Journal of Mathematics and Statistics 4 (4): 245-249, 2008
ISSN 1549-3644

Fundamental Properties of the Galois Correspondence

Ayinde S. Olukayode and Oyekan E. Abiodun
Department of Mathematics and Statistics, Bowen University,
P.M.B 284, Iwo, Osun State, Nigeria

Abstract: Problem Statement: Let K is the splitting field of a polynomial f(x) over a field F and α_n be the roots of f in K. Let G be embedded as a subgroup of the symmetric group ς. We determined the Galois group G, and the subgroup. **Approach:** computed some auxiliary polynomials that had roots in K, where the permutation of a set was considered distinct. The Galois Theory was deduced using the primitive element and Splitting theorems. **Results:** The Galois extension K/L to identity L and its Galois group is a subgroup of G. which was referred to as the main theorem which we proved. **Conclusion:** Hence the findings suggest the need for computing more auxiliary polynomials that have roots.

Key words: Splitting fields, symmetric group, galois group and theory, resolvents.

INTRODUCTION

Let $p_1(u_1, u_2,\ldots,u_n)$ be a polynomial with coefficients in F. The symmetric group ς operates on the polynomial ring F $[u_1, u_2,\ldots u_n]$; Let its orbit under the action of ς be $\{p_1, p_2, \ldots, p_r\}$.

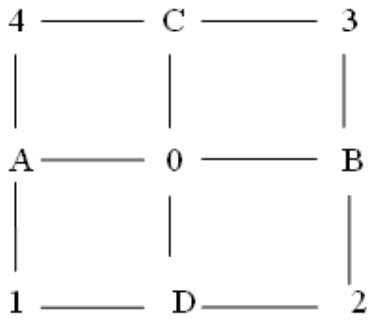
Lemma 1[1]**:** Let $\{p_1, p_2,\ldots p_r\}$ be the orbit of a polynomial $p_i(u_1, u_2,\ldots u_n)$ for the operation of permuting the variables. Let $f(y_1, y_2,.....y_n)$ be a symmetric polynomial in some variables $y_1, y_2, \ldots y_r$. Then $f(p_1, p_2, \ldots p_r)$ is a symmetric polynomial in $u_1, u_2, \ldots u_n$.

Proof: A permutation of $u_1, u_2,\ldots u_n$ permutes the orbit $\{p_1, p_2,\ldots p_r\}$. The corresponding permutation of $y_1, y_2,\ldots y_r$ fixes the symmetric polynomial f.

For example, if $p_1 = u_1u_2$, the orbit of p_1 consists of the products u_iu_j with $i \neq j$. Therefore, we expand the polynomial. $\gamma(x) = (x-p_1)(x-p_2)\ldots(x-p_r)$. Its coefficients are elementary symmetric functions in $p_1, p_2, \ldots p_r$, so they are also symmetric functions of u and can be written in terms of the elementary symmetric functions $s_i(u)$, say $s_j(p_1, p_2,\ldots,p_r) = q_j(s_1,s_2,\ldots s_n)$, where $s_i = s_i(u)$. We make the substitution $u_i = \alpha_i$. Let $\beta_j = p_j(\alpha_1, \alpha_2,\ldots\alpha_n)$ and let $g(x) = (x-\beta_1)\ldots(x-\beta_r) = x^r-b_1x^{r-1}+b_2x^{r-2}+\ldots\pm b_r$.

The coefficients of g are obtained by the same substitution into $q_j(s_1,s_2,\ldots s_n)$, so $b_j = q_j(a_1, a_2, \ldots,a_n)$. Therefore, g(x) has coefficients in F.

Lloyd R. Jaisingh *et al.*[2] show these permutation which are of good example in this result. Consider the square below with vertices denoted by (1,2,3,4) locate its centre 0, the bisectors AOB and COD of its parallel sides and the diagonals 103 and 204. We shall be concerned with all rigid motions (rotations in the plane about 0 and in space about the bisectors and diagonals) such that the square will look the same after the motion as before.



