INVERSE GALOIS PROBLEM WITH VIEWPOINT TO GALOIS THEORY AND IT'S APPLICATIONS

Dr. Ajay Kumar Gupta[1], Vinod Kumar[2]

[1] *Associate Professor, Bhagwant Institute of Technology, Muzaffarnagar,Uttar Pradesh, India*
[2] *Research Scholar, Deptt. Of Mathematics, Bhagwant University, Ajmer, Rajasthan, India*

ABSTRACT

In this paper we are presenting a review of the inverse Galois Problem and its applications. In mathematics, more specifically in abstract algebra, Galois Theory, named after Évariste Galois, provides a connection between field theory and group theory. Using Galois Theory, certain problems in field theory can be reduced to group theory, which is, in some sense, simpler and better understood. Originally, Galois used permutation groups to describe how the various roots of a given polynomial equation are related to each other. Galois Theory is the algebraic study of groups that can be associated with polynomial equations.
In this survey we outline the milestones of the Inverse Problem of Galois theory historically up to the present time. We summarize as well the contribution of the authors to the Galois Embedding Problem, which is the most natural approach to the Inverse Problem in the case of non-simple groups.

Keyword : - *Problem, Contribution, Field Theory, and Simple Group etc.*

1. INTRODUCTION

The inverse problem of Galois Theory was developed in the early 1800's as an approach to understand polynomials and their roots. The inverse Galois problem states whether any finite group can be realized as a Galois group over $\mathbb{Q}$ (field of rational numbers). There has been considerable progress in this as yet unsolved problem. Here, we shall discuss some of the most significant results on this problem. This Thesis also presents a nice variety of significant methods in connection with the problem such as the Hilbert irreducibility theorem, Noether's problem, and rigidity method and so on. We give a self-contained elementary solution for the inverse Galois problem over the field of rational functions over the complex numbers. We will explicate Galois Theory over the complex numbers. We assume a basic knowledge of algebra, both in the classic sense of division and remainders of polynomials, and in the sense of group theory. Although the build-up to the result which we want is quite long, the subject matter along with its historical place in mathematics provides strong motivation. Galois Theory has applications in classic problems such as squaring the circle and determining solvability of polynomials (its original purpose), as well as in number theory, differential equations, and algebraic geometry. Moreover, in the history of mathematics, Galois Theory was one of the things which sparked the modern understanding of groups, and as a result Galois is regarded as one of the founders of modern algebra. Cox (mathematics, Amherst College) covers both classic applications of the theory and some of the more novel approaches. He begins with polynomials in the theory's foundations, cubic equations, advancing to symmetric polynomials and the roots of polynomials. He precedes explaining fields, including extension fields, normal and separable extensions, the Galois group, and Galois correspondence. Topics in applications include solvability by radicals, cyclotomic extensions, geometric constructions and finite fields. He then considers the work of Lagrange, Galois and Kronecker in concert, the process of computing Galois groups, solvable permutation groups, and the lemniscates, including the lemniscates function, complex multiplication and Abel's theorem.
Galois Theory" covers classic applications of the theory, such as solvability by radicals, geometric constructions, and finite fields. The book also delves into more novel topics, including Abel's theory of Abelian equations, the problem of expressing real roots by real radicals (the casus irreducible), and the Galois Theory of origami. Anyone

fascinated by abstract algebra will find careful discussions of such topics as: The contributions of Lagrange, Galois, and Kronecker How to compute Galois groups Galois's results about irreducible polynomials of prime or prime-squared degree Abel's theorem about geometric constructions on the lemniscates.

2. INVERSE GALOIS PROBLEM

All finite groups do occur as Galois groups. It is easy to construct field extensions with any given finite group as Galois group, as long as one does not also specify the ground field.
For that, choose a field K and a finite group G. Cayley's theorem says that G is (up to isomorphism) a subgroup of the symmetric group S on the elements of G. Choose indeterminate $\{x_\alpha\}$, one for each element α of G, and adjoin them to K to get the field $F = K(\{x_\alpha\})$. Contained within F is the field L of symmetric rational functions in the $\{x_\alpha\}$. The Galois group of F/L is S, by a basic result of Emil Artin. G acts on F by restriction of action of S. If the fixed field of this action is M, then, by the fundamental theorem of Galois Theory, the Galois group of F/M is G *[13]*.
It is an open problem to prove the existence of a field extension of the rational field Q with a given finite group as Galois group. Hilbert played a part in solving the problem for all symmetric and alternating groups. Igor Shafarevich proved that every solvable finite group is the Galois group of some extension of Q. Various people have solved the inverse Galois problem for selected non-abelian simple groups. Existence of solutions has been shown for all but possibly one (Mathieu group M_{23}) of the 26 sporadic simple groups. There is even a polynomial with integral coefficients whose Galois group is the Monster group.

