Pure and Applied Mathematics Journal
2012; 1(1) : 10-16
Published online December 30, 2012 (http://www.sciencepublishinggroup.com/j/pamj)
doi: 10.11648/j.pamj.20120101.12

Galois groups of polynomials and the construction of finite fields

S. M. Tudunkaya[1], A. I. Kiri[2]

[1]Department of Mathematics, Kano University of Science and Technology, Wudil, Nigeria
[2]Department of Mathematical Sciences, Bayero University, Kano, Nigeria

Email address:
tudunkayaunique@yahoo.com (S. M. Tudunkaya)

To cite this article:
S. M. Tudunkaya, A. I. Kiri. Galois Groups of Polynomials and the Construction of Finite Fields, *Pure and Applied Mathematics Journal.* Vol. 1, No. 1, 2012, pp. 10-16. doi: 10.11648/j.pamj.20120101.12

Abstract: In this note an attempt was made in constructing finite fields with the aid of Galois groups of polynomials of small degree. The properties of these polynomials, their base fields and their splitting fields werediscussed. From these properties corollaries were developed upon which the constructions were done. The aim was to provide concrete and physical explanations on some aspects of finite fields and Galois theory.

Keywords: Group, Galois Group, Galois Extension, Field, Finite Field, Field Extension, Isomorphism

1. Introduction

The nature of polynomials of small degree was explored in [1], their general solutions were found which allow for the application of Galois ideas to analyse their splitting fields. The Galois groups of these polynomials (of degree less than or equal to four) were found up to isomorphism. In this note, these results were followed step by step and upon them, corollaries were developed which were used to construct finite fields with the aid of ideas and methods presented in [2, 3-5, 6].

Reference [7], defined a monoid as a set G with a law of composition

$$(for\ all\ x, y \in G, then\ xy \in G)$$

which is associative

$$(for\ all\ x, y, z \in G\ then\ (xy)z = x(yz) \in G)$$

and having a unit element

$$(there\ exists\ e \in G\ such\ ex = x = xe\ for\ all\ x \in G)\ .$$

The set G is called a group if for every element $x \in G$ there is a unique element $y \in G$ such that

$$xy = yx = e.$$

Also, by [8] G is called a commutative group if for all

$$x, y \in G\ \ xy = yx \in G.$$

A commutative additive group G, where multiplication is associative and having a unit element such that for all

$$x, y, z \in G, (x + y)z = xz + yz$$

and

$$z(x + y) = zx + zy$$

is called a ring as given in [7].

In [9], a field was defined as a set F with two composition laws + and • such that:

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

b) $(F^*, \bullet)$, where $F^* = F/\{0\}$ is a commutative group and

c) the distributive law holds.

in [7], ring homomorphism from the ring R to the ring H, was defined as a mapping

$$f : R \to H$$

such that

$$f(x + y) = f(x) + f(y),\ f(xy) = f(x)f(y), f(1) = 1,\ f(0) = 0.$$

According to [11], a ring homomorphism is a field homomorphism, if it is one to one it is called a monomorphism, when it is onto it is called an endomorphism. A homomorphism that is both a monomorphism and an endomorphism is called a isomorphism and if

$$R = H$$

then it is called an automorphism. The set γ of all automorphisms of a field forms a group under composition and distinct isomorphisms $\gamma_1, \gamma_2, \ldots, \gamma_k$ of R onto H are linearly independent over H such that if

$$\gamma(a_i) = b_i \in H$$

Then

$$a_1 b_1 + a_2 b_2 + \cdots + a_k b_k = 0$$

only if all

$$a_{i\prime s} = 0.$$

The following results and definitions are as given in [1, 3-6, 10]. K is said to be a field extension of F, if $F \subseteq K$, where K and F are both fields. This is often denoted as K/F. Galois extension was defined as a finite extension K of a field F, if F is the fixed field of the group of F-automorphims of K (i.e. the automorphism, which leaves the elements of F fixed), this group is then called the Galois group of K over F and it is denoted Gal (K/F).

A polynomial $f \in F[x]$ is irreducible in F if it can not be expressed as a product of two non scalar polynomials in F. $F[x]$ is the set of all polynomials defined over the ring F.

The smallest field in which the polynomial f is reducible, is called the splitting field of f.

The following results are stated for their relevance and importance.

1.1. Theorem

If f is irreducible in $F[x]$ its splitting over F exist and are isomorphic.

