PRINCIPLES OF GALOIS THEORY

Xantcha

22nd November 2013

> La Nature est un temple où de vivants piliers
> Laissent parfois sortir de confuses paroles;
> L'homme y passe à travers des forêts de symboles
> Qui l'observent avec des regards familiers.
>
> — Baudelaire, *Correspondances*

These lecture notes were compiled with the modest aim of providing a brief, non-technical introduction to the Galois Correspondence. Without delving into a profusion of detail of this complicated machinery, it will, or so we hope, still manage communicate the essential ideas — a *Galois Theory for Dummies*, so to speak.

Being a simplified version, the theory presented is valid only for algebraic extensions of $\mathbf{Q}$. Hence, there shall always be a tacit understanding that all fields be extensions of $\mathbf{Q}$ and therefore, being algebraic, contained in $\overline{\mathbf{Q}}$.

Basic knowledge of Group and Field Theory will be assumed on the part of the reader:

1. Algebraic elements, their minimal polynomials and degrees.
2. Algebraic extensions and their degrees. The *Tower Law:* If $K \geqslant E \geqslant F$, then
$$[K : F] = [K : E][E : F].$$
Finite extensions are algebraic.
3. The structure of Simple Extensions: If α is algebraic over F, with minimal polynomial $p(x)$, then
$$F(\alpha) \cong F[x]/(p(x)).$$

4. Algebraic closure. An algebraically closed field has no non-trivial algebraic extensions.

5. Soluble groups: G is *soluble* if there exists a chain of subgroups

$$\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_{n-1} \trianglelefteq G_n = G,$$

with all successive factor groups G_k/G_{k-1} *cyclic*.

Briefly, Galois Theory traces its origins to mankind's desire to solve algebraical equations — by *algebraical means*, it ought to be added. This latter word denotes the four standard operations of arithmetic, in conjunction with root extractions. It scored one of Abstract Algebra's earliest and most glorious victories when it was cleverly deployed, by Abel and Galois independently, to shew that such a feat is not always possible.

An historical outline goes as follows:

The Linear Equation. Solved by all four River Civilisations (Egypt, Mesopotamia, India, China).

The Quadratic Equation. Solved by the Babylonians and the Chinese. Because they had no symbolic algebra available, and so could express no formulæ, their discourse would always be based on a lengthy argument in words. Also, what we nowadays consider a general quadratic would be split up into several cases, because negative numbers were yet not available.

The Cubical Equation. The Art of Symbolic Algebra ripened during the Renaissance, and reaped two victories in quick succession: resolving the cubic *and* the quartic, with mere decades in between. The solution of the cubic was accomplished by del Ferro and Tartaglia during the first half of the 16th century, and the method was subsequently published in the *magnum opus* of Cardano, *Ars Magna* (1545). It has, of course, been credited to neither del Ferro nor Tartaglia, but is known as *Cardano's Formula*.

The Quartical Equation. Resolved by Cardano's student Ferrari. The solution was also included in the *Ars Magna*.

The Quintical Equation. Lagrange made the first progress on the problem when he shewed that those methods which had successfully attacked the equations of lower degree, would invariably *fail* for the quintic. From his vague ideas, and drawing on the crisp and powerful language of Abstract Algebra, at that time sprouting, crystallised Abel and Galois's brilliant

insight that *the general quintical equation is insoluble in radicals*, in the sense that *no general closed formula, applying the four standard operations of arithmetic and successive root extractions to the co-efficients, will manufacture the solutions.* This is *Abel's Impossibility Theorem* (1824); see Theorem 9 below.

§1. Splitting Fields

The notion of a splitting field is rather a natural one. When adjoining one root of a polynomial equation to the ground field, one may well ask: why not adjoin all of them?

Definition 1. — Let $f(x) \in F[x]$. The **splitting field** of $f(x)$ is the smallest subfield of $\overline{F}$ containing (F and) the zeroes of $f(x)$.

The splitting field is thus the smallest field in which $f(x)$ *splits completely* (decomposes as a product of linear factors).