3. APPLICATION OF GALOIS THEORY

The birth and development of Galois Theory was caused by the following question, whose answer is known as the Abel Ruffini Theorem:

- Why is there no formula for the roots of a fifth (or higher) degree polynomial equation in terms of the coefficients of the polynomial, using only the usual algebraic operations (addition, subtraction, multiplication, division) and application of radicals (square roots, cube roots, etc)?
- Galois theory not only provides a beautiful answer to this question, it also explains in detail why it *is* possible to solve equations of degree four or lower in the above manner, and why their solutions take the form that they do. Further, it gives a conceptually clear, and often practical, means of telling when some particular equation of higher degree can be solved in that manner.
- Galois Theory also gives a clear insight into questions concerning problems in compass and straightedge construction. It gives an elegant characterization of the ratios of lengths that can be constructed with this method. Using this, it becomes relatively easy to answer such classical problems of geometry as
- Which regular polygons are constructible polygons?
- Why is it not possible to trisect every angle using a compass and straightedge?

4. VIEWPOINT TO GALOIS THEORY

Given a polynomial, it may be that some of the roots are connected by various algebraic equations. For example, it may be that for two of the roots, say A and B, that $A^2 + 5B^3 = 7$. The central idea of Galois Theory is to consider those permutations (or rearrangements) of the roots having the property that *any* algebraic equation satisfied by the roots is still satisfied after the roots have been permuted. An important provision is that we restrict ourselves to algebraic equations whose coefficients are rational numbers. (One might instead specify a certain field in which the coefficients should lie but, for the simple examples below, we will restrict ourselves to the field of rational numbers.)

5. PRESENT MOVE TOWARD BY FIELD THEORY

In the modern approach, one starts with a field extension L/K (read: L over K), and examines the group of field automorphisms of L/K (these are bijective ring homomorphisms $\alpha: L \to L$ such that $\alpha(x) = x$ for all x in K). See the article on Galois groups for further explanation and examples.
The connection between the two approaches is as follows. The coefficients of the polynomial in question should be chosen from the base field K. The top field L should be the field obtained by adjoining the roots of the polynomial in

question to the base field. Any permutation of the roots which respects algebraic equations as described above gives rise to an automorphism of *L*/*K*, and vice versa.
In the first example above, we were studying the extension Q (√3)/Q, where Q is the field of rational numbers, and Q (√3) is the field obtained from Q by adjoining √3. In the second example, we were studying the extension Q (*A, B, C, and D*)/Q.
There are several advantages to the modern approach over the permutation group approach.

- It permits a far simpler statement of the fundamental theorem of Galois Theory.
- The use of base fields other than Q is crucial in many areas of mathematics. For example, in algebraic number theory, one often does Galois Theory using number fields, finite fields or local fields as the base field.
- It allows one to more easily study infinite extensions. Again this is important in algebraic number theory, where for example one often discusses the absolute Galois group of **Q**, defined to be the Galois group of *K*/Q where *K* is an algebraic closure of Q.
- It allows for consideration of inseparable extensions. This issue does not arise in the classical framework, since it was always implicitly assumed that arithmetic took place in characteristic zero, but nonzero characteristic arises frequently in number theory and in algebraic geometry.
- It removes the rather artificial reliance on chasing roots of polynomials. That is, different polynomials may yield the same extension fields, and the modern approach recognizes the connection between these polynomials.

6. DIFFRENCE BETWEEN PURE MATHEMATICS AND APPLIED MATHEMATICS

There are two separate disciplines within the general subject area – Pure Mathematics and Applied Mathematics. You may choose units from either or both disciplines.
If you enjoy problem solving, working with computers and using your mathematics to deal with real applications in science, engineering, economics and biology then you should consider enrolling in some Applied Mathematics units. You will attain a high level of mathematical expertise and a good deal of practical computer experience, both of which will stand you in good stead in a wide variety of possible careers, for example in computing, finance, telecommunications and mathematics research.
If you appreciate the elegance of conceptual reasoning, or enjoy the challenge of abstract problems, you should consider enrolling in some Pure Mathematics units. They are wise choices not only for those whose principal interest lies in mathematics itself, but for all who wish to extend their reasoning ability: many students whose main interests lie in other disciplines find Pure Mathematics an ideal second major. A wide variety of pure units are offered, at both Advanced and Normal levels, covering all major branches of mathematics.

