International Journal of Engineering & Scientific Research
Vol. 10 Issue 8, August 2022,
ISSN: 2347-6532 Impact Factor: 6.660
Journal Homepage: http://esrjournal.com, Email: esrjeditor@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

A study on fundamental theorem of Galois Theory

Dr. Sudesh Rathee, Associate professor,

G.C.W. Bahadurgarh, Distt. Jhajjar, Haryana

ABSTRACT

Galois theory is based on a remarkable correspondence between subgroups of the Galois group of an extension E/F and intermediate fields between E and F . In this section we will set up the machinery for the fundamental theorem. [A remark on notation: Throughout the chapter, the composition τ σ of two autom𝜗rphisms will be written as a product τσ.] E'mile Picard and Ernest Vessiot were the ones who first presented the Galois hypothesis. In this particular instance, the group that is associated with the differential equation is an algebraic group that is linear, and a characterisation of equations that may be solved by quadratures is provided in terms of the Galois group. Clarification of the Picard-Vessiot theory was provided by Ellis Kolchin in the middle of the 20th century. Kolchin was also responsible for laying the foundations for the theory of linear algebraic groups. Kolchin produced the Fundamental Theorem of Picard-Vessiot theory by using the differential algebra constructed by Joseph F. Ritt. This theorem is the equivalent of its namesake theorem in polynomial Galois theory. According to the basic theorem of Galois theory, the structure of extensions of a field F is precisely the same as the structure of subgroups of the group of automorphisms of the field. This is what the theory tells us about the relationship between these two structures. F.

Keyword: fundamental theorem; of Galois theory

INTRODUCTION

We begin by presenting a few traditional approaches to the solution of certain differential equations, and then we show how these approaches may be unified by associating with the equation a set of transformations that leave the equation unchanged. This concept, which may be attributed to Sophus Lie, was the impetus for the development of differential Galois theory. Therefore, information about the characteristics of the solutions may be obtained from the group that is connected with the differential equation. However, the vast majority of differential equations do not permit the transformation of a nontrivial collection of variables. In the situation of ordinary homogeneous linear differential equations, there is a Galois theory that may be used to solve the problem to one's satisfaction. This theory was first presented by Emile Picard and Ernest Vessiot. In this particular instance, the group that is associated with the differential equation is an algebraic group that is linear, and a characterisation of equations that may be solved by quadrature is provided in terms of the Galois group. Clarification of the Picard-Vessiot theory was provided by Ellis Kolchin in the middle of the 20th century. Kolchin was also responsible for laying the foundations for the theory of linear algebraic groups. Kolchin produced the Fundamental Theorem of Picard-Vessiot theory by using the differential algebra constructed by Joseph F. Ritt. This theorem is the equivalent of its namesake theorem in polynomial Galois theory. In our lecture notes, we construct the Picard-Vesiot theory from a fundamentalist perspective, using the contemporary theory of algebraic groups as the foundation. Graduate students who already have some experience with abstract algebra and differential equations are the primary audience for these materials. The appendices cover the required concepts of algebraic geometry as well as linear algebraic group theory.

We begin by introducing differential rings and differential extensions, and then proceed to examine differential equations that may be defined over any differential field. In chapter 3, we demonstrate that it is possible to associate an ordinary linear differential equation with a differential field K, of characteristic 0, and an algebraically closed field of constants with a uniquely determined minimal extension L of K that contains the solutions to the equation. This extension is known as the Picard-Vessiot extension. In chapter 4, we introduce the differential Galois group of an ordinary linear differential equation defined over the field K as the group of differential Automorphisms of its PicardVessiot extension L and prove that it is a linear algebraic group. This is done by defining the differential Galois group as the group of differential Automorphisms of its PicardVessiot extension L. The fundamental theorem of Picard-Vessiot theory is shown in chapter 5. This theorem establishes a bijective relationship between the intermediate fields of a Picard-Vessiot extension and the Zariski closed subgroups of the Galois group associated with that extension. In chapter 6, we provide a characterisation of homogeneous linear differential equations solvable by quadrature's in terms of their differential Galois group. This characterization is given for homogeneous linear differential equations. These lecture notes were derived from the authors' experiences teaching differential Galois theory at the University of Barcelona and the Cracow University of Technology. During the academic year 2006-2007, some aspects of them were discussed in the Differential Galois Theory Seminar held at the Mathematical Institute of the Cracow University of Technology. The authors of these notes would like to extend their gratitude to the participants of the DGT Seminar, in particular Dr. Marcin Skrzynski and Dr. Artur Pekosz, who provided insightful feedback on an earlier version of these notes. During the time that they spent working on this monograph, both of the writers had their efforts subsidised by grants from Poland (N20103831/3261) and Spain (MTM200604895). Teresa Crespo was provided financial assistance from the Spanish fellowship PR20060528 when she was a student at the Cracow University of Technology.

