_n) = 0\\
&\quad . \qquad\qquad\qquad . \qquad\qquad\qquad .\\
&\quad . \qquad\qquad\qquad . \qquad\qquad\qquad .\\
&\quad . \qquad\qquad\qquad . \qquad\qquad\qquad .\\
&a_1\tau_n(x_1) + a_2\tau_n(x_2) + ... + a_n\tau_n(x_n) = 0,
\end{aligned}$$

in K, say, $\alpha_1, \alpha_2, ..., \alpha_n$. Since trace is a non-zero homomorphism, so there exists an element α of K such that $S_{K/F}(\alpha)$ is non-zero. If α_k is non-zero, we multiply the above system of equations by $\alpha\alpha_k^{-1}$ to obtain:

$$\begin{aligned}
&\beta_1\tau_1(x_1) + \beta_2\tau_1(x_2) + ... + \beta_n\tau_1(x_n) = 0\\
&\beta_1\tau_2(x_1) + \beta_2\tau_2(x_2) + ... + \beta_n\tau_2(x_n) = 0\\
&\quad . \qquad\qquad\qquad . \qquad\qquad\qquad .\\
&\quad . \qquad\qquad\qquad . \qquad\qquad\qquad .\\
&\quad . \qquad\qquad\qquad . \qquad\qquad\qquad .\\
&\beta_1\tau_n(x_1) + \beta_2\tau_n(x_2) + ... + \beta_n\tau_n(x_n) = 0,
\end{aligned}$$

where $\beta_j = \alpha\alpha_k^{-1}\alpha_j$ (j = 1, …, n). Applying the F-automorphisms $\tau_1^{-1}, \tau_2^{-1}, ..., \tau_n^{-1}$ to the above equations respectively, to obtain

$$\begin{aligned}
&\tau_1^{-1}(\beta_1)x_1 + \tau_1^{-1}(\beta_2)x_2 + ... + \tau_1^{-1}(\beta_n)x_n = 0\\
&\tau_2^{-1}(\beta_1)x_1 + \tau_2^{-1}(\beta_2)x_2 + ... + \tau_2^{-1}(\beta_n)x_n = 0\\
&\quad . \qquad\qquad\qquad . \qquad\qquad\qquad .\\
&\quad . \qquad\qquad\qquad . \qquad\qquad\qquad .\\
&\quad . \qquad\qquad\qquad . \qquad\qquad\qquad .\\
&\tau_n^{-1}(\beta_1)x_1 + \tau_n^{-1}(\beta_2)x_2 + ... + \tau_n^{-1}(\beta_n)x_n = 0,
\end{aligned}$$

Adding all these equations, as τ_i runs through the group G, so does τ_i^{-1}. we deduce that

$$S_{K/F}(\beta_1)x_1 + \dots + S_{K/F}(\beta_n)x_n = 0.$$

As $S_{K/F}(\beta_k)$ is a member of F and $\beta_k = \alpha\alpha_k^{-1}\alpha_k = \alpha$, so $S_{K/F}(\beta_k) = S_{K/F}(\alpha)$ is non zero, hence the set $\{x_1, x_2, ..., x_n\}$ is linearly dependent over F and so it does not form a basis, a contradiction to the assumption. Hence the result follows.

3.3.2. Corollary. The collection $\{\tau_1(x), \tau_2(x), ..., \tau_n(x)\}$, images of an element x under the automorphisms in the Galois group $G(K,F) = \{\tau_1, \tau_2, ..., \tau_n\}$, form a normal basis if and only if the matrix $(\tau_i\tau_j(x))$ is non-singular.

Next result proves that every separable normal extension of finite degree has a normal basis. However, we will prove the result for an infinite field first.

Before starting the main result we are defining some terms:

1. If K is any field, then $P_n(K)$ represents the collection of all polynomials in n indeterminates with scalars from the field K.
2. If K is any field and f(x) is a polynomial over F, for $\alpha \in K$, we define $\sigma_\alpha(f) = f(\alpha)$. Further, if $f \in P_n(F)$, means it is a polynomial in n inderminates, say $x_1, x_2, ..., x_n$, then for any n-tuple $\alpha = (\alpha_1, \alpha_2, ..., \alpha_n)$ we can obtain $\sigma_\alpha(f)$ by replacing x_i with α_i for $1 \le i \le n$.

