BHARATHIDASAN UNIVERSITY

Tiruchirappalli- 620024

Tamil Nadu, India

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

UNIT - V

THE FUNDAMENTAL THEOREM OF GALOIS THEORY

Dr. C. Durairajan

Professor

Department of Mathematics

The Fundamental Theorem of Galois Theory

A partially ordered set (poset for short) is a set P with a binary relation $\preceq$ satisfying all of the following.

1. (reflexivity) $x \preceq x$ for all $x \in P$
2. (antisymmetry) $x \preceq y$ and $y \preceq x$ implies $x = y$
3. (transitivity) $x \preceq y$ and $y \preceq z$ implies $x \preceq z$

Example 1.

1. The power set of a nonempty set X with inclusion relation,
2. $P = \{1, 2, \cdots, \}$ and $n \preceq m$ if $n \leq m$,
3. $P = \{1, 2, \cdots, \}$ and $n \preceq m$ if n divides m,
4. $P = \{A_1, A_2, \cdots, A_m\}$ and $A_i \preceq A_j$ if $A_i \subset A_j$

are posets.

Continue ...

Let $(P, \preceq)$ be a poset. An element m is said to be the **least upper bound of** a **and** b if

1. $a \preceq m$ and $b \preceq m$
2. if M is any upper bound of a and b, then $m \preceq M$

Similarly, we can define the greatest lower bound.

A **lattice** is a partially ordered set $(L, \preceq)$ in which each pair of elements $a, b \in L$ has the least upper bound $a \vee b$ and the greatest lower bound $a \wedge b$.

Examples

1. The set of all real numbers with the usual ordering $<$ is a lattice.
2. If G is a group, let Sub(G) be the family of all the subgroups of G, and define $H \preceq K$ if $H \subseteq K$. Then Sub(G) is a lattice with $H \vee K$ the subgroup generated by H and K, and $H \wedge K = H \cap K$.
3. Let $\mathbb{E} \mid \mathbb{F}$ be a field extension, let $Lat(\mathbb{E} \mid \mathbb{F})$ be the family of all intermediate fields, and define $B \preceq C$ if $B \subseteq C$. Then $Lat(\mathbb{E} \mid \mathbb{F})$ is a lattice with $B \vee C$ the smallest field containing B and C and $B \wedge C = B \cap C$.
4. Let L be the set of all integers $n > 1$ and define $n \preceq m$ if $n \mid m$. Then L is a lattice with $n \vee m = lcm\{n, m\}$, $n \wedge m = gcd\{n, m\}$.

Continue ...

The set of continuous real-valued functions on a topological space is a lattice under the pointwise order, and $(f \vee g)(x) = f(x) \vee g(x)$ and $(f \wedge g)(x) = f(x) \wedge g(x)$ for each x.

Lemma 2.

If L and L' are lattices and $\gamma : L \to L'$ is an order reversing bijection $[a \preceq b$ implies $\gamma(b) \preceq \gamma(a)]$, then $\gamma(a \vee b) = \gamma(a) \wedge \gamma(b)$ and $\gamma(a \wedge b) = \gamma(a) \vee \gamma(b)$

Continue ...

Theorem 3 (Fundamental Theorem of Galois Theory).

Let $\mathbb{E} \mid \mathbb{F}$ be a Galois extension with Galois group $G = G(\mathbb{E} \mid \mathbb{F})$.

1. *The function $\gamma : Sub(G) \to Lat(\mathbb{E} \mid \mathbb{F})$, defined by $H \mapsto \mathbb{E}^H$, is an order reversing bijection with inverse $\delta : \mathbb{B} \mapsto G(\mathbb{E} \mid \mathbb{B})$.*
2. $E^{G(\mathbb{E}|\mathbb{B})} = \mathbb{B}$ *and* $G(\mathbb{E} \mid \mathbb{E}^H) = H$.
3. $\mathbb{E}^{H \vee K} = \mathbb{E}^H \cap \mathbb{E}^K, \mathbb{E}^{H \cap K} = \mathbb{E}^H \vee \mathbb{E}^K$ *and*
$$G(\mathbb{E} \mid \mathbb{B} \vee C) = G(\mathbb{E} \mid \mathbb{B}) \cap G(\mathbb{E} \mid C)$$
$$G(\mathbb{E} \mid \mathbb{B} \cap C) = G(\mathbb{E} \mid \mathbb{B}) \vee G(\mathbb{E} \mid C).$$
4. $[\mathbb{B} : \mathbb{F}] = [G : G(\mathbb{E} \mid \mathbb{B})]$ *and* $[G : H] = [E^H : \mathbb{F}]$.
5. $\mathbb{B} \mid \mathbb{F}$ *is a Galois extension if and only if* $G(\mathbb{E} \mid \mathbb{B})$ *is a normal subgroup of* G.

Applications

1. A Galois extension $\mathbb{E} \mid \mathbb{F}$ has only finitely many intermediate fields.
2. A finite extension $\mathbb{E} \mid \mathbb{F}$ is simple if and only if it has only finitely many intermediate fields.
   This is theorem is known as Steinitz Theorem.
3. If $\mathbb{E} \mid \mathbb{F}$ is a finite simple extension and B is an intermediate field, then B/F is simple.
4. Every Galois extension $\mathbb{E} \mid \mathbb{F}$ is simple.
5. The Galois field $GF(p^n)$ has exactly one subfield of order p^d for every divisor d of n.
6. If $\mathbb{E} \mid \mathbb{F}$ is an abelian extension, i.e., a Galois extension whose Galois group $G(\mathbb{E} \mid \mathbb{F})$ is abelian, then every intermediate field B is a Galois extension.

