American Journal of Science and Technology
2016; 3(1): 43-46
Published online March 1, 2016 (http://www.aascit.org/journal/ajst)
ISSN: 2375-3846

American Association for Science and Technology

Keywords
Basis,
Extension Fields,
Galois Group,
Irreducible Polynomials,
Minimal Polynomial,
Monic Polynomial,
Splitting Fields,
Transcendental

Received: December 26, 2015
Revised: January 19, 2016
Accepted: January 21, 2016

On Galois Groups

Faisal Hussain Nesayef

Department of Mathematics, Faculty of Science, University of Kirkuk, Kirkuk, Iraq

Email address
fnesayef@yahoo.com

Citation
Faisal Hussain Nesayef. On Galois Groups. *American Journal of Science and Technology*. Vol. 3, No. 1, 2016, pp. 43-46.

Abstract
Galois Theory is one of the interesting subjects in Mathematics. It constitutes a link between Polynomials, Fields and Groups. This paper considers manipulation of polynomials, studies and investigates some applications of groups and Fields and their extensions. Polynomials are regarded as an essential tools in the construction of rings and fields. Consequently the ring theory plays the basic role in the study of Galois groups, particular attention has been given to the algebraic polynomials, in terms of their reducible or irreducible properties. This has led to the study of Fields, Extension Fields and the Galois groups. The subject was extensively studied by the great mathematician Galois first. Subsequently many other mathematicians contributed in this field, appreciating Galois' great achievement in this area of mathematics.

1. Introduction

In this paper some properties have been studied in order to find out about the basic relationships between the fields, rings and polynomials. Some results have been stated and used from [1], [2], [3] and [4]. The main objective of this paper is to investigate the Automorphisms of the field extensions.

In section one, the basic principles and properties have been covered in order to make the consequent progress as smooth as possible.

Section two deals with the basic properties of the polynomial rings, the nature and the structure of the extension fields.

Section three tackles some important results discovered by many other researchers.

Section four deals with some applications of the Galois Groups, their nature, and their structural properties and characteristics.

The conclusion of this paper is to investigate the relationship between the roots of unity and the Galois Groups Gal ($\mathbb{Q}(n)/\mathbb{Q}$). Also to prove that for $n \in \mathbb{N}$ and $a \in \mathbb{Q}$, the Galois group will not be necessary abelian.

2. Basics

In this section we cover the basic terminologies required as a background knowledge in the latter sections. These are mainly given in other reference, such as [1], [2], etc.

Definition 1.1: Let F be a field. Then F[x] denotes the ring of polynomials with coefficients in F. i.e. $f(x) = a_n x^n + \cdots + a_1 x + a_0$ Where $a_0 \neq 0$, where $a_0, \dots, a_n \in F$.

Let f and g be polynomials in F[x], with $f \neq 0$. Then there exist polynomials $q \text{ and } r \in F[x]$ such that $g(x) = q(x)f(x) + r(x)$, where either r = 0 or $\deg(r) < \deg(f)$.

Definition 1.2: Let f, g, h be polynomials in F(x). Then g divides f, ie (g | f) if there exists $q \in F$ such that f = q g.

The polynomial f is reducible if it is non-constant and whenever we have factorization f = g h, either g or h is a unit. In this case

$$g.c.d\ (f,g) = \begin{cases} f & if\ f|g \\ 1\ other\ wise \end{cases}$$

Proposition 1.3: Suppose $\alpha = {}^{r}/_{s} \in Q$ where $r\ and\ s \in \mathbb{Z}$ are co-prime is a root of $f(x) = a_n x^n + \cdots + a_1 x + a_0\ a_0 \in \mathbb{Z}$. Then $r|a_0$ and $s|a_n$

$$\text{Proof} \quad \alpha = {}^{r}/_{s} \Rightarrow f(\alpha) = 0$$

$$0 = s^n f\left({}^{r}/_{s}\right) = a_n r^n + a_{n-1} r^{n-1}\, s + \cdots + a_1 r^{n-1} s + a_0 s^n$$

Since r divides each term in this expression, then $r|a_0 s^n$.

Also r and s are co-prime, therefore $r|a_0$. Also $s|a_n r^n$ and since r and s are co-primes, then s divides a_n.