Example 1. — The field $\mathbf{C}$ contains the zeroes of x^2+1, but it is not the smallest such field, hence not the splitting field. The splitting field of x^2+1 (over $\mathbf{Q}$) is, of course, $\mathbf{Q}(i)$. △

Example 2. — The field $\mathbf{Q}(e^{\frac{\pi i}{4}})$ is the splitting field of both x^4+1 and $x^8-1 = (x^4-1)(x^4+1)$. The latter polynomial is not irreducible, but such a requirement was never stipulated. △

Theorem 1. — *If E is the splitting field of F, then any irreducible polynomial over F having but a single zero in E, must necessarily have* all *its zeroes in E, and so will split completely into linear factors.*

There may, of course, still exist polynomials that do not split over E, namely those *not* having a single zero in E. In order to furnish zeroes to *all* polynomials over F, one has to pass to the algebraic closure.

§2. Finite Extensions

We already know that finite extensions are algebraic. The theorem that follows asserts that finite extensions of $\mathbf{Q}$, the only type that shall concern us, are always simple. This knowledge is extremely useful, the structure of simple extensions admitting an explicit description (as the quotient of the polynomial ring by the minimal polynomial). The theorem is a classic of Field Theory.

Theorem 2: The Primitive Element Theorem. — *Suppose F is an algebraic extension of $\mathbf{Q}$. All finite extensions of F are simple.*

Proof. A finite extension is generated by finitely many elements. By induction, it shall be sufficient to shew that an extension $F(\alpha, \beta)$ generated by two elements is, in fact, generated by a single element. Since everything is algebraic, we have $\mathbf{Q} \leqslant F \leqslant F(\alpha, \beta) \leqslant \overline{\mathbf{Q}}$.

Let the zeroes of $f(x) = \operatorname{irr}_F \alpha$ be $\alpha = \alpha_1, \ldots, \alpha_m$ and those of $g(x) = \operatorname{irr}_F \beta$ be $\beta = \beta_1, \ldots, \beta_n$. The element β is a single zero of g since, if it were not, then it would be a zero also of $g'(x)$, which is of lower degree than $g(x)$.

Choose $q \in F$ such that $q(\beta_j - \beta) \neq \alpha_i - \alpha$, for all i and $j \neq 1$. Obviously $F(\alpha, \beta) \supseteq F(\alpha - q\beta)$. We now prove that containment also goes the other way.

Consider the polynomial

$$h(x) = f(\alpha + q(x - \beta)) \in F(\alpha - q\beta)[x].$$

It fulfils $h(\beta_j) = 0$ precisely when $j = 1$, so it is divisible by $\operatorname{irr}_{F(\alpha - q\beta)} \beta$. But $\operatorname{irr}_{F(\alpha - q\beta)} \beta$ also divides $\operatorname{irr}_F \beta = g(x)$, and the polynomials g and h only have the common zero β, which, as we just shewed, is single. Consequently, $\operatorname{irr}_{F(\alpha - q\beta)} \beta = x - \beta$, and so $\beta \in F(\alpha - q\beta)$. Then also $\alpha \in F(\alpha - q\beta)$, and hence $F(\alpha, \beta) = F(\alpha - q\beta)$. □

§3. The Conjugation Isomorphisms

The pivotal theme Galois Theory revolves around is Field Automorphisms, isomorphisms of a field with itself. Before restricting our attention to this particular type, we shall ensure an adequate supply of isomorphisms of (possibly distinct) fields.

Theorem 3: The Conjugation Isomorphism Theorem. — *Let* α *and* β *be algebraic over the field* F*. The map*

$$\psi_{\alpha,\beta} \colon F(\alpha) \to F(\beta)$$
$$c_0 + c_1\alpha + \cdots + c_k\alpha^k \mapsto c_0 + c_1\beta + \cdots + c_k\beta^k,$$

is an isomorphism of fields if and only if α *and* β *have the same minimal polynomial over* F*.*

Proof. Suppose $\psi_{\alpha,\beta}$, as defined above, is an isomorphism, and let the minimal polynomial of α be $a_0 + a_1 x + \cdots + a_n x^n$. Then

$$0 = \psi_{\alpha,\beta}(0) = \psi_{\alpha,\beta}(a_0 + a_1\alpha + \cdots + a_n\alpha^n) = a_0 + a_1\beta + \cdots + a_n\beta^n,$$

and since a minimal polynomial is always irreducible, $a_0 + a_1 x + \cdots + a_n x^n$ is the minimal polynomial also of β.