Denote by ω the counterclockwise rotation of the square about 0 through 90^o. Its effect is to have (12), (23), (34), (41), thus ω = (1234). Now $\omega^2 = \omega.\omega$ = (13) (24) is a rotation about O of 180°. ω^3 = (1432) is a rotation of 270° and ω^4 = (1) =V is a rotation about O of 360o or 0°. The rotations through 180° about the bisectors AOB and COD give rise respectively to σ^2 = (14) (23) and τ^2 = (12) (34) while the rotations through 180^o about the diagonals 103 and 204 give rise to e = (24) and b = (13).

Corresponding Author: Ayinde S. Olukayode. Department of Mathematics and Statistics, Bowen University, P. M. B 284, Iwo, Osun State, Nigeria

By the operation of the roots, G embeds as a subgroup of the symmetric group $S_n = \varsigma$, which permutations of the roots come from F-automorphisms of K, where K is a splitting field of the polynomial.

MATERIALS AND METHODS

Computation of auxiliary polynomials: The need for computing the auxiliary polynomials and show that they have roots in F. A permutation z of the set $\{u_1, u_2,\ldots u_n\}$ defines some more permutations:

- Since the α_i are distinct, z can equally well be thought of as a permutation of the set $\{\alpha_1, \alpha_2, \ldots\alpha_n\}$
- Z induces a permutation $\bar{Z}$ of the set $\{p_1, p_2,\ldots P_r\}$.
- Provided that the βj are distinct, $\bar{Z}$ can be used to permute $\{\beta_1, \beta_2,\ldots B_r\}$

Therefore, clearly we can see that Z sends $u_i \rightarrow Zu_i$. Then $\bar{Z}(p_j(u_1, u_2, \ldots u_n) = p_j(zu_1, zu_2, \ldots zu_n)$, which is another one of the polynomials $\{p_1, p_2,\ldots p_k\}$, Assuming that βj are distinct, we substitute $u_1=\alpha_i$: $Z(\beta j) = \bar{Z}(p_j(\alpha_1, \alpha_2, \ldots\alpha_n) = p_j(z\alpha_1, z\alpha_2, \ldots z\alpha_n) = \beta_i$.

Lemma 2: Assume that the βj are distinct. Let σ be an F - automorphism of K and let Z be the permutation of the roots $\{\alpha 1, \alpha_2, \ldots\alpha_n\}$ it defines. Then the permutation $\bar{Z}$ of $\{\beta_1, \beta_2,\ldots\beta_r\}$ determine by z is the one defined by σ too.

Proof:
$$\begin{aligned}\bar{Z}(\beta j) &= p_j(z\alpha_1, z\alpha_2, \ldots z\alpha_n)\\ &= p_j(\sigma\alpha_1, \sigma\alpha_2, \ldots\sigma\alpha_n)\\ &= \sigma(p_j(\alpha_1, \alpha_2, \ldots\alpha_n))\\ &= \sigma(\beta j)\end{aligned}$$

Let H_j be the stabilizer of the polynomial βj for the operation of G. Then if G is not the whole symmetric group ς, then there is no reason to suppose that the set $\{\beta_1, \beta_2,\ldots\beta_r\}$ forms a single G - orbit in K and if not, then g(x) will be reducible. From the general property of group operations, H_j are conjugate subgroups of G, because the polynomials p_j form one orbit.

Theorem 1:[5] With the notation above in lemma 1, suppose that $\beta_1, \beta_2,\ldots\beta_r$ are distinct elements of K. Then $\beta_j \in F$ if and only if G is a subgroup of H_j.

