A Brief Introduction to Galois Theory
Part II: Galois Theory

Robert H. C. Moir

January 26, 2004

Contents

1 Review of 'Part I: The Fundamentals'

1.1 Review of the Fundamental Algebraic Definitions

1.1.1 Groups

Group A *group* is a set G together with a law of composition $\cdot : G \times G \to G$ which is associative and has an identity element, and such that every element of G has an inverse.

An *abelian group* is a group whose law of composition is also commutative.

Isomorphism An *isomorhpism* is a bijective homomorphism. An *automorphism* is an isomorphism where the domain and range are the same set.

Cosets Let H be a subgroup of a group G, denoted $H \leq G$. A *left coset* is a subset of the form

$$aH = \{ah | h \in H\}.$$

It is easy to show that cosets form equivalence classes and hence partition the group. This allows us to define the *index* of a subgroup.

Index of a subgroup Let $H \leq G$. The *index* of H in G, denoted $[H : G]$, is the number of left cosets of H in G.

Normal subgroup Let $N \leq G$. N is a *normal subgroup* of G, denoted $N \trianglelefteq G$, if for every $a \in N$ and every $b \in G$, the conjugate bab^{-1} is in N.

It is easy to show that when a subgroup of a given group is normal the product of two cosets is again a coset, i.e. $(aN)(bN) = abN$. This has the effect of turning the set of cosets into a group.

Quotient group Let $N \trianglelefteq G$. Then the *quotient group* of G relative to N, denoted G/N, is the set of all cosets of N in G.

If $H \leq G$ is any subgroup the set of cosets is still denoted G/H, but G/H is only a group if H is normal.

1.1.2 Fields

Field A *field* is a set F together with two laws of composition $+ : F \times F \to F$ $((a, b) \rightsquigarrow a + b)$ and $\cdot : F \times F \to F$ $((a, b) \rightsquigarrow ab)$ called addition and multiplication, which satisfy the following axioms:

1. Addition makes F into an abelian group F^+.

2. Multiplication is associative and commutative and makes $F^\times = F - \{0\}$ into a group.
3. Distributive law: For all $a, b, c \in F$, $(a + b)c = ac + bc$.

Number field A *number field* K is a subfield of $\mathbb{C}$.

Characteristic of a field A field F is said to have *characteristic* p if $1+\cdots+1(p \text{ terms}) = 0$ in F, and if p is the smallest integer with this property. In the case the order is infinite, i.e. $1 + \cdots + 1$ is never 0 in F, the field is said to have *characteristic zero*.

Algebraically Closed Field A field F is said to be *algebraically closed* if every polynomial $f(x) \in F[x]$ of positive degree has a root in F.

Of course, the fact that the field $\mathbb{C}$ of complex numbers is algebraically closed is called the Fundamental Theorem of Algebra.

Field extension A *field extension* K of a field F, denoted K/F, is a field such that $F \subset K$.

Algebraic and transcendental elements Let K be an extension of a field F and let $\alpha \in K$. α is *algebraic over* F if it is the root of some nonzero polynomial with coefficients in F. An element α is called *transcendental over* F if it is not algebraic over F, i.e. it is not the root of any polynomial with coefficients in F.

F-isomorphism Let K and K' be field extensions of F. An *isomorphism of field extensions*, or *F-isomorphism*, is an isomorphism $\varphi : K \to K'$ which restricts to the identity on the subfield F.

A field extension can always be considered to be an F-vector space. Addition is the addition law in K and scalar multiplication of an element α of K by an element c of F is defined to be the product $c\alpha$ formed by multiplying these two elements in K. This leads us to another important definition.

Degree of a field extenison The *degree* of a field extension, denoted $[K : F]$, is the dimension of K as an F-vector space.

This is a convenient place to introduce the notion of a finite field extension.

Finite extension A field extension K of F is a *finite extension* iff its degree $[K : F]$ is finite.

Algebraic extension An extension K of a field F is an *algebraic extension*, and K is said to be *algebraic over* F, if all its elements are algebraic.