Fixed Fields and Galois Groups

The fundamental tenet of Galois theory is that there exists a striking correlation between the subgroups of the Galois group of an extension E/F and the intermediate fields that exist between E and F. In this part of the article, we are going to provide the groundwork for the basic theorem. [A comment about the notation that follows: The composition continues all the way through the chapter. τ σ of two automorphisms will be written as a product $\tau\sigma$.]

Definitions and Comments

Let G = Gal(E/F) represent the Galois group associated with the extension E/F. The fixed field of H is the set of elements that are fixed by every automorphism in H, which means that if H is a subgroup of G, the fixed field of H is G.,

$F(H) = \{x \in E : \sigma(x) = x \text{ for every } \sigma \in H\}$.

If K is an intermediate field, that is, $F \leq K \leq E$, define

$G(K) = Gal(E/K) = \{\sigma \in G : \sigma(x) = x \text{ for every } x \in K\}$.

I like the term "fixing group of K" for G(K), since (K) is the collection of automorphisms of E that maintain the original value of K. The subject matter of Galois theory is the connection between fixed fields and fixing groups. In particular, the following finding implies that the biggest subgroup corresponds to the smallest subfield F. This was found by comparing the two. G.

Proposition

Let E/F be a finite Galois extension with Galois group G = Gal(E/F). Then

The fixed field of G is F ;

If H is a proper subgroup of G, then the fixed field of H properly contains F .

Proof. (iLet the fixed field of G be denoted by F0. If is a F automorphism of E, then according to the definition of F0, resolves all of the issues with F0. Because of this, the F automorphisms of G are identical to the F0 automorphisms of G. Now, using (3.4.7) and (3.5.8), we can establish that E/F0 is Galois. According to (3.5.9), the degree of a finite Galois extension is equal to the size of the Galois group that the extension contains. As a result, [E: F] = [E: F0], and according to (3.1.9), F = F0..

(ii) Suppose that F = F(H). By the theorem of the primitive element (3.5.12), we ve $E = F(\alpha)$ for some $\alpha \in E$. Define a polynomial $f(X) \in E[X]$ by $f(X) = \sigma \in H - \sigma(\alpha))$.

If τ is any automorphism in H, then we may apply τ to f (that is, to the coefficients of f ; we discussed this idea in the proof of (3.5.2)). The result is $(\tau f)(X) = \sigma \in H - (\tau\sigma)(\alpha))$.

But as σ ranges over all of H, so does $\tau\sigma$, and consequently $\tau f = f$. Thus each coefficient of f is fixed by H, so f F [X]. Now α is a root of f , since X $\sigma(\alpha)$ is 0 when $X = \alpha$ and σ is the identity. We can say two things about the degree of f :

By definition of f , deg f = H < G = [E : F], and, since f is a multiple of the minimal polynomial of α over F ,

$\deg f \geq [F(\alpha) : F] = [E : F]$, and we have a contradiction.

There is a converse to the first part of (6.1.2).

Proposition

Let E/F be a finite extension with Galois group G. If the fixed field of G is F , then E/F

is Galois.

Proof. Let G = σ1,..., σn , where σ1 is the identity. To show that E/F is normal, we consider an irreducible polynomial f F [X] with a root α E. Apply each au to morphism in G to α, and suppose that there are r distinct images α = α1 = σ1(α), α2 = σ2(α),..., αr = σr(α). If σ is any member of G, then σ will map each αi to some αj, and since σ is an injective map of the finite set α1,..., αr to itself, it is surjective as well. To put it simply, σ permutes the αi. Now we examine what σ does to the elementary symmetric functions of the αi, which are given byΣre1 =Σαi, e2 =αiαj, e3 =iαjαk,... i=1<jrer =i=1αi.i<j<k

Since σ permutes the αi, it follows that σ(ei) = ei for all i. Thus the ei belong to the fixed field of G, which is F by hypothesis. Now we form a monic polynomial whose roots are the αi:

g(X) = (X − α1) ··· (X − αr) = Xr − e1Xr−1 + e2Xr−2 − ··· + (−1)rer.