Example 1: let $f(x) = 3x^2 - 3x - 1$

Then the only possible roots are $\pm 1, \pm {}^{1}/_{3}$

$$f(x) = -1, f(-1) = 5, f({}^{1}/_{3}) = {}^{-5}/_{3}\ and\ f({}^{-1}/_{3}) = {}^{1}/_{3}$$

Therefore f is irreducible.

Definition 1.3: A field is a set F with two binary operations "+" and "." such that

(a) $(F, +)$ is a commutative group

(b) $(F^X, .)$ is a commutative group, where $F^X = F \backslash \{0\}$

(c) The distribution law holds.

An example of a field is $Q[\sqrt{2}]$. The set of all numbers which can be written a+b√2 for a and b rational numbers.

Definition (Algebraic Number): f α is a real number with the property that $p(\alpha)$=0 for some polynomial $p(x)$, then we say that α is an *algebraic number.*

If α is an algebraic number then $Q[\alpha]$ is a field. $Q[\alpha]$ consists the set of elements of the form $a0+a1\alpha+\ldots+an-1\alpha n-1$ where each ai is a rational number and n is the smallest integer such that there is a polynomial $p(x)$ of degree n with $p(\alpha)$=0. $Q[\alpha]$ is the smallest field extension of Q containing α. Q[2√3]={a+b2√3+c2√3.2:a,b,c ∈ Q} is another example of a field. This idea can be extended to define, for α, β both algebraic, $Q[\alpha,\beta]$ to be the set of all expressions like $2\alpha\beta$, $\alpha+\alpha 2\beta$, and so on. [√2,√3]={a+b√2+c√3+d√6: a, b, c, d ∈Q} is an example of a Field.

The characteristic of a field

Definition 1.4: A field F is of finite characteristic p (Char (F) = p) if there is a least positive integer p such that (1+1+1+…+1) = 0 in F, (p-times). If there is no such integer, then F is said to have characteristic 0.

3. Extension Fields

Definition 2.1: Let F be a field. A field extension of F is a field E containing F. We write E/F as a field extension. E.g. C/R, Q/Q, Q$\sqrt{2}$ / Q

If E is a field containing F then, for all $e \in E\ and\ \lambda \in F$, then product λe is defined in E ; thus we have a scalar multiplication by F on E. Looking at the axioms for E to be a vector space over F, we see that they are all special cases of the axioms for E to be a field. Hence E is indeed a vector space over F and it has a basis and dimension over F.

Definition 2.2: Let E/F be a field extension. If E is finite dimensional as a vector space over F then we say that E/F is a finite extension, otherwise it is infinite. If it is finite then the degree of E/F is $[E: F] = dim_F(E)$.

For example, in the extensions above we have:

- $\mathbb{C}/\mathbb{R}$ is finite of degree $[\mathbb{C}: \mathbb{R}]$ = 2, because {1,i} is a basic for $\mathbb{C}$ as a $\mathbb{R}$-vector space.
- $\mathbb{C}/\mathbb{Q}$ is finite;
- $\mathbb{C}/\mathbb{Q}$ is finite of degree $[\mathbb{Q}: \mathbb{Q}]$=1, because { q } is a basis for any $q \in \mathbb{Q}^X$;
- $\mathbb{Q}(\sqrt{-2})/\mathbb{Q}$ is finite of degree 2, because B = $\{1, \sqrt{-2}\}$ is a basis. In this case it is clear that B spans $\mathbb{Q}(\sqrt{-2})$, since $\mathbb{Q}(\sqrt{-2}) = \{a + b\sqrt{-2}: a, b, \in \mathbb{Q}\}$. To see that B is linearly independent over $\mathbb{Q}$, suppose $a + b\sqrt{-2} = 0$, for some $a, b, \in \mathbb{Q}$.

If $b \neq 0$ then $\sqrt{2} = a/b \in \mathbb{Q}$ which is absurd. Hence b = 0 and so a = 0.

Algebraic extensions

Definition 2.3: Let E/F be a field extension and $\alpha\ \in E. \alpha$ is algebraic over F if there is a non-zero polynomial $f \in F[x]$ such that $(\alpha) = 0$; otherwise α is transcendental over F.