Fundamental Theorem of Algebra

In 1799, the fundamental theorem of algebra was first proved by Gauss. Before proving this theorem, first let us learn a few basic concepts

1. If $f(x) \in \mathbb{R}[x]$ and there exist $a, b \in \mathbb{R}$ such that $f(a) > 0$ and $f(b) < 0$, then $f(x)$ has a real root.
2. Using this, we prove every positive real number r has a real square root.

   For this, let $f(x) = x^2 - r$, then $f(r+1) = r^2 + r + 1 > 0$ and $f(0) = -r < 0$. Therefore, $f(x)$ has a real root. That is, r has a real square root.
3. Every quadratic polynomial over $\mathbb{C}$ has a complex root.

   For this, let $z \in \mathbb{C}$, then the polar form of z is $z = |z|\, e^{i\theta}$. By the above, $\sqrt{|z|} \in \mathbb{R}$ and $e^{\frac{i\theta}{2}} \in \mathbb{C}$. Therefore, $\sqrt{z} = \sqrt{|z|}e^{\frac{i\theta}{2}} \in \mathbb{C}$.

Fundamental Theorem of Algebra

1. The field $\mathbb{C}$ has no extensions of degree 2.
   Suppose it has an extension of degree 2. Then there exists a quadratic irreducible polynomial over $\mathbb{C}$, a contradiction to the above.
2. Every polynomial over $\mathbb{R}$ having odd degree has a real root.
   For this, if $a + ib$, $b \neq 0$, is root, then $a - ib$ is also a root. This implies, every polynomial has even number of complex roots and hence every polynomial over $\mathbb{R}$ having odd degree has a real root.

Theorem 4 (Fundamental Theorem of Algebra).

Every nonconstant $f(x) \in \mathbb{C}[x]$ has a complex root.

Repeatedly using this theorem, we prove

Corollary 5.

Every $f(x) \in \mathbb{C}[X]$ *of degree* $n \geq 1$ *splits over* $\mathbb{C}$, *that is,* $f(x) = c(x - \alpha_1) \cdots (x - \alpha_n)$ *where* $c, \alpha_1, \cdots, \alpha_n \in \mathbb{C}$.

If $\alpha = a + ib$ is a complex root of $f(x)$, then $\overline{\alpha} = a - ib$ is also a root of $f(x)$. Therefore, $(x - \alpha)(x - \overline{\alpha}) \in \mathbb{R}$ is a factor of $f(x)$. Thus, every polynomial of degree greater than 1 over $\mathbb{C}$ is written as a product of quadratic or linear factors over $\mathbb{R}$.

Lemma 6.

Let $\mathbb{E} \mid \mathbb{F}$ be a splitting field of $f(x) \in \mathbb{F}[x]$ with Galois group $G = G(\mathbb{E} \mid \mathbb{F})$. If $\mathbb{F}^*/\mathbb{F}$ is an extension and $\mathbb{E}^*/\mathbb{F}^*$ is a splitting field of $f(x)$ containing $\mathbb{E}$, then restriction $\sigma \mapsto \sigma_{|\mathbb{E}}$ is an infective homomorphism

$$G(\mathbb{E}^*/\mathbb{F}^*) \to G(\mathbb{E} \mid \mathbb{F}).$$

Definition 7.

If $\mathbb{E} \mid \mathbb{F}$ is a Galois extension and a $\alpha \in \mathbb{E}^* = \mathbb{E} \setminus \{0\}$, define its **norm** $N(\alpha)$ by

$$N(\alpha) = \prod_{\sigma \in G(\mathbb{E}|\mathbb{F})} \sigma(\alpha)$$

Theorem 8 (Hilbert's Theorem).

Let $\mathbb{E} \mid \mathbb{F}$ be a Galois extension whose Galois group $G = G(\mathbb{E} \mid \mathbb{F})$ is cyclic of order n and let σ be a generator of G. Then $N(\alpha) = 1$ if and only if there exists $\beta \in \mathbb{E}^*$ with $\alpha = \beta\sigma(\beta^{-1})$

Corollary 9.

Let $\mathbb{E} \mid \mathbb{F}$ be a Galois extension of prime degree p. If $\mathbb{F}$ has a primitive pth root of unity, then $E = F(\beta)$, where $\beta^p \in F$, and so $\mathbb{E} \mid \mathbb{F}$ is a pure extension.

Galois's Great Theorem

Theorem 10 (Galois).

Let $\mathbb{F}$ be a field of characteristic 0, and let $\mathbb{E} \mid \mathbb{F}$ be a Galois extension. Then $G = G(\mathbb{E} \mid \mathbb{F})$ is a solvable group if and only if $\mathbb{E}$ can be imbedded in a radical extension of F.

Therefore, the Galois group of $f(x) \in \mathbb{F}[x]$, where $\mathbb{F}$ is a field of characteristic 0, is a solvable group if and only if $f(x)$ is solvable by radicals.

Corollary 11.

If $\mathbb{F}$ is a field of characteristic 0, then every polynomial in $\mathbb{F}[x]$ of degree $n \leq 4$ is 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.