3.3.3. Theorem. Let K be some extension of an infinite subfield F and f be a non-zero polynomial in $P_n(K)$. Then there are infinitely many ordered n-tuples $\alpha = (\alpha_1, \alpha_2, ..., \alpha_n)$ of elements of F such that $\sigma_\alpha(f) \neq 0$.

Proof. Mathematical induction on n is applied to obtain the required result.

For n = 1, let f(x) be a polynomial of degree d in P(K) = K[x]. Then f can have at most d roots in F (as obtained earlier in Section - I), and so there are infinitely many elements in F which does not satisfy f(x), that is, $f(\alpha) \neq 0$ or $\sigma_\alpha(f) \neq 0$ for infinitely many α in F.

Now assume that result holds for n = k, that is, if g is any polynomial in $P_k(K)$ then there are infinitely many ordered k-tuples $\beta = (\beta_1, \beta_2, ..., \beta_k)$ of elements of F such that $\sigma_\beta(g) \neq 0$.

Consider n = k+1, and let f be any non-zero polynomial in $P_{k+1}(K) = P(P_k(K))$, so we may express f in the form

$$f = g_0 + g_1x_{k+1} + g_2x_{k+1}^2 + ... + g_tx_{k+1}^t,$$

where $g_0, g_1, g_2, ..., g_t$ are polynomials in $P_k(K)$. Since f is a non-zero polynomial, at least one of the polynomials $g_0, g_1, g_2, ..., g_t$ must be non-zero, say, g_i. According to the induction hypothesis, there are infinitely many ordered k-tuples $\beta = (\beta_1, \beta_2, ..., \beta_k)$ of elements of F such that $\sigma_\beta(g_i) \neq 0$. For each of these k-tuples $\beta = (\beta_1, \beta_2, ..., \beta_k)$, the polynomial

$$f_\beta = \sigma_\beta(g_0) + \sigma_\beta(g_1)x_{k+1} + \sigma_\beta(g_2)x_{k+1}^2 + ... + \sigma_\beta(g_t)x_{k+1}^t$$

is a non-zero polynomial in P(K). Now following the similar lines as for n = 1, we conclude that there are infinitely many elements δ of F such that $\sigma_\delta(f_\beta) \neq 0$. But if we set $\alpha = (\beta_1, \beta_2, ..., \beta_k, \delta)$ it is clear that $\sigma_\alpha(f) = \sigma_\delta(f_\beta)$.

Hence we see that the result is true for n = k+1. This completes the induction.

3.3.4. Theorem. Let K be a finite separable normal extension of degree n over an infinite subfield F. Let $G(K,F) = \{\tau_1, \tau_2, ..., \tau_n\}$ be the Galois group of K over F. If f is a polynomial in $P_n(K)$ with indeterminates $X_1, X_2, ..., X_n$ such that, for every $\alpha \in K$, $\sigma_{\tau(\alpha)}(f) = 0,$ where, $\tau(\alpha) = (\tau_1(\alpha), \tau_2(\alpha), ..., \tau_n(\alpha))$ then f is the zero polynomial.

Proof. Let $\{x_1, x_2, ..., x_n\}$ be a basis for K over F. Then, due to Theorem 1, the matrix $(\tau_i(x_j))$ is non-singular, and so is invertible with inverse, say, (p_{ij}). Thus, $(\tau_i(x_j))(p_{ij}) = I_n$ and so the (i , r)th entry of this matrix are

$$\sum_{j=1}^{n} \tau_i(x_j) p_{jr} = \begin{cases} 1, & \text{if i = r} \\ 0, & \text{if i} \neq \text{r} \end{cases}$$