Proof: The theorem follows from the fact that F is the fixed K^G. Let σ be an F- automorphism of K, let z denote the permutation of $\{u_1, u_2,\ldots u_n\}$ which corresponds to the permutation induced by σ on $\{\alpha_1, \alpha_2,\ldots\alpha_n\}$ and let $\bar{Z}$ be the permutation of $\{p_j\}$ induced by z. We apply the lemma, because β_j are distinct, σ fixes β_j if and only if $\bar{Z}$ fixes u_j and this happens if and only if $z \in H_j$. Then $\beta_j \in F$ if and only if β_j is fixed by all $\sigma \in G$, which is true if and only if $G \subset H_j$.

Theorem of symmetric functions:

Lemma 3: Let $p(u_1, u_2,\ldots u_n)$ be a symmetric polynomial with coefficients in F. Then with $\alpha_1, \alpha_2, \ldots,\alpha_n$ as above, that is $\alpha_i \in F$, $p(\alpha_1, \alpha_2,\ldots,\alpha_n) \in F$.

Proof: Theorem 1 tells us that p is a polynomial in the elementary symmetric functions with coefficients in F, say $p(u) = q(s_1, s_2, \ldots s_n)$. Then because $a_i \in F$, $p(\alpha) = q(s_1(\alpha), s_2(\alpha),\ldots s_n(\alpha)) = q(\alpha_1, \alpha_2, \ldots,\alpha_n)$ also in F.

Now let $p(u_1, u_2,\ldots,u_n)$ be an arbitrary polynomial and let its orbit under the action of the symmetric group S_n be $\{p_1,p_2,\ldots.p_r\}$, where $p = p_i$,

Lemma 4: Let $\{p_1,p_2,\ldots p_r\}$ be the orbit of a polynomial in $F[u_1,u_2,\ldots u_n]$ and let $h(w_1,w_2,\ldots w_r)$ be a symmetric function in some variables $w_1,w_2,\ldots w_r$. Then $h(p_1,p_2,\ldots p_r)$ is a symmetric function in $u_1,u_2,\ldots u_n$.

Proof: see J. P. Tignol[6]

Lemma 5: Let $\{p_1,p_2,\ldots p_r\}$ be the orbit of a polynomial $p_i(u_1,u_2,\ldots u_n)$. For $j = 1,2,\ldots r$. Let $\beta_j = P_j(\alpha_1, \alpha_2, \ldots,\alpha_n)$. The polynomial $h(x) = (x - \beta_1)(x - \beta_2)\ldots(x - \beta_r) = x^r - b_1x^{r-1} + b_2x^{r-2} - \ldots \pm b_r$, has coefficients in F.

Proof: We consider the polynomial $H(x) = (x - w_1)\ldots(x - w_r) = x^r - B_1x^{r-1} + B_2x^{r-2} - \ldots \pm B_r$

Its coefficients B_j are the elementary symmetric functions in $w_1, w_2,\ldots w_r$. Our polynomial h(x) is obtained by substituting $w_j = \beta_j$ into H(x). This substitution sends $Bj \rightarrow bj$ and it can be made in two steps $w_j \rightarrow p_j(u) \rightarrow p_j(\alpha) = \beta_j$. Since the coefficients B_j are symmetric polynomials in $w_1,w_2,...w_r$. Lemma 3 and 4 tell us that their images b_j are in F.

With these ideas, we have the following theorem called splitting theorem and it allows us to call to a splitting field K a finite field extension such that any irreducible polynomial over F with one root in K splits completely.

Theorem 2 (Splitting theorem): Let K be a splitting field of a polynomial $f(x) \in F[x]$. If an irreducible polynomial $g(x) \in F[x]$ has one root in K, then it splits completely in K.

Proof: Let β be a root of the irreducible polynomial g(x) in the splitting field K. We write β as a polynomial in α_i, say $\beta = p(\alpha_1, \alpha_2,\ldots.,\alpha_n)$, with $p(u_1,u_2,\ldots..u_n) \in$

$F[u_1,u_2,...u_n]$. Let $\{p_1,p_2,\ldots p_r\}$ be the orbit of $p = p_i$ and let $\beta j = p_j(\alpha_1, \alpha_2, \ldots,\alpha_n)$, so that $\beta = \beta_i$.

