Fundamental Properties of the Galois Correspondence

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

Abstract: Problem Statement: Let K be the splitting field of a polynomial f(x) over a field F and \( \alpha_r \) be the roots of f in K. Let G be embedded as a subgroup of the symmetric group \( \varsigma \). 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 \( \varsigma \) operates on the polynomial ring F \([u_1, u_2, \ldots, u_n]\); Let its orbit under the action of \( \varsigma \) 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 \( f(y_1, y_2, \ldots, y_r) \) 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 \( f \).

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

Denote by \( \alpha \) the counterclockwise rotation of the square about 0 through 90°. Its effect is to have (12), (23), (34), (41), thus \( \omega = (1234) \). Now \( \omega^2 = \omega \omega = (13) \) (24) is a rotation about O of 180°. \( \omega^3 = (1432) \) is a rotation of 270° and \( \omega^4 = (1) \) is a rotation about O of 360° or 0°. The rotations through 180° about the bisectors AOB and COD give rise respectively to \( \sigma^2 = (12) \) and \( \tau^2 = (12) \) (34) while the rotations through 180° about the diagonals 103 and 204 give rise to \( e = (24) \) and \( b = (13) \).
By the operation of the roots, G embeds as a subgroup of the symmetric group $S_n = \zeta$, which contains 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 $a_i$ are distinct, $z$ can equally well be thought of as a permutation of the set $\{a_1, a_2, \ldots, a_n\}$
- $Z$ induces a permutation $Z$ of the set $\{p_1, p_2, \ldots, p_j\}$
- Provided that the $b_j$ are distinct, $Z$ can be used to permute $\{b_1, b_2, \ldots, b_r\}$

Therefore, clearly we can see that $Z$ sends $u_j \mapsto Zu_j$. Then $Z(p_1(u_1, u_2, \ldots, u_n)) = p(zu_1, zu_2, \ldots, zu_n)$, which is another one of the polynomials $\{P_1, P_2, \ldots, P_{j}\}$.

**Lemma 2:** Assume that the $b_j$ are distinct. Let $\sigma$ be an F-automorphism of K and let $Z$ be the permutation of the roots $\{a_1, a_2, \ldots, a_n\}$ it defines. Then the permutation $Z$ of $\{b_1, b_2, \ldots, b_r\}$ determine by $z$ is the one defined by $\sigma$ too.

**Proof:** $Z(b_j) = p(za_1, za_2, \ldots, za_n) = p(\sigma a_1, \sigma a_2, \ldots, \sigma a_n) = \sigma(p(a_1, a_2, \ldots, a_n)) = \sigma(b_j)$

Let $H_j$ be the stabilizer of the polynomial $b_j$ for the operation of G. Then if G is not the whole symmetric group $\zeta$, then there is no reason to suppose that the set $\{b_1, b_2, \ldots, b_r\}$ 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 $p_i$ form one orbit.

**Theorem 1:** With the notation above in lemma 1, suppose that $b_1, b_2, \ldots, b_r$ 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 $\sigma$ 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 $\sigma$ on $\{a_1, a_2, \ldots, a_n\}$ and let $Z$ be the permutation of $\{p_j\}$ induced by $z$. We apply the lemma, because $\beta_j$ are distinct, $\sigma$ fixes $\beta_j$ if and only if $Z$ fixes $u_j$ and this happens if and only if $z \in H_j$. Then $\beta_j \in F$ if and only if $\beta_j$ 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 $a_1, a_2, \ldots, a_n$ as above, that is $a_i \in F$, $p(a_1, a_2, \ldots, a_n) \in F$.

**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 $a_i \in F$, $p(a) = q(s_1(a), s_2(a), \ldots, s_n(a)) = q(a_1, a_2, \ldots, a_n)$ 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 $\{p_1, p_2, \ldots, p_j\}$, where $p = p_0$.

**Lemma 4:** Let $\{p_1, p_2, \ldots, p_j\}$ be the orbit of a polynomial $p_0(u_1, u_2, \ldots, u_n)$ 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 $h(p_1, p_2, \ldots, p_j)$ is a symmetric function in $u_1, u_2, \ldots, u_n$.

**Proof:** see J. P. Tignol[6]

**Lemma 5:** Let $\{p_1, p_2, \ldots, p_j\}$ be the orbit of a polynomial $p_0(u_1, u_2, \ldots, u_n)$. For $j = 1, 2, \ldots, r$ let $\beta_j = P_j(a_1, a_2, \ldots, a_n)$. The polynomial $h(x) = (x - \beta_1)(x - \beta_2)(x - \beta_r) = x^r - b_1x^{r-1} + b_2x^{r-2} - \ldots + b_r$ has coefficients in F.

**Proof:** We consider the polynomial $H(x) = (x - w_1)(x - w_2)\ldots(x - w_r) = x^r - B_1x^{r-1} + B_2x^{r-2} - \ldots + B_r$.