Let $\beta_i = \sum_{j=1}^{n} \tau_i(x_j) X_j = \tau_i(x_1)X_1 + \tau_i(x_2)X_2 + ... + \tau_i(x_n)X_n$ and $\beta = (\beta_1, \beta_2, ..., \beta_n)$. Then, define the polynomial g in $P_n(K)$ as

$$g(X_1, X_2, ..., X_n) = \sigma_\beta(f).$$

If $a = (a_1, a_2, ..., a_n)$ is any ordered n-tuple of elements of F and $\alpha = a_1x_1 + a_2x_2 + ... + a_nx_n$, then

$$\begin{aligned} \sigma_a(g) = g(a_1, a_2, ..., a_n) &= f\left(\sum_{j=1}^{n} \tau_1(x_j)a_j, \sum_{j=1}^{n} \tau_2(x_j)a_j, ..., \sum_{j=1}^{n} \tau_n(x_j)a_j \right) \\ &= f\left(\sum_{j=1}^{n} \tau_1(a_jx_j), \sum_{j=1}^{n} \tau_2(a_jx_j), ..., \sum_{j=1}^{n} \tau_n(a_jx_j) \right) \\ &= f\left(\tau_1(\alpha), \tau_2(\alpha), ..., \tau_n(\alpha)\right) \\ &= 0 \end{aligned}$$

by given hypothesis.

Now, if $b = (b_1, b_2, ..., b_n)$ be any ordered n-tuple of elements of F and $c_j = \sum_{r=1}^{n} p_{jr} b_r$, for $1 \leq j \leq n$. Then,

$$\sum_{j=1}^{n} \tau_i(x_j)c_j = \sum_{j=1}^{n}\sum_{r=1}^{n} \tau_i(x_j) p_{jr} b_r = \sum_{r=1}^{n}\sum_{j=1}^{n} \left(\tau_i(x_j) p_{jr}\right) b_r = b_i,$$

since $\sum_{j=1}^{n} \tau_i(x_j) p_{jr} = \begin{cases} 1, & \text{if i = r} \\ 0, & \text{if i} \neq \text{r} \end{cases}$.

Hence if $c=(c_1,c_2,...,c_n)$, then

$$\begin{aligned}\sigma_c(g)=g(c_1,c_2,...,c_n)&=f\left(\sum_{j=1}^{n}\tau_1(x_j)c_j,\sum_{j=1}^{n}\tau_2(x_j)c_j,...,\sum_{j=1}^{n}\tau_n(x_j)c_j\right)\\ &=f\left(b_1,b_2,...,b_n\right)\\ &=\sigma_b(f)\end{aligned}$$

However, $\sigma_c(g)=0$ as obtained above, so $\sigma_b(f)=0$ for any ordered n-tuple $b=(b_1,b_2,...,b_n)$ of elements of F. Thus f is the zero polynomial, otherwise it will contradict Theorem 2.

Remark. Let $G(K,F)=\{\tau_1,\tau_2,...,\tau_n\}$ be a Galois group of K over F. If $\tau_i,\tau_j\in G(K,F)$, then $\tau_i\tau_j\in G(K,F)$ and so it must be an element of $\{\tau_1,\tau_2,...,\tau_n\}$. We consider $\tau_i\tau_j=\tau_{p(i,j)}$. Since $G(K,F)=\{\tau_1,\tau_2,...,\tau_n\}$ is a group so due to left and right cancellation laws, $\tau_i\tau_j=\tau_i\tau_k$ if and only if j = k, that is, $\tau_{p(i,j)}=\tau_{p(i,k)}$ if and only if j = k, it follows that p(i, j) = p(i, k) if and only if j = k. Similarly, p(h, j) = p(i, j) if and only if h = i.

We can now prove the Normal Basis Theorem for the case of infinite fields.

3.3.5. Theorem. Let K be a finite separable normal extension of on infinite subfield F. Then there exists a normal basis for K over F.