Since the ei belong to F , g F [X], and since the αi are in E, g splits over E. We claim that g is the minimal polynomial of α over F . To see this, let h(X) = b0+b1X+ +bmXm be any polynomial in F [X] having α as a root. Applying σi to the equation

b0 + b1α + bmαm = 0

we have

b0 + b1αi + ··· bmαm = 0, so that each αi is a root of h, hence g divides h and therefore g =min(α, F). But our original polynomial f F [X] is a constant multiple of g since it is irreducible and has the root as part of its expression. Therefore, f divides across E, demonstrating that the ratio of E to F is typical. There are no repeating roots in g since the I I = 1,..., and r are all separate. Therefore, it can be shown that is separable over F, which demonstrates that the extension E/F is also separable. It is worthwhile to do a more in-depth investigation of basic symmetric functions.

OBJECTIVE OF THE STUDY

1. To concentrate one's attention on an explicit formula for the resolvent cubic
2. To do research pertaining to Fixed Fields and Galois Groups

International Journal of Engineering & Scientific Research
Vol. 10 Issue 8, August 2022,
ISSN: 2347-6532 Impact Factor: 6.660
Journal Homepage: http://esrjournal.com, Email: esrjeditor@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Theorem

Let f be a symmetric polynomial in the n variables X1,..., Xn. [This means that if σ is any permutation in Sn and we replace Xi by Xσ(i) for i = 1,..., n, then f is unchanged.] If e1,..., en are the elementary symmetric functions of the Xi, then f can be expressed as a polynomial in the ei.

Proof. We give an algorithm. The polynomial f is a linear combination of monomials

of the form Xr1 $\cdot_1\cdot$ Xrn $_n$ and we order the monomials lexicographically: $_1$Xr1 $\cdot\cdot_n$ Xrn >

Xs1 $\cdot_1\cdot$ Xsn$_n$ iff the first disagreement between ri and si results in ri > si. Since f is

symmetric, all terms generated by applying a permutation σ ∈ Sn to the subscripts of

Xr1 $\cdot_1\cdot$ Xrn$_n$ will furthermore make a contribution to f. By deducting an expression of the type, the goal is to get rid of the leading words, which are the ones that are linked with the monomial that comes first in the ordering. et1 et2 ⋯ etn = (X1 + ⋯ + Xn)t1 ⋯ (X1 ⋯ Xn)tn1 2 n

which has leading term

Xt1 (X1X2)t2 (X1X2X3)t3 ⋯ (X1 ⋯ Xn)tn = Xt1+⋯+tn Xt2+⋯+tn ⋯ Xtn.

This will be possible if we choose1 2 n

t1 = r1 − r2, t2 = r2 − r3, . .., tn−1 = rn−1 − rn, tn = rn.

Following the application of the subtraction operation, the resultant polynomial contains a leading term that falls in the lexicographic ordering below Xr1 > Xrn. After that, we may go on with the process, which must be completed in a certain number of stages. Corollary

If g is a polynomial in F [X] and f (α1,..., αn) is any symmetric polynomial in the roots

α1,..., αn of g, then f ∈ F [X].

Proof. It is safe to assume, without limiting ourselves in any way, that g is monic. After that, in a field that is divided by g, we have

g(X) = (X − α1) ⋯ (X − αn) = Xn − e1Xn−1 + ⋯ + (−1)nen.

By (6.1.4), f is a polynomial in the ei, and since the ei are simply ± the coefficients of g, the coefficients of f are in F .

The explicit formula for the resolvent cubic is as follows:

g(X) = X3 − 2qX2 + (q2 − 4s)X + r2.

We need some results concerning subgroups of Sn, n ≥ 3.

Lemma An is produced by three cycles, and each of those three cycles constitutes a commutator.

An is the sole subgroup of Sn that has an index value of 2.

Proof. Please refer to Section 5.6, Problem 4 on the first statement of I Regarding the second statement of item I please be aware that

$(a, b)(a, c)(a, b)^{-1}(a, c)^{-1} = (a, b)(a, c)(a, b)(a, c) = (a, b, c)$.

To prove (ii), let H be a subgroup of Sn with index 2; H is normal by Section 1.3, Problem 6. Thus Sn/H has order 2, hence is abelian. But then by (5.7.2), part 5,

$Sn' \leq H$, and since An also has index 2, the same argument gives $Sn' \leq An$. By (i),$An \leq Sn'$, so $An = Sn' \leq H$. It stands to reason that H is equivalent to An given that both An and H contain the same finite number of elements, n!/2. A6.11 Proposition

Let there be a subgroup of S4 called G whose order is a multiple of 4, and let there be a group V consisting of the number four (see the discussion preceding A6.7). Let the order of the quotient group be denoted by m. G/(G V).