7. THE PRIMARY THEOREM OF GALOIS THEORY

Proposition: Let F be a field, and let G be a subgroup of Aut(F). Then
$\{ a \in F \mid \theta(a) = a \text{ for all } \theta \in G \}$
is a subfield of F [18].
Definition: Let F be a field, and let G be a subgroup of Aut (F). Then
$\{ a \in F \mid \theta(a) = a \text{ for all } \theta \in G \}$
is called the G-fixed subfield of F, or the G-invariant subfield of F, and is denoted by F^G.
Proposition: The polynomial f(x) in K[x] has no multiple roots if and only if gcd(f(x),f'(x)) = 1.
Proposition: Let f(x) be an irreducible polynomial over the field K. Then f(x) has no multiple roots unless chr(K) = $p \neq 0$ and f(x) has the form
$f(x) = a_0 + a_1 x^p + a_2 x^{2p} + \cdots + a_n x^{np}$.

8. CONCLUSIONS

In this paper we are discussing the inverse Galois problem and its application to view point of Galois thery. We also describe in this paper the primary theorem of Galois Theory. There are two separate disciplines within the general subject area – Pure Mathematics and Applied Mathematics. It permits a far simpler statement of the fundamental theorem of Galois Theory. Some of the roots are connected by various algebraic equations. For example, it may be that for two of the roots, say *A* and *B*, that $A^2 + 5B^3 = 7$. If you appreciate the elegance of conceptual reasoning, or

enjoy the challenge of abstract problems, you should consider enrolling in some Pure Mathematics units. It permits a far simpler statement of the fundamental theorem of Galois Theory.

9. REFERENCES

[1]. R. Biggers and M. Fried, "Moduli spaces of covers and the Hurwitz monodromy group," Crelles Journal335 , 87–121, 1982.

[2]. M.D. Fried and H. Volklein, "The inverse Galois problem and rational points on moduli spaces," Math. Annalen290, 771–800, 1991.

[3]. H. Volklein, "Review of Malle/Matzat: "Inverse Galois Theory," BAMS 38, 245–250, 2001.

[4]. M.D. Fried, " Fields of definition of function fields and Hurwitz families and groups as Galois groups," Communications in Algebra 5 , 17–82, 1977.

[5]. H. Volklein, "Groups as Galois Groups, 53, Cambridge Studies in Advanced Mathematics," Camb. U. Press, Camb. England, 1996.

[6]. Alexander M. Macbeath, "Extensions of the Rationals with Galois Group $PGL(2,Z_n)$," Bull. London Math. Soc., 1, 332-338, 1969.

[7]. Gunter Malle and B. Heinrich Matzat, "Inverse Galois Theory," Springer, 1999.

[8]. Helmut Völklein, "Groups as Galois Groups: An introduction," Cambridge University Press, 1996.

[9]. http://mathworld.wolfram.com/Trisection.html (trisecting angles, no proofs) no proofs) 2013.

[10]. http://mathworld.wolfram.com/Constructible Polygon.html (constructible polygons) 2014.

[11]. http://www.cut-the-knot.org/arithmetic/ rational.shtml (constructible numbers, with proofs) 2012.

[12]. http://www.cut-the-knot.com/arithmetic/ cubic.shtml (trisecting angles, with proofs) 2014.

[13]. Berndt, Bruce C. (with Rankin, Robert A.) Ramanujan, "Letters and commentary. History of Mathematics," 9. American Mathematical Society,Providence,RI; London Mathemcatical socirty, London, 1995.xiv+347pp, 1995.

[14]. Cobb, George W. and Moore, David S "Mathematics, Statistics, and Teaching". The American Mathematical Monthly **104** (9): pp. 801-823. http://www.jstor.org/stable/2975286.1997.

[15]. D. Harbater, "Fundamental groups and embedding problems in characteristic p," Recent Developments in the Inverse Galois Problem (Seattle, WA, 1993), Contemp. Math. 186, 353-369, 1995.