Proof. Consider now the polynomial f in $P_n(K)$ obtained by

$$f=\det\begin{pmatrix}X_{p(1,1)} & X_{p(1,2)} & \cdots & X_{p(1,n)}\\ X_{p(2,1)} & X_{p(2,2)} & \cdots & X_{p(2,n)}\\ \vdots & & \ddots & \vdots\\ X_{p(n,1)} & X_{p(n,2)} & \cdots & X_{p(n,n)}\end{pmatrix}.$$

Then as discussed in the remark above X_i occurs exactly once in each row and exactly once in each column of this matrix. If we replace ordered n-tuple $(X_1,X_2,...,X_n)$ by (1, 0, …, 0) in f, we obtain the determinant of a matrix in which the identity element 1 of F occurs exactly once in each row and exactly once in each column; the determinant of such matrix is either 1 or –1. Hence f is a non-zero polynomial.

Due to Theorem 3, there is at least one element x of K such that

$$f\left(\tau_1(x),\tau_2(x),...,\tau_n(x)\right)\neq 0.$$

By the definition of the polynomial f, this in term becomes

$$\det\left(\tau_i\tau_j(x)\right)\neq 0.$$

Hence, by corollary to Theorem 1, $\{\tau_1(x),\tau_2(x),...,\tau_n(x)\}$ is a normal basis for K over F.

3.4. Cyclotomic Extensions. Let F be a field, for every positive integer m define

$$k_m = X^m - 1$$

in $F[X]$. If an extension K of F, is a splitting field of one of the polynomials k_m, then it is called a **cyclotomic extension**.

3.4.1. Theorem. Let F be a field with non-zero characteristic, then the cyclotomic extension is both separable and normal.

Proof. Suppose that F has non-zero characteristic p, then every positive integer m can be expressed in the form $m = p^r m_1$, where $r \geq 0$ and p does not divide m_1. Then we have $k_m = X^m - 1 = \left(X^{m_1} - 1\right)^{p^r} = (k_{m_1})^{p^r}$, and so roots of k_m are similar to those k_{m_1}. Thus splitting field of k_{m_1} over F is also a splitting field for k_m over F. Thus in this case we consider only those polynomials k_m for which m is not divisible by the characteristic. Then,

$$\frac{dk_m}{dX} = mX^{m-1}$$

The only non-zero factor of this polynomial are powers of X, none of which is a factor of k_m. Thus, no roots of k_m are repeated and so k_m is a separable polynomial. Also being a splitting field of some non-zero polynomial this extension is normal too. Hence all cyclotomic extensions of F are separable and normal.

Remark. Let K_m be a splitting field for k_m over F, where m is not divisible by the characteristic of F. Also assume that F is contained in K_m. As the m roots of k_m in K_m are all distinct, we call them the m^{th} roots of unity in K_m and denote them by $\xi_1, \dots, \xi_m$. Now if ξ_i and ξ_j are m^{th} roots of unity in K_m, we have $(\xi_i \xi_j)^m = \xi_i{}^m \xi_j{}^m = 1$ so $\xi_i \xi_j$ is also m^{th} roots of unity, therefore the collection of m^{th} roots of unity form a subgroup of the multiplicative group on non-zero elements of K_m. Further, being a finite multiplicative subgroup of non-zero elements of a group this subgroup must be a cyclic group. Any generator of this group is called a primitive m^{th} root of unity in K_m. If ξ is a primitive m^{th} root of unity, then ξ^r is also a primitive m^{th} root of unity for each r, relatively prime to m.

If m is a prime number, then every m^{th} root of unity, except the identity element, is a primitive m^{th} root of unity. It is clear that any primitive m^{th} root of unity ξ may be taken as a primitive element for K_m over F, that is to say, $K_m = F(\xi)$.

First we are to define the group $\boldsymbol{R_m}$.

The elements of $\boldsymbol{R}_m$ are the residue classes modulo m consisting of integers which are relatively prime to m, with the product of two relatively prime residue classes C_1, C_2 is defined to be the residue class containing $n_1 n_2$, where n_1, n_2 are members from C_1, C_2 respectively. The order of $\boldsymbol{R}_m$ by $\emptyset(m)$.

In the next theorem we will obtain the Galois group of a cyclotomic extension.