1.2. Theorem

The degree of the polynomial f in $F[x]$ is the same as the degree of its splitting field over F.

The formal derivative of a polynomial

$$f(x) = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0$$

where

$$a_i \in F$$

Is

$$f'(x) = m a_m x^{m-1} + (m-1) a_{m-1} x^{m-2} + \cdots + a_1$$

of degree $m-1$, which can be zero even if f is not a constant polynomial. If f and g are polynomials in F such that $deg\, f > deg\, g$, then by the Euclidean algorithm, there exists two polynomials q and r such that $f = qg + r$, where r may be zero and $deg\, r < deg\, g$ and the greatest common divisor (gcd) of f and g denoted by

$$(f,g) = af + bg$$

for some

$$a, b \in F[x].$$

1.3. Theorem

If f and g are in F and F^* an extension of F, then
(a) $(f,g) = d$ in $F[x]$ iff $(f,g) = d$ in $F^*[x]$
(b) f/g in $F[x]$ iff f/g in $F^*[x]$
(c) f has multiple zero iff $(f,g) \neq 1$

1.4. Theorem

Every $f \in F[x]$ of degree m has at most m zeros in F^*.

1.5. Theorem

The characteristic of F_p is p.

1.6. Theorem

F^* is a vector space over F.

1.7. Theorem

For any prime p and a monic irreducible f in $F_p[x]$ of degree n, the ring $F_p[x]/f$ is a field of order p^n.

1.8. Theorem

$|F_{p^n}| = p^n$ where n is any positive integer.

1.9. Theorem

F_{p^n} is the splitting field for $ax^{p^n} - ax$.

1.10. Corollary

For any prime p and any positive integer n, F_{p^n} exists.

1.11. Theorem

Any finite field has a prime power order.

1.12. Theorem

Any two finite fields of the same order are isomorphic.

1.13. Theorem

$(F_{p^n}, \bullet)$ is cyclic.

Recall that an element that generates a cyclic group is called a primitive element.

1.14. Theorem

Over any field F_p, $(ax^m - a) / (ax^k - a)$ iff m/k.

1.15. Corollary

For any prime integer p, $(ax^{p^m} - a) / (ax^{p^k} - a)$ iff m/k.

1.16. Theorem

F_{p^m} is a subfield of F_{p^n} iff m/n.

1.17. Corollary

For any prime integer p and positive integer n, there is a monic irreducible of degree n in $F_p[x]$

1.18. Theorem

Let

$$f(x)=x^2-bx+c\in Q(x)$$

be a quadratic polynomial then the Galois group G of $f(x)$ is one of the following:

i) If $f(x)$ splits in $Q(x)$ and

$$D=\sqrt{b^2-4ac}\in Q$$

then G=<e> i.e. G is generated by the identity element.

ii) If $f(x)$ does not split in $Q(x)$ then $f(x)$ is irreducible, then $D\notin Q$ and

$$G\cong S_2\cong Z_2$$

1.19. Theorem

Let

$$f(x)\in Q$$

be a cubic polynomial with Galois group G and let

$$g(x)=x^3+px+q$$

be its reduced form, then exactly one of the following cases holds:

i) $f(x)$ is reducible and

$$f(x)=(x-x_1)\,h(x)$$

where $x_1\in Q$ then G is the Galois group of $h(x)$.

ii) $f(x)$ is irreducible and

$$D^2=-27q-4p^3<0,$$

then f has exactly one real root and $G\cong S_3$.

iii) $f(x)$ is irreducible and $D^2>0$. Therefore, $f(x)$ has three real roots and if $D\in Q$, we have

$$G\cong S_3\cong D_3,$$

otherwise G is isomorphic to S_3.

1.20. Theorem

Let $f(x)\in Q$ be a reducible quartic polynomial with Galois group G, then there are two cases;

i) $f(x)$ contains a rational root u and it factors into

$$f(x)=(x-u)\,h(x)$$

where $h(x)$ is a cubic polynomial. Then G is just the Galois group of $h(x)$.

(ii) $f(x)$ does not have a rational root but factors into

$$f(x)=g(x)\,h(x)$$

where $g(x)$ and $h(x)$ are two irreducible quadratic polynomials. Then G is isomorphic to Z_2 or to $Z_2\times Z_2$.

b) Let

$$f(x)\in Q$$

be an arbitrary, irreducible, quartic polynomial with Galois group G and E the splitting field of it's reduced cubic $g(x)$. Let n be the order of Gal (E/Q).