Lemma 4 tells us that $h(x) = (x - \beta_1)(x - \beta_2)\ldots(x - \beta_r)$ has coefficients in F. Therefore β is a common root of the two polynomials g and h in F[x]. Since g is irreducible, it divides any polynomial in F[x] which has β as a root. Therefore, g divides h. Since h splits completely in K, so does g.

Main theorem of galois theory:

Proposition 1: Let $\sigma : K \to K^{l}$' be an F - isomorphism between extensions fields of F, let f be a polynomial in F[x] which has α root, $\alpha \in K$. Then σα is a root of f in' K^{l}.

Proposition 2: Let f be an irreducible polynomial F[x] and let K and K^{l} be field extension of F in which f has roots, say $\alpha \in K$ and $a^{l} \in K^{l}$. Suppose that $K = F[\alpha]$ and $K^{l} = [a^{l}]$. There is a unique F - isomorphism $\alpha : K \to K^{l}$ such that $\sigma\alpha = a^{l}$.

Remark: From above, any finite field extensions turned out to be generated by one element. Such an element, if it exists, is called a primitive element. Hence to see that under mild restrictions primitive element exists.

Theorem 3[3]**:** (Primitive Element Theorem) Let K/F be a finite extension. An element $\alpha \in K$ for which $K = F[\alpha]$ exists if and only if there exist only finitely many intermediate fields G: $K \supset G \supset F$. If K is separable over F then such an element exist.

Proof: If F is finite then K is also finite and therefore the multiplicative group of K is generated by one element which is then primitive. So let us assume that F is infinite.

Suppose that there exist only finitely many fields intermediate between K and F. Let $\alpha, \beta \in K$. For $c \in K$ there exist only finitely many fields of the form $F(\alpha + c\beta)$. Therefore there are $c_1, c_2, \in F$, $c_1 \neq c_2$ and such that $F(\alpha + c_1\beta) = F(\alpha + c_2\beta)$.

Note that $\alpha+c_1\beta$ and $\alpha+c_2\beta$ belong to the same field, hence $(c_1-c_2)\beta$ also belongs to this field and therefore β does so as well. Thus, α also belongs to the same field and it follows that
F (α, β) is generated by one element (e.g. $\alpha + c_1\beta$). An obvious induction shows that any intermediate field generated by finitely many elements (in particular, K itself is generated by one element).

Conversely, suppose that $K = F[\alpha]$ for some α. Let m(x) be the minimal polynomial of α over F. For any intermediate field G consider $m_G(x)$, the minimal polynomial of α over G. Clearly, m_G divides m. Since there are only finitely many (monic) divisors of m we obtain a map

$G \mapsto m_G$ from the set of intermediate fields into a finite set of polynomials. Let G_0 be the subfield in G generated by the coefficients of the polynomial m_G. Then m_G in G_0 and it is irreducible over G_0 since it is even irreducible over G. Therefore the degree of α over G is the same as the degree of α over G_0. It follows that $G_0 = G$. We conclude that G is determined uniquely by m_G and therefore the above map is injective. This finishes the proof of the first statement of the theorem.

Now suppose that K is separable over F. Using induction, the general case is reduced to the one when $K = F(\alpha, \beta)$ where α, β are separable over F. let σ_1, $\sigma_2,\ldots\sigma_r$ different embeddings of F into the normal closure of K. (Using the condition that $K \supset F$ is separable)

Set $P(x) = \prod_{i\neq j}(\sigma_i(\alpha) + x\sigma_i(\beta) - \sigma_j(\alpha) - x\sigma_j(\beta))$.

Clearly, P(x) is a nonzero polynomial and therefore there exists an element $c \in F$ for which $P(c) \neq 0$. Then the elements $\sigma_i(\alpha + c\beta)$ are all different and therefore $F(\alpha + c\beta)$ has degree over F no less that n. However n = [F (α, β): F] and therefore F (α, β) = F(c).