Conversely, suppose α and β share the minimal polynomial $p(x)$. Then, by the structure of simple extensions,

$$F(\alpha) \cong F[x]/(p(x)) \cong F(\beta),$$

with the isomorphism $F[x]/(p(x)) \to F(\alpha)$ given by $x + (p(x)) \mapsto \alpha$. The composite isomorphism

$$F(\alpha) \to F[x]/(p(x)) \to F(\beta)$$

is then given by

$$\alpha \mapsto x + (p(x)) \mapsto \beta,$$

which is the map $\psi_{\alpha,\beta}$ sought for. □

Definition 2. — Two elements sharing the same minimal polynomial, as in the theorem above, are called **conjugate**.

The Conjugation Isomorphism Theorem then states: An algebraic element may transform into any of its conjugates, and into its conjugates *only*, under a field isomorphism.

Example 3. — Consider, for example, the two numbers $\sqrt[3]{2}$ and $\sqrt[3]{2}\zeta$, where $\zeta = e^{\frac{2\pi i}{3}}$ denotes a third root of unity. They share the minimal polynomial $x^3 - 2$. By the theorem, the map

$$\psi_{\sqrt[3]{2},\sqrt[3]{2}\zeta} \colon a + b\sqrt[3]{2} + c\sqrt[3]{4} \mapsto a + b\sqrt[3]{2}\zeta + c\sqrt[3]{4}\zeta^2$$

provides an isomorphism $\mathbf{Q}(\sqrt[3]{2}) \to \mathbf{Q}(\sqrt[3]{2}\zeta)$. △

§4. Extension of Isomorphisms

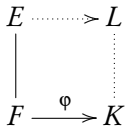
Extension of isomorphisms is a recurrent theme in Galois Theory. We here state, without proof, a very general theorem governing these.

We remind the reader that, by an *extension* of the map $\varphi \colon X \to Y$, is meant a map $\hat{\varphi} \colon X' \to Y'$, where $X' \supseteq X$ and $Y' \supseteq Y$, such that $\hat{\varphi}(x) = \varphi(x)$ for all $x \in X$:

$$\begin{array}{ccc} X' & \xrightarrow{\hat{\varphi}} & Y' \\ \big| & & \big| \\ X & \xrightarrow{\varphi} & Y \end{array}$$

Theorem 4: The Isomorphism Extension Theorem. — *Let $F \leqslant E$ be an algebraic extension and let $\varphi \colon F \to K$ be an isomorphism. Then there exists an extension of φ*

to an isomorphism of E with some algebraic extension L of K.



Example 4. — Consider again the previous example, that of the isomorphism

$$\begin{gathered}\mathbf{Q}(\sqrt[3]{2}) \to \mathbf{Q}(\sqrt[3]{2}\zeta) \\ a + b\sqrt[3]{2} + c\sqrt[3]{4} \mapsto a + b\sqrt[3]{2}\zeta + c\sqrt[3]{4}\zeta^2.\end{gathered}$$

By the theorem, this isomorphism extends to an isomorphism

$$\mathbf{Q}(\sqrt[3]{2}, \zeta) \to L,$$

for some algebraic extension $L \supseteq \mathbf{Q}(\sqrt[3]{2}\zeta)$, and also to an isomorphism

$$\overline{\mathbf{Q}} \to M,$$

for some (presumably larger) algebraic extension $M \supseteq \mathbf{Q}(\sqrt[3]{2}\zeta)$. △

§5. Field Automorphisms

Definition 3. — An isomorphism of a field with itself is called an **automorphism** of the field.

Definition 4. — Let $F \leqslant E$ be a field extension. The **automorphism group** of E over F is

$$\operatorname{Aut}(E/F) = \{\, \sigma\colon E \to E \mid \forall \alpha \in F : \sigma(\alpha) = \alpha \,\}.$$

It is the set of those automorphisms of E *fixing* F.

Definition 5. — Let $F \leqslant E$ be a field extension and let $G \leqslant \operatorname{Aut}(E/F)$. The **fixed field** of G is

$$\operatorname{Fix} G = \{\, \alpha \in E \mid \forall \sigma \in G : \sigma(\alpha) = \alpha \,\}.$$

It is the set of those field elements *left fixed* by the automorphisms in G.

Example 5. — Consider the map

$$\begin{gathered}\mathbf{Q}(\sqrt{2}, \sqrt{3}) \to \mathbf{Q}(\sqrt{2}, \sqrt{3}) \\ a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mapsto a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}.\end{gathered}$$

It may be viewed as the conjugation isomorphism

$$\psi_{\sqrt{3},-\sqrt{3}}\colon \mathbf{Q}(\sqrt{2})(\sqrt{3}) \to \mathbf{Q}(\sqrt{2})(\sqrt{3})$$

— note that $\pm\sqrt{3}$ share the minimal polynomial $x^2 - 3$ over $\mathbf{Q}(\sqrt{2})$.

