BHARATHIDASAN UNIVERSITY

Tiruchirappalli- 620024

Tamil Nadu, India

Programme	:	M. Sc. Mathematics
Course Title	:	ALGEBRA - II
Course Code	:	21S3M08CC

UNIT - III

CLASSICAL FORMULAS AND SPLITTING FIELDS

Dr. C. Durairajan

Professor

Department of Mathematics

The Galois Groups

If $\mathbb{E}$ is a field, then an **automorphism of** $\mathbb{E}$ is an isomorphism of $\mathbb{E}$ with itself. If $\mathbb{E} \mid \mathbb{F}$ is a field extension, then an **automorphism** σ **of** $\mathbb{E}$ **fixes** $\mathbb{F}$ **pointwise** if $\sigma(c) = c$ for every $c \in \mathbb{F}$.

Lemma 1.

Let $f(x) \in \mathbb{F}[x]$ and let $\mathbb{E} \mid \mathbb{F}$ be an extension field of $\mathbb{F}$. If $\sigma : \mathbb{E} \to \mathbb{E}$ is an automorphism fixing $\mathbb{F}$ pointwise and if $\alpha \in \mathbb{E}$ is a root of $f(x)$, then $\sigma(\alpha)$ is also a root of $f(x)$.

Let $\mathbb{E} \mid \mathbb{F}$ be a field extension. Then

$$G(\mathbb{E} \mid \mathbb{F}) = \{ \text{ automorphisms } \sigma \text{ of } \mathbb{E} \text{ fixing } \mathbb{F} \text{ pointwise } \}$$

is a group under the binary operation of composition. This group is called the **Galois group** of $\mathbb{E} \mid \mathbb{F}$. If $f(x) \in \mathbb{F}[x]$ has splitting field $\mathbb{E}$, then the **Galois group of** $f(x)$ is $G(\mathbb{E} \mid \mathbb{F})$.

Continue ...

Theorem 2.

If $f(x) \in \mathbb{F}[x]$ has n distinct roots in its splitting field $\mathbb{E}$, then $G(\mathbb{E} \mid \mathbb{F})$ is isomorphic to a subgroup of the symmetric group S_n and so its order is a divisor of $n!$.

Theorem 3.

If $f(x) \in \mathbb{F}[x]$ is a separable polynomial and if $\mathbb{E} \mid \mathbb{F}$ is its splitting field, then $|G(\mathbb{E} \mid \mathbb{F})| = [\mathbb{E} : \mathbb{F}]$.

Lemma 4.

Let $\mathbb{F} \subseteq \mathbb{B} \subseteq \mathbb{E}$ be a tower of fields with $\mathbb{B} \mid \mathbb{F}$ the splitting field of some polynomial $f(x) \in \mathbb{F}[x]$. If $\sigma \in G(\mathbb{E} \mid \mathbb{F})$, then $\sigma_{|B} \in G(\mathbb{B} \mid \mathbb{F})$ where $\sigma_{|B}$ is the σ restricted to B.

Continue ...

Theorem 5.

Let $\mathbb{F} \subseteq \mathbb{B} \subseteq \mathbb{E}$ be a tower of fields with $\mathbb{B} \mid \mathbb{F}$ the splitting field of some polynomial $f(x) \in \mathbb{F}[x]$ and $\mathbb{E} \mid \mathbb{F}$ the splitting field of some $g(x) \in F[x]$. Then $G(\mathbb{E} \mid \mathbb{B})$ is a normal subgroup of $G(\mathbb{E} \mid \mathbb{F})$ and $\frac{G(\mathbb{E}|\mathbb{F})}{G(\mathbb{E}|\mathbb{B})} \cong G(\mathbb{B} \mid \mathbb{F})$.

Lemma 6.

1. *If $C = \langle a \rangle$ is a cyclic group of order n and generator a, then has a unique subgroup of order d for each divisor d of n and this subgroup is cyclic.*
2. *C is a cyclic group of order n iff for every divisor d of n, C has at most one cyclic subgroup of order d.*

The Galois Group

Theorem 7.

If $\mathbb{F}$ is a field with multiplicative group $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$, then every finite subgroup G of $\mathbb{F}^*$ is cyclic.

For every finite field $\mathbb{F}$, $\mathbb{F}^*$ is a finite subgroup of itself. Therefore, we have

Corollary 8.

If $\mathbb{F}$ is a finite field with multiplicative group $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$, then $\mathbb{F}^*$ is cyclic.

If $\mathbb{F}$ is a finite field of characteristic p, then an element $\alpha \in \mathbb{F}$ is called a **primitive element** if $\mathbb{F} = \mathbb{Z}_p(\alpha)$.

Roots of Unity

The following theorem gives us the existence of irreducible polynomial of any positive degree n over $\mathbb{Z}_p[x]$.

Lemma 9.

If α is a primitive element of $GF(p^n)$, then α is a root of an irreducible polynomial in $\mathbb{Z}_p[x]$ of degree n.

Theorem 10.

$G(GF(p^n) \mid GF(P)) \cong \mathbb{Z}_n$ *with generator* $u \mapsto u^p$.

This generator is called the **Frobenius automorphism**.

Lemma 11.

Let n be a positive integer and let $\mathbb{F}$ be a field. If the characteristic of $\mathbb{F}$ is either 0 or is a prime not dividing n, then $x^n - 1$ has n distinct roots in a splitting field.