1.2 The Fundamentals of Field Extensions

Since Galois theory draws much from the theory of groups and of fields we must look at the important theorems in these areas that Galois theory depends on. This section is concerned with the results of Field Theory and the following section with those of Group Theory.

1.2.1 Algebraic Elements

The theory that we will consider here will assume that all fields are number fields. The entire theory that follows can be broached in a more general context by considering subfields that are all subfields of some fixed but otherwise arbitrary algebraically closed field of characteristic zero. This said, some of the theorems as they are stated, including the fundamental theorem, do hold for such general fields.

Let F be an arbitrary number field and let $\alpha_1, \cdots, \alpha_n$ be arbitrary numbers. Consider all possible fields which are extensions of the field F and contain all the numbers $\alpha_1, \cdots, \alpha_n$. The intersection of these fields, which is itself a field, is the *minimal extension* of the field F which contains $\alpha_1, \cdots, \alpha_n$. This minimal extension is denoted by $F(\alpha_1, \cdots, \alpha_n)$ and is called the extension *generated* by the numbers $\alpha_1, \cdots, \alpha_n$. It is useful to note that it can be shown that $F(\alpha_1, \cdots, \alpha_n) = F(\alpha_1)(\alpha_2)\cdots(\alpha_n)$, and so the extensions produced by adding numbers individually and all together produce the same field extension.

Let F be an arbitrary field and let α be algebraic over F. Then, by definition, α is a zero of some polynomial over the field F. The polynomial $f(x)$ with the smallest degree of all of these polynomials is called the *minimal polynomial* of the algebraic number α. This polynomial is irreducible because if it was reducible then α would be a root of a polynomial of smaller degree than $f(x)$ which contradicts the definition of $f(x)$. Thus we talk about the irreducible polynomial, or the minimal polynomial, corresponding to a number α algebraic over F. The unique degree of this polynomial is called the *degree of the algebraic number* α over the field F.

The degree has two important properties that should be pointed out.

Theorem 1 *If α is algebraic over F, then $[F(\alpha) : F]$ is the degree of the irreducible polynomial for α over F.*

Theorem 2 *Let $F \subset K \subset L$ be fields. Then $[L : F] = [L : K][K : F]$.*

I will end this section with two important propositions fundamental to the theory of field extensions. The first of these guarantees the existence of extensions that contains a root of an irreducible polynomial.

Theorem 3 *If $f(x)$ is an irreducible polynomial with coefficients in a field F, then there exists an extension K of F in which $f(x)$ has a root.*

This theorem is assuming that F is a number field, but there is a formal version of this theorem that allows you to adjoin a formal root to a given irreducible polynomal. The last theorem in this section gives the circumstances under which there is an isomorphism $F(\alpha) \longrightarrow F(\beta)$ which fixes F and sends α to β.

Theorem 4 *Let $\alpha \in K$ and $\beta \in L$ be algebraic elements of two extension fields of F. There is an isomorphism of fields*

$$\sigma : F(\alpha) \longrightarrow F(\beta),$$

which is the identity on the subfield F and which sends $\alpha \rightsquigarrow \beta$ iff the irreducible polynomials for α and β are equal.

1.2.2 Splitting Fields

Before we continue I must clarify an extra bit of notation that I will be using. In the formal approach to the theory of polynomials we consider a ring R, which is like a field but without a multiplicative inverse, with an indeterminate element x added to it. This forms a ring called a *polynomial ring* which is denoted $R[x]$. In our context here the coefficient ring is actually a field F, which forms a polynomial ring $F[x]$. So $F[x]$ is the set of all (formal) polynomials with coefficients in F.

If F, K and L are three fields such that $F \subset L \subset K$, then we call L an *intermediate field*. If K is an extension of a field F in which a polynomial $f(x)$ in $F[x]$ can be factored into linear factors and if $f(x)$ cannot be so factored in any intermediate field, then K is called a *splitting field* for $f(x)$. It follows from this definition that if K is the splitting field of $f(x)$, the roots of $f(x)$ generate K. A consequence of this is that $[K : F]$ is finite.

Theorem 5 *If $f(x)$ is a polynomial in $F[x]$, then there exists a splitting field K of $f(x)$.*

We now consider a theorem that gives us a better understanding of the structure of splitting fields.