Since $\psi^2_{\sqrt{3},-\sqrt{3}} = \iota$, the two automorphisms

$$\{\iota, \psi_{\sqrt{3},-\sqrt{3}}\}$$

form a two-element subgroup of $\mathrm{Aut}(\mathbf{Q}(\sqrt{2},\sqrt{3})/\mathbf{Q})$. The fixed field is

$$\mathrm{Fix}\{\iota, \psi_{\sqrt{3},-\sqrt{3}}\} = \mathbf{Q}(\sqrt{2}),$$

for

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}$$

if and only if $c = d = 0$. This means, of course, that both ι and $\psi_{\sqrt{3},-\sqrt{3}}$, in fact, belong to

$$\mathrm{Aut}(\mathbf{Q}(\sqrt{2},\sqrt{3})/\mathbf{Q}(\sqrt{2})).$$

Hence the *group* $\{\iota, \psi_{\sqrt{3},-\sqrt{3}}\}$ has the fixed *field* $\mathbf{Q}(\sqrt{2})$, and, conversely, the *field* $\mathbf{Q}(\sqrt{2})$ gives rise to the automorphism *group*

$$\mathrm{Aut}(\mathbf{Q}(\sqrt{2},\sqrt{3})/\mathbf{Q}(\sqrt{2})) = \{\iota, \psi_{\sqrt{3},-\sqrt{3}}\}.$$

This is our first fleeting glimpse of the Galois Correspondence, the remarkable dual relationship between *Automorphism Groups*, on the one hand, and their *Fixed Fields*, on the other. △

§6. Normal Extensions

We now examine two concrete instances exhibiting the Galois Correspondence at play, and then proceed to investigate a field extension which does *not* reproduce this effect. From a fastidious analysis of the malfunction, we are led to the notion of a *normal extension*.

Example 6. — As our first, simple example, we consider the field extension

$$\mathbf{Q} \leqslant \mathbf{Q}(\sqrt{2}) = \left\{\, a + b\sqrt{2} \;\middle|\; a, b \in \mathbf{Q} \,\right\}.$$

Associating, to each of these two fields F, the automorphism group

$$\mathrm{Aut}(\mathbf{Q}(\sqrt{2})/F),$$

we are led to the following picture:

$$\begin{array}{ccc} \mathbf{Q}(\sqrt{2}) & & \mathrm{Aut}(\mathbf{Q}(\sqrt{2})/(\mathbf{Q}\sqrt{2})) = \{[\sqrt{2}\mapsto\sqrt{2}]\} \\ \Big| & & \Big| \\ \mathbf{Q} & & \mathrm{Aut}(\mathbf{Q}(\sqrt{2})/\mathbf{Q}) = \{[\sqrt{2}\mapsto\sqrt{2}]\,,[\sqrt{2}\mapsto-\sqrt{2}]\} \end{array}$$

The bottom group, consisting of those automorphisms fixing $\mathbf{Q}$ only, is the group with two elements, whereas the top group, consisting of those automorphisms fixing the whole of $\mathbf{Q}(\sqrt{2})$, contains just the identity map. One may reverse the procedure. Given one of the two groups G, it arises from the field $\mathrm{Fix}\, G$.

We observe that the smallest field leads to the largest group, and conversely. The group lattice is upside-down, with the smallest group on top. △

Example 7. — Next, we return to the field extension

$$\mathbf{Q} \leqslant \mathbf{Q}(\sqrt{2},\sqrt{3}) = \left\{ a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \;\middle|\; a,b,c,d \in \mathbf{Q} \right\}.$$

There are three intermediate fields, shewn in Figure 1. Again we have, to each field F, associated the group

$$\mathrm{Aut}(\mathbf{Q}(\sqrt{2},\sqrt{3})/F)$$

of automorphisms fixing F. Once more, we observe that the group lattice is pitched upside-down, with the smallest group residing on top, and that the procedure may be reversed. To each group G corresponds the field $\mathrm{Fix}\, G$. Every intermediate field has been included in the field lattice, and all subgroups of

$$\mathrm{Aut}(\mathbf{Q}(\sqrt{2},\sqrt{3})/\mathbf{Q}) \cong \mathbf{Z}_2 \times \mathbf{Z}_2$$

occur in the group lattice. △

The preceding cases display the ideas at the heart of Galois Theory, and the reader is advised to study them carefully. The next example is issued as an admonition.