If $g(x)$ has no zero roots there are four possibilities for n and exactly one of the following cases holds:

i. If $n=1$, then $G\cong H$, with H as defined above

ii. If $n=2$, $g(x)$ has a rational root P_1^2 and two irrational roots P_2^2 and P_3^2. If $P_1\in E$ but $P_1\notin Q$, then $G\cong Z_4$; otherwise, G is isomorphic to the dihedral group D_4.

2. Results

Upon the above properties, the following corollaries are developed and discussed in this work:

2.1. Corollary

Let

$$f(x)=x^2-bx+c\in Q(x)$$

be a quadratic polynomial, if $f(x)$ does not split in $Q(x)$ then $D\notin Q$ and $G\cong S_2\cong Z_2$ hence there is a finite field of order 2^2.

Discussion

Since

$$G\cong S_2\cong Z_2$$

and $Z_2=\{\bar{0},\bar{1}\}$ is a field, also the operations of addition and multiplication are done modulo 2, Z_2 is a prime filed. The entire monic irreducible quadratic polynomials with

coefficients in the field are:

$$x^2$$

$$x^2 + 1$$

$$x^2 + x$$

$$x^2 + x + 1$$

To find the irreducible ones, we can see clearly that, those without a constant term are reducible. Now to find the irreducible ones among the rest, we take each in turn and substitute all the elements of the field for x, if none of the substitutions evaluates to zero then the polynomial is irreducible (remember that even integers are isomorphic to 0 and odd integers are isomorphic to 1 in this field) for this reasons, the only irreducible polynomial here is

$$x^2 + x + 1.$$

Now, to make the most useful representation of the field making μ to be the zero of

$$x^2 + x + 1$$

and for the fact that the multiplication group of this field is cyclic, μ must be a primitive element (i.e. generator of a cyclic group) therefore:

$$\mu^2+\mu+1 =0$$

means

$$\mu^2 = \mu + 1$$

so that

$$\mu^1 = \mu$$

$$\mu^2=\mu+1$$

$$\mu^3 = \mu\ (\mu+1)= \mu^2+\mu=1$$

We can now see that the field elements are represented as 3 powers of μ together with 0.

2.2. Corollary

Let

$$f(x) \in Q$$

be a cubic polynomial with Galois group G and let

$$g(x) = x^3 + px + q$$

be its reduced form, $f(x)$ is irreducible and $D^2 > 0$, $f(x)$ has three real roots and if $D \in Q$, we have

$$G \cong S_3 \cong D_3$$

then there exists a finite field of order 3^3.

Discussion

$$Z_3 = \{\bar{0}, \bar{1}, \bar{2}\}$$

is a field, it is simple and therefore a prime subfield of itself, where addition and multiplication are done modulo 3.

The entire monic cubic polynomials with coefficients in this field can be listed as follows:

$$x^3$$

$$x^3 + 1$$

$$x^3 + 2$$

$$x^3 + x$$

$$x^3 + x + 1$$

$$x^3 + x + 2$$

$$x^3 + x^2 + x + 1$$

$$x^3 + x^2 + x + 2$$

$$x^3 + 2x$$

$$x^3 + 2x + 1$$

$$x^3 + 2x + 2$$

$$x^3 + 2x^2 + 1$$

$$x^3 + 2x^2 + 2$$

$$x^3 + x^2 + 2x + 1$$

$$x^3 + x^2 + 2x + 2$$

$$x^3 + 2x^2 + x + 1$$

$$x^3 + 2x^2 + x + 2$$

$$x^3 + x^2 + 1$$

$$x^3 + x^2 + 2$$

$$x^3 + x^2$$

$$x^3 + 2x^2$$

$$x^3 + x^2 + x$$

$$x^3 + x^2 + 2x$$

$$x^3 + 2x^2 + x$$

$$x^3 + 2x^2 + 2x$$

$$x^3 + 2x^2 + 2x + 1$$

$$x^3 + 2x^2 + 2x + 2$$

To find the irreducible cubic polynomials, we simply cross out the ones without a constant term. Also, taking each of the elements of the prime filed and substituting it for x as in the quadratic case above, we see that the irreducible polynomials are:

$$x^3 + x^2 + x + 2$$

$$x^3 + 2x + 1$$

$$x^3 + 2x + 2$$

$$x^3 + 2x^2 + 1$$

$$x^3 + x^2 + 2x + 1$$

$$x^3 + 2x^2 + x + 1$$

$$x^3 + x^2 + 2$$

Now, since the multiplicative group of the field is cyclic, we can search for a primitive element among the roots of these polynomials. We should note that it is not all the roots that are primitive for instance, letting β to be the root of

$$x^3 + x^2 + x + 2$$

which means

$$\beta^3=2\beta^2+2\beta+1$$

i.e.