Splitting Fields

Definition 2.4: Let F be a field, let $f \in F[x]$ and let E/F be an extension.

(i) We say that f splits over E if it factorizes completely in E[x], i.e it can be expressed as a product of linear factors

$$f(x) = a_0(X - \alpha_1) \ldots (X - \alpha_n), with\ \alpha_1, \ldots, \alpha_n \in E, a_0 \in F^X$$

(ii) We say that E is a splitting field for f over F if f splits over E but not over any intermediate extension $L, E \supseteq L \supseteq F$.

Remark: If f splits over E as above, then we can describe a splitting filed for f over F quite easily. $F(\alpha_1)$ is the subfield of E of rational functions in α_1 with coefficients in F (equivalently, it is the smallest subfield of E containing F and α_1). Inductively we can define:

$F\ (\alpha_1, \ldots, \alpha_n) = F(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n)$, since E is a field extension of $F(\alpha_1, \ldots, \alpha_{n-1})$, then $F\ (\alpha_1, \ldots, \alpha_n)$ is the smallest field containing F and all the root $\alpha_1, \ldots, \alpha_n$ of f. So it is a splitting for f over F.

$$\begin{tikzcd}
F \arrow[r, "i"] \arrow[dr, "j"'] & E \arrow[d, "\varphi"] \\
 & E'
\end{tikzcd}$$

Figure (1). *Isomorphism of two splitting fields E and E' of the field F.*

Theorem 2.5: Let F be a field and $f \in F[x]$ a polynomial of degree n. Then there exists a splitting filed E for f over F, and $[E:F] \le n!$

Moreover if E' is another splitting filed for f over F then E is isomorphic to E' as extensions of F, i.e. there is an isomorphism $\varphi: E \xrightarrow{\sim} E'$ such that the following diagram commutes: That is, $\varphi(x) = x\ for\ all\ x\ \in F.$

Proof of existence. By the remark above. It is sufficient to find an extension of degree at most n!, in which f splits. We proceed by induction on n, noting that when n = 1 the polynomial f already factorizes over F and [F:F] = 1. So we turn to the inductive step and start by factorizing f over F,

$$f(x) = p_1(x) \dots p_r(x)\ in\ F[x]$$

where each p_i is irreducible in F[x] and deg $(p_1) \le (p_2) \le \cdots \le \deg(p_r)$

Put $F_1 = F[x]/(p_1(x))$, an extension of F of degree $\deg(p_1) \le$ n which contains a root α_1 of $p_1(x)$. Since α_1 is also a root of f, we can factorize

$$f(X) = (X - \alpha_1)f_1(X)\ in\ F_1[X]$$

Now $\deg(f_1) = n - 1$ so we can apply the inductive hypothesis to find an extension E of F_1 of degree at most (n-1)!, in which f_1 splits. Then f also splits in E and by the Tower Law

$[E:F] = [E:F_1][F_1:F] \le (n-1)!\,n = n!$, as required

To prove the uniqueness we consider the following example:

Example 2: Find the degree of the splitting field of $X^3 - 1\ over\ \mathbb{Q}$

Solution: we have to factorize the polynomial first. We have $X^3 - 1 = (X-1)(X^2 + X + 1)$ and the second factor is irreducible as the only possible roots are ± 1 but neither is a root.

Let $w = e^{2\pi i/3}$ be a root of $X^2 + X + 1$ in $\mathbb{C}$ then $\mathbb{Q}(w)$ is a splitting field, since $X^3 - 1 = (X-1)(X+w)(X+w^2)$ and $[\mathbb{Q}(w):\mathbb{Q}] = 2$, since w has minimal polynomial $X^2 + X + 1\ over\ \mathbb{Q}$ of degree 2.

Normality

Definition 2.6: finite extension E/F is normal if any irreducible polynomial $f \in F\,[X]$ which has a root in E splits completely over E.

Note that normality is a property of the extension not of the field. Also note that, to show that an extension E/F is not normal, we need only find an irreducible polynomial in F[X] which has a root in E but does not split over E. On the other hand, to prove that an extension is normal, we need the following proposition which is stated in [4].