Theorem 6 *Let f be an irreducible polynomial in $F[x]$. Then f has no multiple root in any field extension of F unless the derivative f' is the zero polynomial. In particular, if F is a field of characteristic zero, then f has no multiple root.*

1.3 Some Results from Group Theory

This section will briefly go through some of the important theorems from group theory.

1.3.1 Important Theorems for Finite Groups

The number of elements of a finite group G, denoted $|G|$, is called the *order* of the group. It is easy to show that there exists a bijection between the cosets of a subgroup H in G. This, together with the fact that the cosets partition the group gives us the important formula,

$$|G| = |H|[G : H]$$

called the *Counting Formula*. Of course this can also be written as $|G| = |H||G/H|$. As a consequence of this formula we get a basic theorem of group theory.

Theorem 7 *Lagrange's Theorem: Let G be a finite group, and let $H \leq G$. Then the order of H divides the order of G.*

2 A Brief Introduction to Galois Theory

Galois theory is concerned with the study of all the roots of an irreducible polynomial

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0,$$

and the symmetries among these roots. Thus it naturally involves the theory of field extensions and groups. The discovery that the relationship between the complete set of roots of a polynomial could be understood in terms of symmetry came out of the work of many mathematicians, especially that of Lagrange and Galois [2]. The original model for this symmetry is complex conjugation, which permutes the two roots $\pm i$ of the irreducible real polynomial $x^2 + 1$, while leaving the real numbers fixed. The group of symmetries among the roots of this polynomial is clearly $S_2 \cong C_2$. We also notice that complex conjugation is an $\mathbb{R}$-automorphism of $\mathbb{C}$. In general, for a field extension K/F, the group of all F-automorphisms of K is called the *Galois group* of the field extension. We denote this group by $G(K/F)$. Thus, for the extension $\mathbb{R}(i)$, the Galois group $G(\mathbb{R}(i)/\mathbb{R})$ is S_2 and hence has order 2.

Theorem 8 *For any finite extension K/F, the order $|G(K/F)|$ of the Galois group divides the degree $[K : F]$ of the extension.*

A finite field extension K/F is called a *Galois extension* if the order of the Galois group is equal to the degree:

$$|G(K/F)| = [K : F].$$

Thus, we see that $\mathbb{R}(i)/\mathbb{R}$ is a Galois extension. If G is a group of automorphisms of a field K, the set of elements of K which are fixed by all the automorphisms in G forms a subfield, called the *fixed field* of G. We will denote the fixed field by K^G:

$$K^G = \{\alpha \in K | \varphi(\alpha) = \alpha \text{ for all } \varphi \in G\}.$$

So the fixed field of $G(\mathbb{R}(i)/\mathbb{R})$ is $\mathbb{R}$. Theorem 8 leads to the following corrolary:

Corollary 1 *Let K/F be a Galois extension, with Galois group $G = G(K/F)$. The fixed field of G is F.*

2.1 Quadratic and Biquadratic Extensions

2.1.1 Quadratic Extensions

We will begin with the simplest possible case, that of an extension K/F of degree 2. Such an extension is generated by any element α of K that is not in F. It is also the case that α is a root of an irreducible quadratic polynomial

$$f(x) = x^2 + bx + c$$

with coefficients in F. It is not hard to see that $\alpha' = -b - \alpha$ is also a root of f and so f splits into linear factors over K. This, along with theorem 4 gives us a symmetry: the isomorphism

$$\sigma : F(\alpha) \longrightarrow F(\alpha'),$$

which is the identity on F and sends $\alpha \rightsquigarrow \alpha'$. Since either root generates the same extension ($F(\alpha) = K = F(\alpha')$), σ is an automorphism of K.

Since the two roots are not identical (otherwise $K = F$), the automorphism is a permutation of the two roots that is not the identity. This is so since $\alpha + \alpha' = b \in F$ and σ fixes F. Thus σ^2 must be the identity. Thus we see that $\{1, \sigma\} \subseteq G(K/F)$ and $|G(K/F)| \geq 2$. By the magic of theorem 8 we see that this implies that $\{1, \sigma\} = G(K/F)$, so that K is a Galois extension of F. Such extensions K are called **quadratic extensions**.