Then

If m = 6, then G = S4;

If m = 3, then G = A4;

If m = 1, then G = V ;

If m = 2, then G = D8 or Z4 or V ;

If G acts transitively on 1, 2, 3, 4 , then the case G = V is excluded in (d). [In all cases, equality is up to isomorphism.]

Proof. If m = 6 or 3, then since $|G| = m|G \cap V|$, 3 is a divisor of |G|. By hypothesis, 4 is also a divisor, so |G| is a multiple of 12. By A6.10 part (ii), G must be S4 or A4. But

$|S4/(S4 \cap V)| = |S4/V| = 24/4 = 6$

and

$|A4/(A4 \cap V)| = |A4/V| = 12/4 = 3$

proving both (a) and (b). If m = 1, then G = G V , so G V , and since G is a multiple of 4 and V = 4, we have G = V , proving (c).

If m = 2, then G = 2 G V , and since V ∩ = 4, G V | is| 1, 2 or 4. If it is 1, then G = 2 1 = 2, contradicting the hypothesis. If it is 2, then G = 2 2 = 4, and G = Z4 or V (the only groups of order 4). Finally, let's suppose that G V = 4, which gives us G = 8. However, a subgroup of S4 of rank 8 is a Sylow 2subgroup, and all conjugate subgroups of this kind are isomorphic because of this property. Due to the fact that the dihedral group of order 8 is a group of permutations of the four vertices of a square, one of these subgroups is denoted by the letter D8. That demonstrates (d).

According to the orbit-stabilizer theorem, if m = 2, G operates transitively on 1, 2, 3, 4, and G = 4, then each stabiliser subgroup G(x) is trivial (since there is only one orbit, and its size is 4). Therefore, any permutation in G other than the identity shifts every integer by one, two, three, or four places. Since

|G V | = 2, G consists of the identity, an extra component of V, and two components that are not present in V; the last two must both be 4cycles. Both of these components must be 4cycles. On the other hand, given that the order of a 4cycle is 4, this proves that G must be cyclic. (e).**Theorem**

Consider the quartic f to be an irreducible separable group that belongs to the Galois group G. Take the order of the Galois group associated with the resolvent cubic to be m. Then:

If m = 6, then G = S4;

If m = 3, then G = A4;

If m = 1, then G = V ;

If m = 2 and f is irreducible over L = F (u, v, w), where u, v and w are the roots of the resolvent cubic, then G = D8;

If m = 2 and f is reducible over L, then G = Z4.

Proof. By A6.7 and the fundamental theorem, [G : G ∩ V] = [L : F]. Because f and g share the same discriminant, the roots of the resolvent cubic g are now completely separate from one another. As a result, L is a splitting field of a separable polynomial, and the Galois representation of L/F is correct. Therefore, [L: F] = metres by metres (3.5.9). In order to use the formula in (A6.11), we need to make sure that G is a multiple of 4. However, since G works transitively on the roots of f, there is only one orbit, and its size is equal to 4 times G divided by G(x). This is a consequence of the orbit-stabilizer theorem. Now we get (A6.11), which gives us (a), (b), and (c), and if m is equal to two, then G is either D8 or Z4. In order to finish the evidence, let's suppose that m equals 2 and G equals D8. We may consider D8 to be formed by the numbers (1, 2, 3, 4) and (2, 4), with V = 1, (1, 2)(3, 4), (1, 3)(2, 4), and (1, 4)(2, 3) if we consider it to be the group of symmetries of a square with the vertices 1,2,3,4 as our starting point. Therefore, the components that make up the various symmetries of the square belong to D8; thuS V = G∩ V = Gal(E/L) by (A6.7).

[E is a splitting field for f over F .] Since V is transitive, for each i, j = 1, 2, 3, 4, i j, there is an Lautomorphism τ of E such that τ (xi) = xj. Applying τ to the equation h(xi) = 0, where h is the minimal polynomial of xi over L, we see that each xj is a root of h, and therefore f h. But h f by minimality of h, so h = f , proving that f is irreducible over L.

Finally, assume m = 2 and G = Z4, which we take as 1, (1, 2, 3, 4), (1, 3)(2, 4),(1, 4, 3, 2) . Then G V = 1, (1, 3)(2, 4) , which is not transitive. Thus for some i = j, xi and xj are not roots of the same irreducible polynomial over L. In particular, f is reducible over L.