Proposition 2.7 Finite extension E/F is normal if and only if it is the splitting field over F of some polynomial in F[X].

Example 3:

(i) $\mathbb{Q}(\sqrt[3]{2})$ is not a normal extension of $\mathbb{Q}$: the irreducible polynomial $f(x) = X^3 - 2$ has a root $\sqrt[3]{2}$ in $\mathbb{Q}(\sqrt[3]{2})$ but does not split in $\mathbb{Q}(\sqrt[3]{2})$, since the other roots of f in $\mathbb{C}$ are not real.

(ii) $\mathbb{Q}(\sqrt[3]{2}, \omega)$ is a normal extension of $\mathbb{Q}$; since we have seen that it is the splitting field over $\mathbb{Q}$ of $X^3 - 2$.

(iii) $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3})$ is a normal extension of $\mathbb{Q}$; since it is the splitting field over $\mathbb{Q}$ of $(X^3 - 2)(X^2 - 3)$.

4. Galois Theory

Automorphisms of field extensions

Definition 4.1 Let E/F be a field extension. An $F - automorphism\ of\ E$ is an isomorphism $\sigma: E \to E$ such that $\sigma(x) = x\ for\ all\ x \in F$. We write Aut (E/F) for the set of $F - automorphism$ of E.

Note that Aut (E/F) is actually a group, with composition:

- If $\sigma, \tau\ \in$ Aut (E/F) then so is $\sigma\tau = \sigma\ o\ \tau$. It is certainly an isomorphism from E to itself, where $\sigma\tau(x) = \sigma(\tau(x)) = x\!: for\ x \in F$.
- The map $i: E \to E$, given by $i(e) = e$ for all $e \in E$, is the identity element of Aut(E/F).
- If $\sigma \in$ Aut $\left(\frac{E}{F}\right)$ then $\sigma^{-1} \in$ Aut $\left(\frac{E}{F}\right)$ as $\sigma^{-1}(\sigma(x)) = i(x) = x$, for $x \in F$.

Example 4 Let $p(x) = x^2 - 2$ be a polynomial, then:

(a) The splitting field of p(x) is Q[√2].(b) The automorphisms of p(x), which are the symmetries of the roots, are given by: f (a + b√2) = a–b√2 and g (x) = x.

Lemma 4.2 Let (E/F) be a field extension. Let α ∈ E be algebraic over F, and let σ ∈ Aut (E/F). Then σ(α) ∈ E is a root of the minimal polynomial of α over F.

Proof: Let $\mathrm{f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in F[X]}$ *be the minimal polynomial over F of* α. *Then*

$$\begin{aligned} f(\sigma(\alpha)) &= (\sigma(\alpha))^n + a_{n-1}(\sigma(\alpha))^{n-1} + \\ &= \sigma(\alpha)^n + \sigma(a_{n-1})\sigma(\alpha^{n-1}) \\ &\quad + \cdots \sigma(a_1)\sigma(\alpha) + \sigma(a_0) \\ &= \sigma(\alpha^n + a_{n-1}\alpha^{n-1} + \cdots a_1\alpha \\ &\quad + a_0) = \sigma(f(\alpha)) = \sigma(0) = 0 \end{aligned}$$

Let $E = F(\alpha_1, \dots, \alpha_n)$ is finite extensionof F. Then

- Any $\sigma\ \in$ Aut (E/F) must map each α_i to a root of its minimal polynomial over F_i.
- $\sigma \in$ Aut $\left(\frac{E}{F}\right)$ is uniquely determined by specifying $\sigma(\alpha_1), \dots \sigma(\alpha_n)$, since any element of E can be written in terms of $\alpha_1, \dots \alpha_n$ and elements of F, while σ is a homomorphism.

Example 5:

(i) Aut $(\mathbb{Q}(\sqrt{2}/\mathbb{Q})$ has at most two elements, since $\sqrt{-2}$ must be mapped to either $\pm\sqrt{-2}$ (as these are the roots of $X^2 + 2$ the minimal polynomial of $\sqrt{-2}$ over $\mathbb{Q}$), and specifying which one of these occurs determines the automorphism. Indeed, there are two: the identity map i, and the map σ given by: $\sigma\left(a + b\sqrt{-2}\right) = a - b\sqrt{-2}$

(ii) Aut $(\mathbb{Q}(\sqrt[3]{2}/\mathbb{Q})$ has only the identity map, as $\sqrt[3]{-2}$ has minimal polynomial $X^3 + 2$ over $\mathbb{Q}$, whose only root in $\mathbb{Q}(\sqrt[3]{2})$ is $\sqrt[3]{2}$ and hence $\sqrt[3]{2}$ can only be mapped to itself.