2.1.2 Biquadratic Extensions

The next simplest example is that of a **biquadratic extension**. A biquadratic extension is defined as a field extension K/F such that $[K : F] = 4$ and which is generated by the roots of two irreducible quadratic polynomials with coefficients in F. It can be shown that every such extension has the form

$$K = F(\alpha, \beta),$$

where $\alpha^2 = a$ and $\beta^2 = b$, and $a, b \in F$.

An important difference between this case and quadratic extensions is that the element α generates an *intermediate field* $F(\alpha)$. Now, since $K = F(\alpha, \beta)$ and $[K : F] = 4$, $F(\alpha)$ has degree 2 over F (by theorem 2), whence β is not an element of $F(\alpha)$. Thus the polynomial $x^2 - b$ is irreducible over $F(\alpha)$. Similarly $x^2 - a$ is irreducible over $F(\beta)$. Notice also that theorem 2 implies that $[K : F(\alpha)] = 2$ and so K is a quadratic extension of $F(\alpha)$. Thus there is an $F(\alpha)$-automorphism σ that interchanges the roots $\pm\beta$ of $x^2 - b$. Since σ it is an $F(\alpha)$-automorphism its fixed field is $F(\alpha)$ and so σ also fixes F. Similarly there is an $F(\beta)$-automorphism τ that interchanges the roots $\pm\alpha$ of $x^2 - a$ that is also an F-automorphism. From this we can now see that τ sends $\alpha \rightsquigarrow -\alpha$ and σ sends $\beta \rightsquigarrow -\beta$, from which it follows that $\sigma\tau$ changes the sign of both roots. Clearly the squares of each of these maps is the identity, so the four automorphisms $\{1, \sigma, \tau, \sigma\tau\}$ form a group of order 4 that satisfies the relations

$$\sigma^2 = 1, \tau^2 = 1, \sigma\tau = \tau\sigma.$$

This happens to be the Klein four group. Thus $\{1, \sigma, \tau, \sigma\tau\} \subseteq G(K/F)$. Once again, by the magic of theorem 8 we see that this implies that $\{1, \sigma, \tau, \sigma\tau\} = G(K/F)$, so that K is a Galois extension of F.

We have seen that quadratic and biquadratic extensions are both Galois extensions. It also happens to be that case that they are splitting fields of irreducible polynomials over the base field F. This is evidence of a general pattern expressed by the following theorem.

Theorem 9 *If K is a splitting field of a polynomial $f(x)$ over F, then K is a Galois extension of F. Conversely, every Galois extension is a splitting field of some polynomial $F[x]$.*

We are now ready to state the fundamental theorem.

2.2 The Fundamental Theorem of Galois Theory

We are now in a position to begin to understand a beautiful theorem called *The Fundamental Theorem of Galois Theory.*

Theorem 10 *The Fundamental Theorem: Let K be a Galois extension of a field F, and let $G = G(K/F)$ be its Galois group. The function*

$$H \rightsquigarrow K^H$$

is a bijective map from the set of subgroups of G to the set of intermediate fields $F \subset L \subset K$. Its inverse function is

$$L \rightsquigarrow G(K/L).$$

This correspondence has the property that if $H = G(K/L)$, then

$$[K : L] = |H|, \text{ and hence } [L : F] = [G : H].$$

2.3 Cubic Equations

With the fundamental theorem in hand, we will now apply it to examine the properties of the splitting fields of cubic equations

$$f(x) = x^3 + a_2x^2 + a_1x + a_0.$$

There is a useful trick that allows us to simplify the form of cubic equations. Using the substitution $x \rightsquigarrow x - a_2/3$, the general cubic above becomes

$$f(x) = x^3 + px + q,$$

where p and q are elements of F. Now let K be a splitting field for $f(x)$ over F and let $\alpha_1, \alpha_2, \alpha_3$ be the roots of f in K, in arbitrary order, so that we have

$$f(x) = x^3 + px + q = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3).$$