Theorem 4: [7] Let K/F be a finite extension and let G be the group of F - automorphisms of K. Then $|G| \leq [K:F]$ and $|G|=[K:F]$ if only if K is a splitting field over F.

Proof: Let n = |G| and N = [K:F]. By the primitive Element Theorem, $K = F[\alpha]$ for some α. Let f(x) be the irreducible polynomial for α over F. Then deg f = deg α = N. let $\alpha_1, \alpha_2, \ldots,\alpha_r$ be the roots of f in K, with $\alpha_1 = \alpha$. We don't know how many roots there are except that $r \leq N$. Let $K=F[\alpha_i]$ for any i, because $[F[\alpha i]: F] = N$ too. Proposition 1 tells us that an element of G sends $\alpha_1 \to \alpha_i$ for some i and proposition 2 tells us that there is a unique F - isomorphism α_i: $K \to K$ sending $\alpha_1 \to \alpha_i$. The elements of G are $\{\sigma_1, \sigma_2,\ldots\sigma_r\}$. This shows that $u = r \leq N$. If K is a splitting field, then f splits completely in K and n = r = N.

Theorem 5: Let G be a finite group of automorphisms of a field K and let $F = K^G$ be its fixed field. Let $\alpha \in K$ have G - orbit $\{\alpha_1, \alpha_2,\ldots,\alpha_r\}$, with $\alpha_i = \alpha$. Then (i) $f(x) = (x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_r)$ is the irreducible polynomial for α over F. (ii) α is algebraic and of degree r over F, and $r \leq |G|$

Proof: Let g(x) be the irreducible polynomial for α_1 over F. Then α_i is a root of g for all i. This follows from proposition 1. So the degree of g is at least r.

The coefficients of f(x) are the elementary symmetric functions in $\alpha_1, \alpha_2, \ldots, \alpha_r$. An element $\sigma \in G$ permutes this orbit, so it fixes the coefficients of f, which shows that $f \in F[x]$. Because g is irreducible and g, f have a common root, g divides f. Therefore the degree of g is at most r. It follows that the degree of g is equal to r and that g = f. Then the degree of α over F is also r.

Theorem 6:[4] let F be the fixed field of a finite group G of automorphisms of a field K. Then K is a Galois extension of F and its Galois group is G.

Proof: Let n= IGI and N=[K:F]. Because the elements of G act as the identity on F, they are F-automorphisms. So $G \subset G(K/F)$. From theorem 4, it clears that $n \leq N$. let F' be an intermediate field, $F \subset F' \subset K$, which is obtained from F by adjoining some finite set of elements of K. Since every element of K is algebraic over F, F' is a finite extension of F and by the Primitive Element Theorem (Theorem 3), F'= F[γ] for some $\gamma \in K$. By theorem 5, the degree of γ is at most n. Hence $[F': F] \leq n$

However, we form a chain of intermediate fields $F < F_1 < F_2 < \ldots$ as follows: If F < K, we choose an element $\beta 1 \in K$ which is not in F and we set $F_1 = F[\beta_1]$. If $F_1 <$ K, choose an element $\beta_2 \in K$ which is not in F_1 and we set $F_2 = F_1[\beta_2]$, etc…If $F_i = K$ at some stage, we stop. Let $d_i = [F_i: F]$. Then $d1 < d2 < \ldots$, because F_i is generated over F by finitely many elements. Theorem 4 tells us that $d_i \leq n$ Therefore the chain must be finite and it ends with some $F_i = K$. Hence $N = d_i \leq n$ and so n = N.

Theorem 7: let K/F be a Galois extension, with Galois group G. Then F is the fixed field K^G.