3.4.2. Theorem. Let F be a field, m a positive integer which is not divisible by the characteristic of F, if ch.F is non-zero. Let K_m be a splitting field for k_m over F including F. Then the Galois group $G(K_m, F)$ is isomorphic to a subgroup of $\mathbf{R}_m$.

Proof. Let ξ be a primitive m^{th} root of unity in K_m. If τ is any element of $G(K_m, F)$, then $\tau(\xi)$ is also a primitive m^{th} root of unity. Hence $\tau(\xi) = \xi^{n_\tau}$, where g.c.d.(n_τ, m) = 1. Define a mapping $: G \to \boldsymbol{R}_m$ as follows:

$$\theta(\tau) = \text{the residue class of } n_\tau \text{ modulo } m.$$

If τ and ρ are elements of G, then

$$\xi^{n_{\tau\rho}} = (\tau\rho)(\xi) = \tau\big(\rho(\xi)\big) = \tau(\xi^{n_\rho}) = (\tau(\xi))^{n_\rho} = \xi^{n_\tau n_\rho},$$

so $n_{\tau\rho} \equiv n_\tau n_\rho (\text{mod } m)$, and therefore $\theta(\tau\rho) = \theta(\tau)\theta(\rho)$. Hence θ is a homomorphism.

Further, θ is one-to-one, as if $\tau \neq \rho$ then $\tau(\xi) \neq \tau(\xi)$, that is, $\xi^{n_\tau} \neq \xi^{n_\rho}$ and hence n_τ and n_ρ are members of different residue classes modulo m.

Hence, G is isomorphic to the subgroup $\theta(G)$ of $\boldsymbol{R}_m$.

3.5. Cyclotomic Polynomial. Let F be an arbitrary field and K_m a splitting field for k_m over F containing F, we assume that m is not divisible by the characteristic of F if ch.F is non-zero. If d/m, the polynomial $k_d = X^d - 1$ divides $k_m = X^m - 1$ and hence roots of k_d are included among the m^{th} roots of unity in K_m, that is, there are d distinct d^{th} roots of unity among the m^{th} roots of unity and, in particular, $\phi(d)$ primitive d^{th} roots of unity. Thus, for each divisor d of m we may define the polynomial ϕ_d in $P(K_m)$ as

$$\phi_d = \prod (X - \xi_d),$$

where the product is taken over all the primitive d^{th} roots of unity ξ_d in K_m, then $deg\phi_d = \emptyset(d)$. Since every m^{th} root of unity ξ is a primitive d^{th} root of unity for some d/m, it follows that

$$k_m = X^m - 1 = \prod_{d/m} \phi_d.$$

The polynomial ϕ_m is called the m^{th} **cyclotomic polynomial**.

3.5.1. Theorem. For every positive integer m, the coefficients of the m^{th} cyclotomic polynomial belong to the prime subfield of F. In case if ch.F = 0, and the prime field is **Q**, then these coefficients are integers.

Proof. Mathematical induction on m is sued to obtain the result.

For m = 1, result is obvious as $\phi_1 = X - 1$ has coefficients in the prime field.

Suppose now that the result holds for all factors d of m such that $d < m$.

Then we have

$$X^m - 1 = \phi_m \prod_{\substack{1 \le d < m \\ d/m}} \phi_d.$$

By hypothesis, all the factors in the product have coefficients in the prime field; $X^m - 1$ has coefficients in the prime field. Hence so does ϕ_m. In the case, when the prime field is $\boldsymbol{Q}$, every factor in the product has integer coefficients with leading coefficient 1, when we divide a polynomial with integer coefficients by a polynomial with integer coefficients and leading coefficient 1 the quotient has integer coefficients. Thus ϕ_m have integer coefficients.