$$\beta^3+ \beta^2+ \beta+2=0$$

$$\beta^1 = \beta$$

$$\beta^2 = \beta^2$$

$$\beta^3 = 2\beta^2 + 2\beta^2 + 1$$

$$\beta^4 = \beta(2\beta^2 + 2\beta + 1) = 2\beta^3 + 2\beta^2 + \beta = 2(2\beta^2 + \beta + 1) + 2\beta^2 + \beta = \beta^2 + \beta + 2 + 2\beta^2 + \beta = 2\beta + 2$$

$$\beta^5 = \beta(2\beta^2 + 2) = 2\beta^3 + 2 + \beta$$

$$\beta^6 = \beta(2\beta^2 + 2\beta) = 2\beta^3 + 2\beta^2 + \beta$$

$$= 2(2\beta^2 + 2\beta + 1) + 2\beta^2 = \beta + 2$$

$$\beta^7 = \beta(\beta + 2) = \beta^3 + 2\beta$$

$$\beta^8 = \beta(\beta^2 + 2\beta) = \beta^3 + 2\beta^2 = 2\beta^2 + 2\beta + 1) + 2\beta^2 = \beta^2 + 2\beta + 1$$

$$\beta^9 = \beta(\beta^2 + 2\beta+1) = \beta^3 + 2\beta^2 + \beta$$

$$= 2\beta^2 + 2\beta + 1 + 2\beta^2 + \beta = \beta^2 + 1$$

$$\beta^{10} = \beta(\beta^2 +1) = \beta^3 + \beta = 2\beta^2 + 2\beta + 1 + \beta = 2\beta^2 + 1$$

$$\beta^{11} = \beta(2\beta^2 +1) = 2\beta^3 + 2\beta^2 + \beta$$

$$= 2\,(2\beta^2 + 2\beta +1) = \beta^2 + 2\beta + 2$$

$$\beta^{12} = \beta(\beta^2 + 2\beta+2) = \beta^3 + 2\beta^2+2\beta$$

$$=2\beta^2+2\beta+1+ 2\beta^2 + 2\beta = \beta^2 + \beta + 1$$

$$\beta^{13} = \beta(\beta^2 + \beta+1) = \beta^3 + \beta^2 + \beta = 2\beta^2 + 2\beta + 1 + \beta^2 + \beta = 1$$

Therefore, β here has order 13, but we are looking for a cyclic group of order 26, hence, β does not generate the cyclic group we are looking for because it is not a primitive element. Now, supposing π is the root of the cubic irreducible polynomial

$$x^3+x^2+2x+1 \text{ i.e. } \pi^3 + \pi^2 + 2\pi + 1 = 0$$

Meaning

$$\pi^3 = 2\pi^2 + \pi + 2$$

so that

$$\pi^1 = \pi$$

$$\pi^2 = \pi^2$$

$$\pi^3 = 2\pi^2 + \pi + 2$$

$$\pi^4 = \pi(2\pi^2 + \pi + 2) = 2\pi^3 + \pi^2 + 2\pi$$

$$= 2(2\pi^2 + \pi + 2) + \pi^2 + 2\pi = 2\pi^2 + \pi + 1$$

$$\pi^5 = \pi(2\pi^2 + \pi + 1) = 2\pi^3 + \pi^2 + 2\pi$$

$$= 2(2\pi^2 + \pi + 2) + \pi^2 + \pi = 2\pi^2 + 1$$

$$\pi^6 = \pi(2\pi^2 + 1) = 2\pi^3 + \pi = 2(2\pi^2 + \pi + 2) + \pi = \pi^2 + 1$$

$$\pi^7 = \pi(\pi^2 + 1) = \pi^3 + \pi = 2\pi^2 + \pi + 2 + \pi = 2\pi^2 + 2\pi + 2$$