Example 6 For each of the following polynomial $in\ \mathbb{Z}[X]$, we find a splitting field E over $\mathbb{Q}$, the Galois group of f over $\mathbb{Q}$, and all intermediate fields: $\mathbb{Q}\ \subseteq L \subseteq E$. We also, identify those subfields for which $L/\mathbb{Q}$ is Galois and in that case, find Gal(L/$\mathbb{Q}$).

$$f(x) = x^4 - 2$$

The splitting field is E = $\mathbb{Q}(\xi, i)$, where $\xi = \sqrt[4]{2}$, since the roots of $X^4 - 2$ are $\pm\xi, \pm i\xi$. This has degree 8 over $\mathbb{Q}$, so writing G = Gal (E / $\mathbb{Q}$). We have $|G| = 8$.

Any automorphism is uniquely determind by its action on ξ and i. It it must map I to $\pm\, i$ and ξ to one of the roots of $x^4 - 2$. Hence there are 8 possible automorphims. Hence there are automorphisms $\sigma, \tau \in G$ such that: $\sigma \;\; (i) = i$, $\sigma(\xi) = i\xi$; $\tau(i) = -i$, $\tau(\xi) = \xi$. Then we can easily check that $G = \{ 1, \sigma, \sigma^2, \sigma^3, \tau, \tau\sigma^2, \tau\sigma^3\} = \{ \sigma, \tau \colon \sigma^4 = 1, \tau^2 = 1, \tau\sigma = \sigma^3\tau \} \simeq D_8$.

This is a dihedral group with 8 elements,

Remark Since G is a subgroup of S_4, we could ask to identify it as such. Numbering the roots $\xi, i\xi, -\xi, -\xi$ as 1,2,3,4 respectively, we see that $\sigma = (1\;2\;3\;4)$ $\tau = (24)$ and G ={1, (1234), (13)(24), (1432), (24), (14)(23), (13), (12)(34)}.

Example 7. Let $p\,(x) = x^2 - 2$ be a polynomial, then $G = Gal\,(p) = \{f, g\}$, where,

$$f\left(a + b\sqrt{2}\right) = a - b\sqrt{2} \; and \; g(x) = x.$$

g is the identity element of the group and $f.f = g$, as $(f.f)\left(a + b\sqrt{2}\right) = f\left(f\left(a + b\sqrt{2}\right)\right) = f\left(a - b\sqrt{2}\right) = g\left(a + b\sqrt{2}\right)$ This group is cyclic of order 2 isomorphic to C_2.

5. Applications

We are now going to introduce some results about application of Galois Group.

Proposition 5.1 Let F be a field with char $(F) \neq 2$. Suppose P is an odd prime. There exists a field (up to homomorphism) with p^2 elements.

Proof Take a field of characteristic p. K contains $\mathbb{F}$. So consider the quadratic extension F_p. Define a homomorphism $\emptyset \colon \mathbb{F}_p^X \rightarrow \mathbb{F}_p^X$ by $\emptyset(a) = a^2$. Then ker $(\emptyset) = \{1, -1\}$.

Therefore $\emptyset$ $(\mathbb{F}_p^X)$ has index two in $\mathbb{F}_p^X$ so $\mathbb{F}_p^X$ is the only possible field which can be $E = \mathbb{F}[x]/(X^2 - a)$.

Proposition 5.2 Let G be the Galois group of the polynomial $X^2 - 2$ over Q, show that $|G| = 20$

Proof: The splitting field Q[η, α], where $\eta^s = 1$ and $\alpha^s = 2$. This is generated by $a = (1\;2\;3\;4\;5) \; and \; \tau = (2\;3\;5\;4)$ where $\sigma\alpha = \eta\alpha$ and $\tau\eta = \eta^2$. So the group has order 20.