By expanding the right side we can see that

$$\alpha_1 + \alpha_2 + \alpha_3 = 0,$$

which implies that the third root α_3 is in the field generated by the other two. Supposing, now, that $f(x)$ is irreducible, this implies that there is a chain of fields

$$F \subset F(\alpha_1) \subseteq K,$$

with $K = F(\alpha_1, \alpha_2) = F(\alpha_1, \alpha_2, \alpha_3)$. Denoting $F(\alpha_1)$ by L, we have two distinct cases:

$$L = K \text{ or } L < K.$$

The former case occurs when α_2 and α_3 can be written in terms of α_1 and elements of F, whereas the latter occurs when there is no such expression.

In $L[x]$, $f(x)$ has the factor $(x - \alpha_1)$ so that

$$f(x) = (x - \alpha_1)h(x),$$

where $h(x)$ is a quadratic polynomial with coefficients in L. From the 'splitting equation' of f above, we see that $h(x) = (x - \alpha_2)(x - \alpha_3)$ in $K[x]$. Thus, we can now see that $L < K$ iff $h(x)$ is irreducible over L. In this case, since h is a quadratic polynomial irreducible over L, $L(\alpha_2) = K$ has degree 2 over L. In either case, because $f(x)$ is irreducible over F, $[L : F] = 3$ by theorem 1. This finally gives us

$$[K : F] = \begin{cases} 3 \text{ if } L=K \\ 6 \text{ if } L<K \end{cases}.$$

From theorem 8 the order of the Galois group $G = G(K/F)$ is equal to the degree $[K : F]$, so K/F is a Galois extension. It can be shown that F-automorphisms permute the roots of the irreducible polynomial, and that the only F-automorphism that fixes all the roots is the identity. This implies that $G \subseteq S_3$, which has order 6. So if $[K : F] = 6$, $G = S_3$ and if $[K : F] = 3$, then $G = A_3$, the only subgroup of S_3 of order 3. In this latter case there are no intermediate fields (A_3 has no subgroups) but there are in the former case and we can determine these using the fundamental theorem.

S_3 has three conjugate subgroups of order 3 and one subgroup of order 3, namely A_3. There are three obvious intermediate fields $F(\alpha_1), F(\alpha_2), F(\alpha_3)$, which are isomorphic but not equal subfields of K, which must correspond to the three subgroups of order 2. The field corresponding to A_3 is more difficult to find, however. From the fundamental theorem we know that $G(K/L) = A_3$, so $[K : L] = 3$ and $[L : F] = 2$ which implies that L is a quadratic extension of F, which can be obtained by adjoining a square root. Thus L, and hence K, contains a square root δ of an element of F. According to the fundamental theorem L is the fixed field of A_3, so an even permutation of the roots leaves δ fixed, while an odd one does not. Thus suggests the choice

$$\delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3).$$

To see that this is the correct choice we note that δ is not fixed by every element of $G(K/F) = S_3$ so $\delta \notin F$. On the other hand δ^2 is fixed by every permutation, so by corollary 1 $\delta^2 \in F$.

2.4 A More Complete Fundamental Theorem

Theorem 11 *The Fundamental Theorem: Let K be a Galois extension of a field F, and let $G = G(K/F)$ be its Galois group. The function*

$$H \rightsquigarrow K^H$$

is a bijective map from the set of subgroups of G to the set of intermediate fields $F \subset L \subset K$. Its inverse function is

$$L \rightsquigarrow G(K/L).$$

This correspondence has the following properties:

1. *if $H = G(K/L)$, then $[K : L] = |H|$, and hence $[L : F] = [G : H]$.*
2. *L is a Galois extension of F iff $H \trianglelefteq G$. In such a case $G(L/F) \cong G/H$.*

References

[1] Artin, Emil. *Galois Theory.* Edwards Brothers, Inc.: Ann Arbour, 1959.

[2] Artin, Michael. *Algebra.* Prentice Hall: New Jersey, 1991.

[3] Postnikov, M. M. *Fundamentals of Galois Theory.* P. Noordhoff Ltd.: Groningen, 1962.