BHARATHIDASAN UNIVERSITY

Tiruchirappalli- 620024

Tamil Nadu, India

Programme : M. Sc. Mathematics

Course Title : ALGEBRA - II

Course Code : 21S3M08CC

UNIT - IV

INDEPENDENCE OF CHARACTERS AND GALOIS EXTENSIONS

Dr. C. Durairajan

Professor

Department of Mathematics

Characters

- A **character** of a group G in a field $\mathbb{E}$ is a homomorphism $\sigma : G \to \mathbb{E}^*$ where $\mathbb{E}^* = \mathbb{E} \setminus \{0\}$ is the multiplicative group of $\mathbb{E}$.
- A set $\{\sigma_1, \sigma_2, \cdots, \sigma_n\}$ of characters of a group G in a field $\mathbb{E}$ is said to be an **independent set** if there do not exist $a_1, a_2, \cdots, a_n \in \mathbb{E}$, not all 0, with

$$\sum a_i \sigma_i(x) = 0 \text{ for all } x \in G.$$

Lemma 1.

Every set $\{\sigma_1, \sigma_2, \cdots, \sigma_n\}$ of distinct characters of a group G in a field $\mathbb{E}$ is independent.

- This lemma is known as the Dedekind Lemma.

Continue...

- It is clear that the set $V(G, \mathbb{E})$ of all characters of a group G in a field $\mathbb{E}$ form a vector space over $\mathbb{E}$ under the operations defined by $(\sigma + \eta)(g) = \sigma(g) + \eta(g), (\alpha\sigma)(g) = \alpha(\sigma(g))$ for all $\alpha \in \mathbb{E}$.
- Independence of characters is linear independent subset of $V(G, \mathbb{E})$.
- Using the above lemma, we can prove

Corollary 2.

Every set $\{\sigma_1, \sigma_2, \cdots, \sigma_n\}$ of distinct automorphisms of a field $\mathbb{E}$ is independent.

- Let $Aut(\mathbb{E})$ be the group of all the automorphisms of a field E. Then $Aut(\mathbb{E})$ is a group under the binary operation composition.

Continue ...

- If G is a subset of $Aut(\mathbb{E})$, then

$$E^G = \{\alpha \in \mathbb{E} \mid \sigma(\alpha) = \alpha \text{ for all } \sigma \in G\}$$

  is called the **fixed field** of G. It is a subfield of $\mathbb{E}$.
- If $\mathbb{E} \mid \mathbb{F}$ is a field extension with Galois group $G = G(\mathbb{E} \mid \mathbb{F})$, then $\mathbb{F} \subseteq \mathbb{E}^G \subseteq \mathbb{E}$.
- In general, whether $\mathbb{F} = \mathbb{E}^G$ or not. For example, if $\mathbb{F} = \mathbb{Q}$ and $\mathbb{E} = \mathbb{Q}(\alpha)$ where α is the real cube root of 2, then $G = G(\mathbb{E} \mid \mathbb{F}) = G(\mathbb{Q}(\alpha) \mid \mathbb{Q}) = \{e\}$ because $\sigma(\alpha)$ is also a root of $x^3 - 2$, but $\mathbb{E}$ does not contain the other two complex roots of the polynomial. Hence $\mathbb{E} = \mathbb{E}^G \neq \mathbb{F}$.

Galois Extensions

It is clear that if H, K are subsets of $Aut(\mathbb{E})$ and $H \subset K$, then $\mathbb{E}^K \subset \mathbb{E}^H$.

Lemma 3.

If $G = \{\sigma_1, \sigma_2, \cdots, \sigma_n\}$ is a set of automorphisms of $\mathbb{E}$, then $[\mathbb{E} : \mathbb{E}^G] \geq n$.

If G is a subgroup if $Aut(\mathbb{E})$, then we have the following

Theorem 4.

If $G = \{\sigma_1, \sigma_2, \cdots, \sigma_n\}$ is a subgroup of $Aut(\mathbb{E})$, then $[\mathbb{E} : \mathbb{E}^G] = |G|$.

Using the above theorems and fact about the fixed field, we prove

Corollary 5.

If G, H are finite subgroups of $Aut(\mathbb{E})$ with $\mathbb{E}^G = \mathbb{E}^H$, then $G = H$.

Continue ...

A finite field extension $\mathbb{E} \mid \mathbb{F}$ is said to be a **Galois (or normal)** extension if $\mathbb{F} = \mathbb{E}^{G(\mathbb{E}|\mathbb{F})}$.

Theorem 6.

The following conditions are equivalent for a finite extension $\mathbb{E} \mid \mathbb{F}$ with Galois group $G = G(\mathbb{E} \mid \mathbb{F})$.