3.5.2. Example. Compute ϕ_{20}.

Since the divisors of 20 are 1, 2, 4, 5, 10 and 20, so we have

$$X^{20} - 1 = \phi_1\phi_2\phi_4\phi_5\phi_{10}\phi_{20.}$$

Similarly, the divisors of 10 are 1, 2, 5 and 10, so we have

$$X^{10} - 1 = \phi_1\phi_2\phi_5\phi_{10}.$$

Hence $\quad X^{10} + 1 = \phi_4\phi_{20.}$

Now we need to calculate ϕ_4. For this, the divisors of 4 are 1, 2 and 4, so we have

$$X^4 - 1 = \phi_1\phi_2\phi_4.$$

Also, $\quad X^2 - 1 = \phi_1\phi_2.$

So, we have $\quad \phi_4 = X^2 + 1.$

Hence $\quad \phi_{20} = \frac{X^{10}+1}{X^2+1}.$

3.6. Cyclotomic Extensions of the Rational Number Field.

In this section, we will consider that the field F = Q, field of rational numbers, and prove that the Galois group $G(K_m, Q)$ is isomorphic to the multiplicative group R_m of residue classes modulo m relatively prime to m.

3.6.1. Content of a Polynomial. Let $f(x) = \lambda_0 + \lambda_1 x + \lambda_2 x^2 + ... + \lambda_n x^n \in Z[x]$ be a polynomial over Z, then the content 't' of f is defined as $t = g.c.d.(\lambda_0, \lambda_1, \lambda_2, ..., \lambda_n)$.

3.6.2. Primitive Polynomial. A polynomial $f(x) \in Z[x]$ is said to be primitive polynomial if its content is 1.

It should be noted that if $f(x) \in Z[x]$, we may write $f(x) = cf_1(x)$, where c is the content of $f(x)$ and $f_1(x)$ is a primitive polynomial in $Z[x]$.

3.6.3. Theorem. If a polynomial $f(x) \in Z[x]$ can be expressed as a product of two polynomials over Q, the rational field, then it can be expressed as a product of two polynomials over Z.

Proof. Let $f(x) \in Z[x]$ and $g_1(x), g_2(x) \in Q[x]$ such that $f(x) = g_1(x).g_2(x)$. Let d_1, d_2 be the least common multiples of the denominators of the coefficients of $g_1(x), g_2(x)$ respectively. Then

$p_1(x) = d_1 g_1(x)$ and $p_2(x) = d_2 g_2(x)$ are polynomials in $Z[x]$. Let t_1 and t_2 be the content of $p_1(x)$ and $p_2(x)$ and write $p_1(x) = t_1 k_1(x)$ and $p_2(x) = t_2 k_2(x)$, where $k_1(x)$ and $k_2(x)$ are primitive polynomials in $Z[x]$. Then we have

$$d_1 d_2 f(x) = t_1 t_2 k_1(x) k_2(x).$$

We claim that $k_1(x)k_2(x)$ is a primitive polynomial.

Let p be any prime number. Since $k_1(x) = a_0 + a_1 x + a_2 x^2 + ...$ and $k_2(x) = b_0 + b_1 x + b_2 x^2 + ...$ are primitive polynomials so each polynomial has at least one coefficient which is not divisible by p. Let a_i and b_j be the first coefficients of $k_1(x)$ and $k_2(x)$ respectively, which are not divisible by p. Then the coefficients of X^{i+j} in $k_1(x).k_2(x)$ is

$$\sum_{u+v=i+j} a_u.b_v .$$

If $v \neq i$, $u \neq j$ and $u + v = i + j$, then either $u < i$ or $v < j$ and hence either a_u is divisible by p or b_v is divisible by p. Thus, all the terms, except for $a_i b_j$, in the summation are divisible by p and so the sum is not divisible by p. It follows that for every prime number p, $k_1(x).k_2(x)$ has at least one coefficient which is not divisible p, which implies that the g.c.d. of the coefficients of $k_1(x).k_2(x)$ is 1. Hence $k_1(x).k_2(x)$ is a primitive polynomial.

Thus, $t_1 t_2$ is the content of $(d_1 d_2) f(x)$. However, $d_1 d_2$ is a divisor of the content of $(d_1 d_2) f(x)$. Hence $\frac{t_1 t_2}{d_1 d_2}$ is an integer, say, l. Then $f(x) = (l k_1(x)) k_2(x)$ is a factorisation of $f(x)$ in $Z[x]$.