Continue ...

Let n be a fixed positive integer. A generator of the group of all n^{th} roots of unity is called a **primitive root of unity**. $U(\mathbb{Z}_n)$ is the collection of all units of $\mathbb{Z}_n$.

Theorem 12.

If $\mathbb{F}$ is a field and $\mathbb{E} = \mathbb{F}(\alpha)$ where α is a primitive n^{th} root of unity, then $G(\mathbb{E} \mid \mathbb{F})$ is isomorphic to a subgroup of $U(\mathbb{Z}_n)$ and hence $G(\mathbb{E} \mid \mathbb{F})$ is an abelian group.

Theorem 13.

Let $\mathbb{F}$ contain a primitive nth root of unity, and let $f(x) = x^n - c \in F[x]$. If $\mathbb{E} \mid \mathbb{F}$ is a splitting field of $f(x)$, then there is an injection $\phi : G = G(\mathbb{E} \mid \mathbb{F}) \to \mathbb{Z}_n$. Moreover, $f(x)$ is irreducible if and only if ϕ is surjective.

Solvability by Radicals

1. A field extension $\mathbb{B} \mid \mathbb{F}$ is said to be a **pure extension of type** m if $\mathbb{B} = \mathbb{F}(\alpha)$ where $\alpha^m \in \mathbb{F}$ for some positive integer m.
2. A tower of fields

$$\mathbb{F} = \mathbb{B}_0 \subset \mathbb{B}_1 \subset \cdots \subset \mathbb{B}_r$$

   is said to be a **radical tower** if each $\mathbb{B}_{i+1}/\mathbb{B}_i$ is a pure extension. In this case, we call $\mathbb{B}_t/\mathbb{F}$ a **radical extension of** $\mathbb{F}$.
3. A polynomial $f(x)$ over $\mathbb{F}$ is said to be **solvable by radicals over** $\mathbb{F}$ if there is a radical extension $\mathbb{B} \mid \mathbb{F}$ which contains a splitting field $\mathbb{E}$ of $f(x)$ over $\mathbb{F}$.

Solvable Groups

A group G is called a **solvable group** if it has a subnormal series whose factor groups are all abelian, that is, if there are subgroups $G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_t = \{e\}$ such that G_i is normal in G_{i-1} and $\frac{G_{i-1}}{G_i}$ is an abelian group for $i = 1, 2, \cdots, t$.

Example 14.

1. Every abelian group is a solvable group.
2. Let p be a prime integer. Then every finite p-group is solvable.
3. S_n is solvable for $n < 5$.
4. S_n is not solvable for $n \geq 5$.

Continue ...

1. The homomorphic image of a solvable group is solvable.
2. Let N be a normal subgroup of G. Then G is solvable iff N and $\frac{G}{N}$ are solvable.
3. If G is solvable, and H is a subgroup of G, then H is solvable.
4. If G and H are solvable, the direct product G $\times$ H is solvable.

Continue ...

Lemma 15.

Let $\mathbb{F}$ be a field of characteristic 0, let $f(x) \in \mathbb{F}[x]$ be solvable by radicals and let $\mathbb{E}$ be a splitting field of $f(x)$ over $\mathbb{F}$.

1. *There is a radical tower*

$$\mathbb{F} = R_0 \subset R_1 \subset \cdots \subset R_t$$

   with $E \subset R_t$, with R_t a splitting field of some polynomial over $\mathbb{F}$, and with each R_i/R_{i-1} is a pure extension of prime type p_i.

2. *If R_i/F is a radical extension as in part (i), and if $\mathbb{F}$ contains the p_ith roots of unity for all i, then $G(\mathbb{E} \mid \mathbb{F})$ is a solvable group.*

Continue ...

Theorem 16.

Let $f(x) \in \mathbb{F}[x]$ be solvable by radicals over a field $\mathbb{F}$ of characteristic 0, and let $\mathbb{E} \mid \mathbb{F}$ be its splitting field. Then $G(\mathbb{E} \mid \mathbb{F})$ is a solvable group.

Using this theorem, Abel and Ruffini proved the following

Theorem 17.

There exists a quintic polynomial $f(x) \in \mathbb{Q}[x]$ that is not solvable by radicals.

In fact, they prove that $x^5 - 4x + 2$ is not solvable by radicals.

References

- M. Artin, **Algebra**, Prentice Hall of India, New Delhi, 1994.
- David S. Dummit and Richard M. Foote,**Abstract Algebra**, 2nd Edition, Wiley Student Edition, 2008.
- I. N. Herstein, **Topics in Algebra**, John Wiley, 2nd Edition, 1975.
- Ian Stewart, **Galois Theory**, Chapman and Hall, 1973.
- Joseph Gallian, **Contemporary Abstract Algebra** , 9th Edition
- Joseph Rotman, **Galois Theory**, 2nd edition, Springer Verlag, 1990.
- C. Lanski, **Concepts in Abstract Algebra**, AMS Indian edition, 2010.
- Serge Lang, **Algebra** - Revised third edition, Springer, Verlag - 2002.
- R. Solomon, **Abstract Algebra**, AMS Indian edition, 2010.
- John B. Fraleigh, **A First course in Abstract Algebra**, Narosa Publishing House, 2003.