$$\pi^8 = \pi(2\pi^2 + 2\pi + 2) = 2\pi^3 + 2\pi^2 + 2\pi$$

$$= 2(2\pi^2 + \pi + 2) + 2\pi^2 + 2\pi = \pi + 1$$

$$\pi^9 = \pi(\pi + 1) = \pi^2 + \pi$$

$$\pi^{10} = \pi(\pi^2 + \pi) = \pi^3 + \pi^2 = 2\pi^2 + \pi + 2 + \pi^2$$

$$= \pi + 2$$

$$\pi^{11} = \pi(\pi + 2) = \pi^2 + 2\pi$$

$$\pi^{12} = \pi(\pi^2 + 2\pi) = \pi^3 + 2\pi^2$$

$$= 2\pi^2 + \pi + 2 + 2\pi^2 = \pi^2 + \pi + 2$$

$$\pi^{13} = \pi(\pi^2 + \pi + 2) = \pi^3 + \pi^2 + 2\pi$$

$$= 2\pi^2 + \pi + 2 + \pi^2 + 2\pi = 2$$

$$\pi^{14} = 2\pi$$

$$\pi^{15} = \pi(2\pi) = 2\pi^2$$

$$\pi^{16} = \pi(2\pi^2) = 2\pi^3 = 2(2\pi^2 + \pi + 2) = \pi^2 + 2\pi + 1$$

$$\pi^{17} = \pi(\pi^2 + 2\pi + 1) = \pi^3 + 2\pi^2 + \pi$$

$$= 2\pi^2 + \pi + 2 + 2\pi^2 + \pi = \pi^2 + 2\pi + 2$$

$$\pi^{18} = \pi(\pi^2 + 2\pi + 2) = \pi^3 + 2\pi^2 + 2\pi$$

$$= 2\pi^2 + \pi + 2 + 2\pi^2 + 2\pi = \pi^2 + 2$$

$$\pi^{19} = \pi(\pi^2 + 2) = \pi^3 + 2\pi = 2\pi^2 + \pi + 2 + 2\pi = 2\pi^2 + 2$$

$$\pi^{20} = \pi(2\pi^2 + 2) = 2\pi^3 + 2\pi$$

$$= 2(2\pi^2 + \pi + 2) + 2\pi = \pi^2 + \pi + 1$$

$$\pi^{21} = \pi(\pi^2 + \pi + 1) = \pi^3 + \pi^2 + \pi$$

$$= 2\pi^2 + \pi + 2 + \pi^2 + \pi = 2\pi + 2$$

$$\pi^{22} = \pi(2\pi + 2) = 2\pi^2 + 2\pi$$

$$\pi^{23} = \pi(2\pi^2 + 2\pi) = 2\pi^3 + 2\pi^2$$

$$= 2(2\pi^2 + \pi + 2) + 2\pi^2 = 2\pi + 1$$

$$\pi^{24} = \pi(2\pi + 1) = 2\pi^2 + \pi$$

$$\pi^{25} = \pi(2\pi^2 + \pi) = 2\pi^3 + \pi^2 =$$

$$2(2\pi^2 + \pi + 2) + \pi^2 = 2\pi^2 + 2\pi + 1$$

$$\pi^{26} = \pi(2\pi^2 + 2\pi + 1) = 2\pi^3 + 2\pi^2 + \pi$$

$$= 2(2\pi^2 + \pi + 2) + 2\pi^2 + \pi = 1$$

We can see that π is a primitive element since it has generated the cyclic group we are looking for. Furthermore, the above is a representation of the 26 powers of π, this together with 0, gave the entire elements of the field.

2.3. Corollary

Let $f(x) \in Q$ be an arbitrary, irreducible, quartic polynomial with Galois group G and E the splitting field of its reduced cubic $g(x)$. Let n be the order of Gal (E/Q).

If $g(x)$ has no zero roots If $n = 2$, $g(x)$ has a rational root P_1^2 and two irrational roots P_2^2 and P_3^2. If $P_1 \in E$ but $P_1 \notin Q$, then $G \cong Z_4$ also since Z_2 is the prime subfield then there is a finite field of order 2^4.