3.6.4. Corollary. If $f(x) \in Q[x]$ is a monic polynomial dividing $x^m - 1$, then $f(x) \in Z[x]$.

3.6.5. Definition. If $f(x) = \lambda_0 + \lambda_1 x + \lambda_2 x^2 + ... + \lambda_n x^n \in F[x]$ and k is any positive integer, then we denote by $f_k(x)$ the polynomial obtained as

$$f_k(x) = \lambda_0 + \lambda_1 x^k + \lambda_2 x^{2k} + ... + \lambda_n x^{nk} \in F[x]$$

3.6.6. Theorem. Let $f(x) \in Z[x]$ divides $x^m - 1$ and k is any positive integer such that g.c.d.(k,m)=1, then $f(x)$ divides $f_k(x)$ in $Z[x]$.

Now we will prove that the Galois group $G(K_m, Q)$ is isomorphic to the multiplicative group R_m of residue classes modulo m relatively prime to m.

3.6.7. Theorem. Let K_m be a splitting field of k_m over **Q.** Then $G(K_m, Q) \cong R_m$.

Proof. Let ζ be a primitive m^{th} root of unity in K_m. Define a monomorphism $: G(K_m, Q) \rightarrow R_m$ as follows:

$$\theta(\tau) = \text{the residue class of } n_\tau \text{ modulo } m,$$

for each automorphism τ in $G(K_m, Q)$, we defined $\tau(\zeta) = \zeta^{n_\tau}$ where n_τ is relatively prime to m.

This mapping is onto as well. Hence the required result holds.

3.6.8. Corollary. The cyclotomic polynomials ϕ_m are all irreducible in $Q[x]$.

3.7. Cyclic Extension. Let F be a field. A finite separable normal extension K of F is said to be cyclic extension of F if $G(K,F)$ is cyclic. We are considering that $F \subseteq K$.

3.7.1. Theorem. Let K be a cyclic extension of a subfield F and $G(K,F) = <\tau>$. If $x \in K$, then $N_{K/F}(x) = 1$ if and only if there is an element $y \in K$ such that $x = \dfrac{y}{\tau(y)}$, and $S_{K/F}(x) = 0$ if and only if there is an element z in K such that $x = z - \tau(z)$.

Proof. Since K is a finite extension of F so let $[K:F] = n;$ then $|G(K,F)|$=n and so $\tau^n = I$, the identity automorphism.

First, suppose that $x = \dfrac{y}{\tau(y)}$. Then

$$N_{K/F}(x) = I(x)\tau(x)\tau^2(x)\ldots\tau^{n-1}(x) = \frac{y}{\tau(x)}\frac{\tau(y)}{\tau^2(y)}\frac{\tau^2(y)}{\tau^3(y)}\cdots\frac{\tau^{n-1}(y)}{\tau^n(y)} = 1.$$

Similarly, if $x = z - \tau(z)$, we have

$$\begin{aligned} S_{K/F}(x) &= I(x) + \tau(x) + \tau^2(x) + \ldots + \tau^{n-1}(x) \\ &= z - \tau(z) + \tau(z) - \tau^2(z) + \tau^2(z) - \tau^3(z) + \ldots + \tau^{n-1}(z) - \tau^n(z) = 0. \end{aligned}$$

Conversely, suppose that

$$N_{K/F}(x) = I(x)\tau(x)\tau^2(x)\ldots\tau^{n-1}(x) = x\tau(x)\tau^2(x)\ldots\tau^{n-1}(x) = 1.$$

Then x is clearly non-zero and so is invertible with $x^{-1} = \tau(x)\tau^2(x)\ldots\tau^{n-1}(x)$.