Example

Let f (X) = X4 + 3X2 + 2X + 1 over Q, with q = 3,r = 2,s = 1. The resolvent cubic is, by (A6.9), g(X) = X3 6X2 ± 5X + 4. To calculate the discriminant of g, we can use the general formula in (A6.6), or compute g(X + 2) = (X + 2)3 6(X + 2)2 + 5(X + 2)+4 = X3 7X 2. [The rational root test gives irreducibility of g and restricts a factorization of f to (X2 + aX 1)(X2 aX 1), a Z, which is impossible. Thus f is irreducible as well.] We have D(g) = 4(7)3 27(2)2 = 1264, which is not a square in Q. Thus m = 6, so the Galois group of f is S4.

CONCLUSION

In this particular instance, the group that is associated with the differential equation is an algebraic group that is linear, and a characterisation of equations that may be solved by quadratures is provided in terms of the Galois group. The fundamental tenet of Galois theory is that there exists a striking correlation between the subgroups of the Galois group of an extension E/F and the intermediate fields that exist between E and F. In this part of the article, we are going to provide the groundwork for the basic theorem. We present, in terms of the differential Galois group, a characterisation of homogeneous linear differential equations that may be solved by quadratures. The writers of these lecture notes taught classes on Differential Galois Theory at the University of Barcelona and the Cracow University of Technology, and those classes served as the basis for these lecture notes. During the academic year 2006-2007, the Mathematical Institute of the Cracow University of Technology hosted a seminar called "Differential Galois Theory Seminar." Some of the components of them were presented there. The authors of these notes would like to extend their gratitude to the participants of the DGT Seminar, in particular Dr. Marcin Skrzynski and Dr. Artur Piekosz, who provided insightful feedback on an earlier version of these notes. [A word on notation: throughout the chapter, the composition of two automorphisms will be expressed as a product.] [An example of the composition is shown below.] Clarification of the Picard-Vessiot theory was provided by Ellis Kolchin in the middle of the 20th century. Kolchin was also responsible for laying the foundations for the theory of linear algebraic groups.

REFERENCES

1. H. Bass et al. eds., Selected works of Ellis Kolchin with commentary, American Mathematical Society, 1999.
2. Borel, Linear Algebraic Groups, Graduate Texts in Mathematics 126, Springer, 1991.
3. M.D. Fried, M. Jarden, Field Arithmetic, Ergebnisse der Mathematik und ihrer Grenzgebiete 11, Springer, 1986.
4. K. Hulek, Elementary algebraic geometry, Student Mathematical Li brary vol. 20, American Mathematical Society, 2003.
5. J.E. Humphreys, Linear Algebraic Groups, Graduate Texts in Mathe matics 21, Springer, 1981.
6. E. Hrushovski, Computing the Galois group of a linear differential equa tion, in: T.Crespo, Z. Hajto (eds.), Proceedings of the Differential Galois Theory workshop, Banach Center Publications 58, Warszawa 2002, pp. 97 138.
7. . Kaplansky, An introduction to differential algebra, Hermann, 1976.[Kl] A. Kleshchev, Lectures on Algebraic Groups, http://darkwing.uoregon.edu/ klesh/teaching/AGLN.pdf
8. E.R. Kolchin, On the Galois theory of differential fields, Amer. J. Math. 77 (1955), 868894; [Ba] pp. 261287.
9. E.R. Kolchin, Some problems in differential algebra, Proceedings of the International Congress of Mathematicians, Moscow, 1968, pp.269276: [Ba] pp. 357364.
10. R. Magid, Lectures on Differential Galois Theory, University Lecture Series 7, American Mathematical Society, 1997.
11. J.J. Morales Ruiz, Differential Galois Theory and nonintegrability of Hamiltonian systems, Progress in Mathematics 179, Birkhäuser, 1999.
12. B. Poizat, Les corps différentiellement clos, compagnons de route de la théorie del modèles, [Ba] pp. 555565.
13. M. van der Put, M.F. Singer, Galois Theory of Linear Differential Equations, Grundlehren der mathematischen Wissenschaften 328, Springer,2003.
14. M.F. Singer, Direct and inverse problems in differential Galois theory, pp. 527554.
15. T.A. Springer, Linear Algebraic Groups, Progress in Mathematics 9, Birkhäuser, 1998.
16. H. Ż olądek, The Monodromy Group, Monografie Matematyczne Instytut Matematyczny PAN 67, Birkhäuser, 2006.