Discussion

$G \cong Z_4$, we will have the prime field to be $Z_2 = \{\bar{0}, \bar{1}\}$. Now, the entire monic quartic polynomials with coefficients in this field are as follows

$$x^4$$

$$x^4 + x$$

$$x^4 + x^2$$

$$x^4 + x^3$$

$$x^4 + 1$$

$$x^4 + x + 1$$

$$x^4 + x^2 + 1$$

$$x^4 + x^3 + 1$$

$$x^4 + x^3 + x$$

$$x^4 + x^3 + x^2$$

$$x^4 + x^3 + x + 1$$

$$x^4 + x^3 + x^2 + 1$$

$$x^4 + x^3 + x^2 + x$$

$$x^4 + x^3 + x^2 + x + 1$$

$$x^4 + x^2 + x$$

$$x^4 + x^2 + x + 1$$

Supposing β is the root of

$$x^4 + x^3 + 1 \text{ i.e. } \beta^4 + \beta^3 + 1 = 0$$

meaning

$$\beta^4 = \beta^3 + 1$$

then

$$\beta^1 = \beta$$

$$\beta^2 = \beta^2$$

$$\beta^3 = \beta^3$$

$$\beta^4 = \beta^3 + 1$$

$$\beta^5 = \beta(\beta^3 + 1) = \beta^4 + \beta = \beta^3 + 1 + \beta$$

$$\beta^6 = \beta(\beta^3 + 1 + \beta) = \beta^4 + \beta + \beta^2 = \beta^3 + 1 + \beta + \beta^2$$

$$\beta^7 = \beta(\beta^3 + 1 + \beta + \beta^2) = \beta^4 + \beta + \beta^2 + \beta^3$$

$$= \beta^3 + 1 + \beta + \beta^2 + \beta^3 = 1 + \beta + \beta^2$$

$$\beta^8 = \beta(1 + \beta + \beta^2) = \beta + \beta^2 + \beta^3$$

$$\beta^9 = \beta(\beta + \beta^2 + \beta^3) = \beta^2 + \beta^3 + \beta^4 = \beta^2 + \beta^3 + \beta^3 + 1$$

$$= \beta^2 + 1$$

$$\beta^{10} = \beta(\beta^2 + 1) = \beta^3 + \beta$$

$$\beta^{11} = \beta(\beta^3 + \beta) = \beta^4 + \beta^2 = \beta^3 + 1 + \beta^2$$

$$\beta^{12} = \beta(\beta^3 + 1 + \beta^2) = \beta^4 + \beta + \beta^3 = \beta^3 + 1 + \beta^3 + \beta = \beta + 1$$

$$\beta^{13} = \beta(1 + \beta) = \beta^2 + \beta$$

$$\beta^{14} = \beta(\beta + \beta^2) = \beta^2 + \beta^3$$

$$\beta^{15} = \beta(\beta^2 + \beta^3) = \beta^3 + \beta^4 = \beta^3 + \beta^3 + 1 = 1$$

So β is a primitive element, hence we gave a representation of the 15 powers of β above. This together with 0 gives complete elements of the field.

3. Conclusion

Galois groups of polynomials of small degree (≤4) were used to construct fields which are finite with the aid of some newly developed corollaries discussed by exploring some existing results. This report is expected to serve as a lecture note and as a reference material.

References

[1] Peters E. M. (1999) Galois Groups of Polynomials of Small Degree. A thesis submitted to the Department of Mathematics,

the Pennsylvania State University, the Schreyer Honors College.

[2] Cherowitz B. (2006) Introduction to Finite Fields, http://www.math.cudenver.edu/wcherowi/vβoutdrd/finflds.html.29k-.

[3] David, J.,(2002). A construction of finite fields. http://www.usna.edu/users/math/wdj/book/node58.html.

[4] Tudunkaya S. M. and Makanjuola S. O. (2012) Certain Quadratic Extensions. Journal of the Nigerian Association of Mathematical Physics, vol. 22, July issue.

[5] Tudunkaya S. M. and Makanjuola S. O. (2012) Certain Constrruction of Finite Fields. Journal of the Nigerian Association of Mathematical Physics, vol. 22, November issue.

[6] Tudunkaya S. M. (2007), Galois Groups of Polynomials of Small Degree and the Construction of Finite Fields. A thesis submitted to the Department of Mathematics, Bayero University, Kano, Nigeria.

[7] Lang, S.,(2004). Algebra, Graduate Texts in Mathematics (fourth edition). New York, Springer-Verlag.

[8] Jaisingh L. R. (2004). Abstract Algebra (second edition). McGRAW-HILL, New York.

[9] Brent, E.,2009. Symmetries of Equations : An introduction to Galois Theory: University of York,York Y010 5DD, England.

[10] Milne J. S. (2005) Fields & Galois Theory. Erehwon, Taiaroa Publishing.

[11] Adamson I. T (1964) Introduction to field theory, New York, Interscience publishers Inc.