Proof: Let n = IGI. By definition of Galois extension, n = [K: F] and by theorem 6, n = [K: K^G]. By definition of F - automorphism, $F \subset K^G$. Examining degrees in the tower $F \subset K^G \subset K$, its clear that $[K^G: F] = 1$, hence that $F = K^G$.

RESULTS

Lemma 5: Let K/F be a Galois extension with Galois group G. (i) Let L be an intermediate field: $F \subset L \subset K$. Then K/L is a Galois extension and its Galois group is a subgroup of G. (ii) conversely, the fixed field of a subgroup H of G is an intermediate field: $F \subset K^H \subset K$.

Proof: (i) Being a Galois extension, K is the splitting field of some polynomial f(x) over F. So f splits in K[x] and that the roots of f generate K over F. Then it is obvious that K is also the splitting field of the same polynomial f over the larger field L. Therefore K/L is a Galois extension. By definition, its Galois group G (K/L) is the set of automorphisms of K which restrict to the identity of L. Any such automorphisms is also the identity on the smaller Field F and therefore is an element of G. So G(K/L) is a subgroup of G. (ii) Being in G, an element $\sigma \in H$ is the identity on F.
So $F \subset K^H$ and of course $K^H \subset K$.

The above generalizations are used in the next theorem referred to as Main Theorem of Galois Theory.

Theorem 8: Let K/F be a Galois extension, with Galois group G. The rules u: $H \rightarrow K^H$ and v : $L \rightarrow G(K/L)$ are inverse maps which define a bijective correspondence.
$H \subset G \qquad F \subset L \subset K$
{Subgroup} ↔ {intermediate fields}

Proof: From the assertion of Lemma 5, it shows that u, v, are maps with domains and ranges as indicated. We need to show that the composition of u and v in either order is the identity. Let H be a subgroup of G and let $L = K^H$. By theorem 6, K/L is a Galois extension and its Galois group is G (K/L) = H. This shows that vuH = H. Let L be an intermediate field and let H = G (K/L). By Theorem 7, $L = K^H$, therefore uvL = L.

DISCUSSION

A Galois extension is one such that IGI = [K:F]. With the Theorem we asserts that K/F is Galois extension if and only if K is a splitting field over F. The Galois group of a Galois extension K is the group of its F - automorphisms.

If G be a group of automorphisms over a field K. Then the fixed field K^G is by definition the set of elements $\alpha \in K$ which are fixed by all $\sigma \in G$, hence is a subfield of K.

CONCLUSION

We therefore conclude that G is embed as a subgroup of the symmetric group, hence the Galois correspondence is deduce using the Splitting theorem and Primitive Element.

ACKNOWLEDGEMENT

I want to acknowledge the effort of Prof. S. A. Ilori (UI. IBADAN), for his encouragement and readiness to give necessary advice when required.

REFERENCE

1. Thomas, W., Hungerford, Algebra, 1974. Graduate Text in Mathematics. 1st Edn., Holt, Rinehart and Winston, Algebra, pp: 502. ISBN: 0030860784.
2. Lloyd, R., Jaisingh and J.R. Frank Ayres, 2004. Theory and Problems of Abstract Algebra, Schaum's Outline Series. 2nd Edn., McGraw-Hill, pp: 384. ISBN: 0071431098.
3. Emil Artin, A.V., 1998. Galois Theory, Notre Dame. Dover Publications Inc., New York, pp: 86. ISBN: 978-0486623429.
4. Victor Shoup, 2002. A Computational Introduction to Number Theory and Algebra. 1st Edn., Springer-Verlag, Cambridge University Press, Cambridge, pp: 464-480.
5. Tignol, J.P., 1988. Galois Theory of Algebraic Equations, Longman. New York, pp: 22-24.
6. Andy Magid, R., 1994, Lectures on Differential Galois Theory. American Mathematical Society, Providence, RI., pp: 105. ISBN-10: 0821870041.
7. Dodson, B., 1984. The structure of galois groups of CM-fields. Trans. Am. Maths. Soc., 283: 1-32.