Its coefficients $B_i$ 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 $B_j \rightarrow b_j$ and it can be made in two steps $w_j \rightarrow p_j(u) \rightarrow p_j(a) = \beta_j$. Since the coefficients $B_j$ are symmetric polynomials in $w_1, w_2, \ldots, w_r$, 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 $\beta$ be a root of the irreducible polynomial $g(x)$ in the splitting field K. We write $\beta$ as a polynomial in $a_i$, say $\beta = p(a_1, a_2, \ldots, a_n)$, with $p(u_1, u_2, \ldots, u_n)$ in $F$.
F[u_1, u_2, ... , u_n]. Let \{p_1, p_2, ... , p_r\} be the orbit of p = p, and let \( \beta = p_1(\alpha_1, \alpha_2, ... , \alpha_n) \), so that \( \beta = \beta_1 \).

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

**Main theorem of Galois theory:**

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

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

**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:** (Primitive Element Theorem) Let K/F be a finite extension. An element \( \alpha \in K \) for which K = \( \mathbb{F}[\alpha] \) exists if and only if there exist only finitely many intermediate fields G: K \to 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 \( \mathbb{F}(\alpha + cf) \). Therefore there are \( c_1, c_2 \in \mathbb{F} \), \( c_1 \neq c_2 \) and such that \( \mathbb{F}(\alpha + c_1\beta) = \mathbb{F}(\alpha + c_2\beta) \).

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 \( \beta \) does so as well. Thus, \( \alpha \) also belongs to the same field and it follows that \( \mathbb{F}(\alpha, \beta) \) 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 \( K = \mathbb{F}[\alpha] \) for some \( \alpha \). Let \( m(x) \) be the minimal polynomial of \( \alpha \) over F. For any intermediate field G consider \( m_G(x) \), the minimal polynomial of \( \alpha \) 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 \( m_G \) is irreducible over \( G_0 \) and it is irreducible 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 \( K = \mathbb{F}(\alpha, \beta) \) where \( \alpha \), \( \beta \) are separable over F. Let \( \alpha_1 \), \( \alpha_2 \), \( \alpha_3 \) different embeddings of \( F \) into the normal closure of \( K \). (Using the condition that \( K \supseteq F \) is separable)

\[ \prod_{i \in I}(\sigma_i(\alpha) + x\sigma_i(\beta)) = \sigma_1(\alpha) = \cdots = \sigma_r(\alpha) = \sigma_r(\beta) \]

Clearly, \( P(x) \) is a nonzero polynomial and therefore there exist an element \( c \in F \) for which \( P(c) \neq 0 \). Then the elements \( \sigma_1(\alpha + cf) \) are all different and therefore \( F(\alpha + cf) \) has degree over F no less than \( n \). However \( n = [F(\alpha, \beta) : F] \) and therefore \( F(\alpha, \beta) = F(c) \).

**Theorem 4:** (i) Let K/F be a finite extension and let G be the group of F - automorphisms of K. Then \( \text{I}G \leq [K:F] \) if and only if K is a splitting field over F.

**Proof:** Let \( n = \text{I}G \) and \( N = [K:F] \). By the primitive Element Theorem, K = \( \mathbb{F}[\alpha] \) for some \( \alpha \). Let f(x) be the irreducible polynomial for \( \alpha \) over F. Then \( \deg f = \deg \alpha = N \). Let \( \alpha_1, \alpha_2, ... , \alpha_n \) 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 = \( \mathbb{F}[\alpha_i] \) for any i, because \([\mathbb{F}[\alpha_1]: F] = N \) 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 \( \alpha : K \to K \) sending \( \alpha_1 \to \alpha_i \). The elements of G are \( \{\sigma_1, \sigma_2, ... , \sigma_n\} \). This shows that \( r \leq N \). 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 \( \{\alpha_1, \alpha_2, ... , \alpha_r\} \), with \( \alpha_1 = \alpha \). Then (i) f(x) = \( (x - \alpha_1) (x - \alpha_2) ... (x - \alpha_r) \) is the irreducible polynomial for \( \alpha \) over F. (ii) \( \alpha \) is algebraic and of degree r over F, and \( r \leq |G| \).
Proof: Let \( g(x) \) be the irreducible polynomial for \( \alpha_i \) over \( F \). Then \( \alpha_i \) 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 \( \alpha_1, \alpha_2, \ldots, \alpha_n \). 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 \( \alpha \) over \( F \) is also \( r \).

Theorem 6: 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 \( n = |GI| \) and \( N = [K:F] \). Because the elements of \( G \) act as the identity on \( F \), they are \( F \)-automorphisms. So \( G \subseteq G(K/F) \). From theorem 4, it clears that \( n \leq N \). Let \( F' \) be an intermediate field, \( F \subseteq F' \subseteq K \), 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), \( F' = F[\gamma] \) for some \( \gamma \in K \). By theorem 5, the degree of \( \gamma \) 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 \( d_1 < d_2 < \ldots \). 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 \( n = |GI| \). By definition of Galois extension, \( n = [K:F] \) and by theorem 6, \( n = [K:K^G] \). By definition of \( F \)-automorphism, \( F \subseteq K^G \). Examining degrees in the tower \( F \subseteq K^G \subseteq K \), it’s 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: \( F \subseteq L \subseteq K \). 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: \( F \subseteq K^H \subseteq K \).

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 \( G \) is the set of automorphisms of \( K \) which restrict to the identity on \( L \). 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 \( F \subseteq K^H \) and of course \( K^H \subseteq K \).

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.

\[ H \subseteq G \quad F \subseteq L \subseteq K \]

{Subgroup} \leftrightarrow \{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 \( G \). 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 \( IG = [K:F] \). 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