1. $\mathbb{F} = \mathbb{E}^G$,
2. *every irreducible $p(x) \in \mathbb{F}[x]$ with one root in $\mathbb{E}$ is separable and has all its roots in $\mathbb{E}$; that is, $p(x)$ splits over $\mathbb{E}$,*
3. *$\mathbb{E}$ is a splitting field of some separable polynomial $f(x) \in \mathbb{F}[x]$.*

Given a field extension $\mathbb{E} \mid \mathbb{F}$, an **intermediate field** is a field $\mathbb{B}$ with $\mathbb{F} \subseteq \mathbb{B} \subseteq \mathbb{E}$.

Continue ...

- Using he above theorem, we can prove that if $\mathbb{E} \mid \mathbb{F}$ is a Galois extension, then $\mathbb{E}$ is a Galois extension over any intermediate field.
- Let $\mathbb{E} \mid \mathbb{F}$ be a Galois extension and let $\mathbb{B}$ and C be intermediate fields. If there exists an isomorphism $\mathbb{B} \to C$ fixing $\mathbb{F}$, then C is called a **conjugate of** $\mathbb{B}$.

Theorem 7.

Let $\mathbb{E} \mid \mathbb{F}$ be a Galois extension, and let $\mathbb{B}$ be an intermediate field. The following conditions are equivalent.

1. $\mathbb{B}$ *has no conjugates (other than* $\mathbb{B}$ *itself).*
2. *If* $\sigma \in G(\mathbb{E} \mid \mathbb{F})$, *then* $\sigma_{|\mathbb{B}} \in G(\mathbb{B} \mid \mathbb{F})$.
3. $\mathbb{B} \mid \mathbb{F}$ *is a Galois extension.*

Examples

1. Let $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. Then a splitting field for $f(x)$ is $\mathbb{E} = \mathbb{Q}(\alpha, \omega)$ where $\alpha = \sqrt[3]{2}$ and ω is primitive cube root of unity. Since $\mathbb{E} \mid \mathbb{Q}$ is a splitting field of a separable polynomial and $\mathbb{Q}$ is a perfect field, $\mathbb{E} \mid \mathbb{Q}$ is a Galois extension.
2. If $g(x) = x^3 - 3x^2 + 3x - 3$, then $g(x)$ is irreducible in $\mathbb{Q}[x]$, by Eisenstein's criterion, but it has a root $\beta = 1 + \alpha$ in $\mathbb{E}$. It follows that $g(x)$ splits in $\mathbb{E}[x]$.
3. The intermediate field $\mathbb{B} = \mathbb{Q}(\omega)$ is a Galois extension over $\mathbb{Q}$, for it is a splitting field of $x^3 - 1$. We know that $G(\mathbb{E} \mid \mathbb{Q}) \cong S_3$. It follows that $\sigma(\mathbb{B}) = \mathbb{B}$ for every $\sigma \in G(G(\mathbb{E} \mid \mathbb{Q})$. On the other hand, if $C = \mathbb{Q}(\alpha)$, then $\mathbb{Q}(\alpha^2)$ is a conjugate of C and$\mathbb{Q}(\alpha^2) \neq C$.

Examples

1. Let $\mathbb{F}$ be a field of characteristic $\neq 2$ and $\mathbb{E} \mid \mathbb{F}$ be a field extension with $[\mathbb{E} : \mathbb{F}] = 2$. Then there exists $\alpha \in \mathbb{E}$ but not in $\mathbb{F}$. Since $[\mathbb{E} : \mathbb{F}] = 2$, $\mathbb{E} = \mathbb{F}(\alpha)$. Then there exist an irreducible polynomial $f(x)$ over $\mathbb{F}$ with α as a root and hence all roots are in $\mathbb{E}$. Therefore, $\mathbb{E} \mid \mathbb{F}$ is a Galois extension.
2. The Galois extensions need not be transitive that is, if $\mathbb{F} \subseteq \mathbb{B} \subseteq \mathbb{E}$ and $\mathbb{E} \mid \mathbb{B}, \mathbb{B} \mid \mathbb{F}$ are Galois, then $\mathbb{E} \mid \mathbb{F}$ need not be Galois. For example, let α be a square root of 2 and β be a fourth root of 2. Clearly $\mathbb{Q}(\alpha)$ is a splitting field of $x^2 - 2$ over $\mathbb{Q}$ and $\mathbb{Q}(\beta)$ is a splitting field of $x^4 - \alpha$ over $\mathbb{Q}(\alpha)$, therefore $\mathbb{Q}(\beta) \mid \mathbb{Q}(\alpha)$ and $\mathbb{Q}(\alpha) \mid \mathbb{Q}$ are Galois extensions but $\mathbb{Q}(\beta) \mid \mathbb{Q}$ is not a Galois extension because $\mathbb{Q}(\beta)$ has a root β of $x^4 - 2 \in \mathbb{Q}[x]$ but not containing other two complex roots.

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.