Proposition 5.3 Every field homomorphism $\emptyset \colon \mathbb{F} \rightarrow \mathbb{F}$ must be one – to –one and onto.

Proof: $\emptyset$ acts as the identity map on $\mathbb{Z}$ and $\mathbb{Q}$. $\emptyset(R^+) = R^+$. Therefore $\emptyset$ preserver the order Therefore if $a \in \mathbb{R}$ we have $\{ r \in \mathbb{Q} \colon a < r\} = \{r \in \mathbb{Q} | \emptyset\,(a) < r\}$ resulting in $\emptyset\,(a) = a$.

Theorem 5.4 If $\eta = e^{2\pi i/n}$ a primitive n^{th} root of unity is $\mathbb{C}$, with $n \geq 0$, then Gal($\mathbb{Q}(n)/\mathbb{Q}$) is abelian of deg. at most n - 1.

Proof: Since η is a root of $X^n - 1 = (X - 1)(X^{n-1} + \cdots + X + 1)$ and $\eta \neq 1$ the minimal polynomial of η and $\mathbb{Q}$ has degree at most n - 1.

Also the roots of $X^n - 1$ are $1, \eta, \eta^2 + \cdots + \eta^{n-1}$ which are all in $\mathbb{Q}(\eta)$.

So this is the splitting field of $X^n - 1$ and so it is a Galois extension.

Let $\pi \in G = Gal\;(\mathbb{Q}(\eta) \,/\, \mathbb{Q})$ is gives by $\pi(\eta) = \eta^{i(\pi)}$ for some $i(\pi) \in \mathbb{Z}/n\,\mathbb{Z}$.

Since $\pi(\eta)$is a root of $X^n - 1$,

Therefore $\tau\pi(\eta) = \tau\left(\eta^{i(\pi)}\right) = \tau(\eta)^{i(\pi)} = \eta^{i(\tau)i(\pi)} = \eta^{i(\pi)i(\tau)} = \pi\tau(\eta)$. Therefore $\tau\pi = \pi\tau$.

Theorem 5.5 Let $n \in \mathbb{N}$ and $a \in \mathbb{Q}$. Then the Galois group of Q is not necessarily abelian.

Proof: Let $f(X) = X - a \; and \; E$ the splitting field of $f(X)$ over $\mathbb{Q}$

If $\omega = \sqrt[n]{a}$ and $\eta = e^{\tau\pi i/n}$ then the root of $f(x)$ in C are: $\omega, \omega\eta\,, \omega\eta^2, \ldots, \omega\eta^{n-1}$ .Take $E = \mathbb{Q}(\omega, \eta)$. Put $K = \mathbb{Q}(\eta)$ the splitting field over $\mathbb{Q}$ of $X^n - 1$, then we have $\mathbb{Q} \subset K \subset E$.

Let $G = Gal(E/Q)$ and $N = Gal(E/K)$. The subgroup of G with respect to the intermediate field K.

Since K/Q is normal, then N is a normal subgroup of G and $N \simeq Gal(K/\mathbb{Q})$.

Also $Gal(K/\mathbb{Q})$ is abelian by theorem 5.4.

References

[1] Artin, M.; Algebra, Prentice Hall, 1991.

[2] Gaal. L.; Classical Galois Theory with Examples, Chelsea Publishing company, New York, N.Y, 1979.

[3] Rottman, Galois Theory, 2nd Edition, Springer Verlag, 1998.

[4] Stewart, I.; Galois Theory, 4th Edition, Chapman and Hall CRC Mathematics, 2004.

[5] Escofier, J. P. and Schueps, L. S.; Galois Theory, Good Text in Mathematics, Springer Verlag, 2000.

[6] Beworsdoff, J.; Galois Theory for beginners, A historical Perspective, (Student Mathematical Library), AMS, 2006.

[7] Stillwell, J.; Galois Theory for beginners, American Mathematical Monthly, V 101, No. 1, 1994.

[8] Tignal, J-P.; Galois Theory of Algebraic Equations, World Scientific, 2011.

[9] Weintraub, S. H.; Galois Theory, Universititext, 2nd Edition, 2009.