Next, since the set of automorphisms $\{I, \tau, \tau^2, \ldots, \tau^{n-1}\}$ is linearly independent over K, the mapping

$$\varepsilon + x\tau + x\tau(x)\tau^2 + \ldots + x\tau(x)\ldots\tau^{n-2}(x)\tau^{n-1}$$

is non-zero mapping of K into itself. That is to say, there is an element t of K such that

$$y = t + x\tau(t) + x\tau(x)\tau^2(t) + \ldots + x\tau(x)\ldots\tau^{n-2}(x)\tau^{n-1}(t)$$

is non-zero. Applying the automorphism τ, we obtain

$$\tau(y) = \tau(t) + \tau(x)\tau^2(t) + \tau(x)\tau^2(x)\tau^3(t) + \ldots \tau(x)\tau^2(x)\ldots\tau^{n-1}(x)t = x^{-1}y.$$

Thus $x = y/\tau(y)$. Similarly suppose

$$S_{K/F}(x) = x + \tau(x) + \tau^2(x) + \ldots + \tau^{n-1}(x) = 0.$$

Then of course $\tau(x) + \tau^2(x) + \ldots + \tau^{n-1}(x) = -x.$

Since $S_{K/F}$ is not the zero mapping; so let t be an element of K such that $S_{K/F}(t)$ is non-zero, and consider the element

$$z_1 = x\tau(t) + (x + \tau(x))\tau^2(t) + \ldots + (x + \tau(x) + \ldots + \tau^{n-2}(x))\tau^{n-1}(t).$$

Applying the automorphism τ we obtain

$$\tau(z_1) = \tau(x)\tau^2(t) + (\tau(x) + \tau^2(x))\tau^3(t) + \ldots + (\tau(x) + \tau^2(x) + \ldots + \tau^{n-1}(x))t$$

$$= \tau(x)\tau^2(t) + (\tau(x) + \tau^2(x))\tau^3(t) + \ldots - xt.$$

Hence we have

$$z_1 - \tau(z_1) = x(t + \tau(t) + \tau^2(t) + \ldots + \tau^{n-1}(t)) = xS_{K/F}(t).$$

Since $S_{K/F}(t)$ lies in F and hence is left fixed by τ, it follows that if we write $z = z_1 / S_{K/F}(t)$, then $x = z - \tau(z)$.

3.7.2. Definition. Let a be any element of a division ring D. Then the **normaliser** of a in D is the set N(a) consisting of elements of D which commute with a:

so n belongs to N(a) if and only if an = na.

3.7.3. Exercise. Let D be a division ring. Then the centre Z of D is a subfield of D and the normalizer of each element of D is a division subring of D including Z.

3.7.4. Wedderburn theorem. Every finite division ring is a field.

Proof. Let D be a finite division ring, with centre Z. Suppose Z has q elements and D has q^n elements. We claim that D = Z and n = 1.

The multiplicative group D* can be expressed as a union of finitely many conjugate classes, say $C_1,\ldots,C_k$, w.r.t. the subgroup Z*. Then, $|C_i| = \dfrac{q^n - 1}{q^{t_i} - 1}$ where $t_i < n$. Thus,

$$q^n - 1 = q - 1 + \sum_{i=1}^{k} \frac{q^n - 1}{q^{t_i} - 1}.$$

Now the nth cyclotomic polynomial Φ_n in P(**Q**) is a factor of both the polynomials $X^n - 1$ and $\dfrac{X^n - 1}{X^{t_i} - 1}$.

Let a = $\Phi_n(q)$. Then a divides $q^n - 1$ and $\dfrac{q^n - 1}{q^{t_i} - 1}$. Hence a divides q – 1.

If n > 1, then for every primitive nth root of unity ζ in the field of complex numbers **C** we have |q - ζ| > q – 1. Hence |a| = ∏| q - ζ |> q – 1, and hence a cannot be a factor of q – 1.

It follows that there is no conjugate class C_i containing more than one element. Hence n = 1 and D = Z, as required.

3.7.5. Corollary. If F is a finite set, then it is a division ring if and only if it is a field.

3.8. Check Your Progress.

1. Design fields of order 27, 16, 25, 49.

2. Compute ϕ_{30}.

3.9. Summary.

In this chapter, we have derived results related to cyclotomic extensions and cyclic extensions. Also It was proved that a finite division ring is a field, therefore we can say that a division ring which is not a field is always infinite.

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 edition, 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.