Example 8. — The field extension

$$\mathbf{Q} \leqslant \mathbf{Q}(\sqrt[3]{2}) = \left\{ a + b\sqrt[3]{2} + c\sqrt[3]{4} \;\middle|\; a,b,c \in \mathbf{Q} \right\}$$

leads to the following field and group lattices:

$$\begin{array}{ccc} \mathbf{Q}(\sqrt[3]{2}) & & \mathrm{Aut}(\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}(\sqrt[3]{2})) = \{[\sqrt[3]{2}\mapsto\sqrt[3]{2}]\} \\ \Big| & & \Big| \\ \mathbf{Q} & & \mathrm{Aut}(\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}) = \{[\sqrt[3]{2}\mapsto\sqrt[3]{2}]\} \end{array}$$

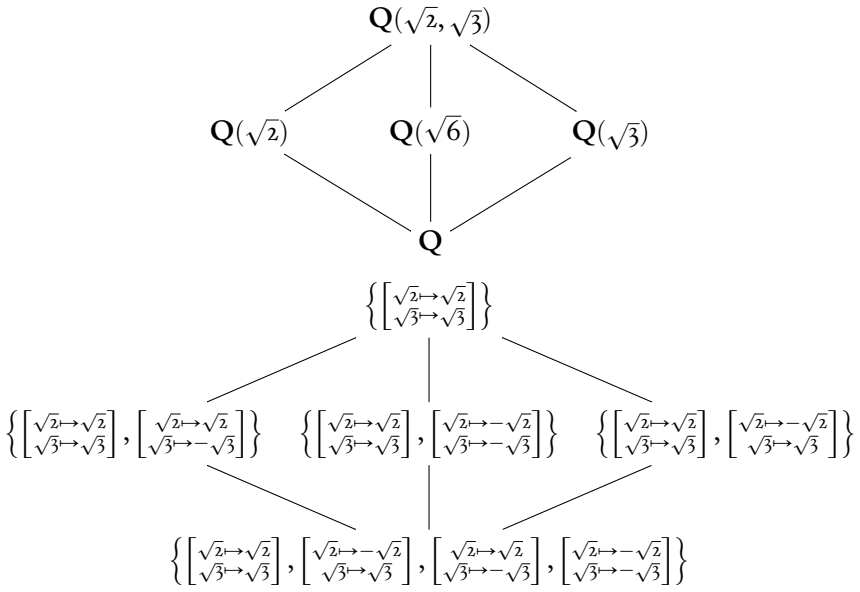


FIGURE 1: Galois Correspondence for the Field Extension $\mathbf{Q} \leqslant \mathbf{Q}(\sqrt{2},\sqrt{3})$.

There are no intermediate fields, because, for any $\mathbf{Q} \leqslant E \leqslant \mathbf{Q}(\sqrt[3]{2})$, we have

$$3 = [\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}] = [\mathbf{Q}(\sqrt[3]{2}) : E][E : \mathbf{Q}]$$

by the Tower Law. Hence either $[\mathbf{Q}(\sqrt[3]{2}) : E] = 1$ or $[E : \mathbf{Q}] = 1$.

The picture painted by this field extension isn't nearly as dainty as those of the two previous examples. *Both* fields produce the same trivial automorphism group, so there is no longer a one-to-one correspondence between fields and groups. △

What went wrong this last time? The anomaly seems to lie with the bottom group. Even though we require these automorphisms to fix only $\mathbf{Q}$, no more automorphisms are obtained — nothing beyond the identity map. How come? Simply because there is no choice for the image of $\sqrt[3]{2}$. By the Conjugation Isomorphism Theorem, $\sqrt[3]{2}$ has to transform into one of its conjugates by an automorphism, but those conjugates are $\sqrt[3]{2}\zeta$ and $\sqrt[3]{2}\zeta^2$ (the minimal polynomial being $x^3 - 2$) and *not included in the field* $\mathbf{Q}(\sqrt[3]{2})$.

What we have witnessed is a defect in the field extension, which we now seek to remedy.

DEFINITION 6. — The finite field extension $F \leqslant E$ is **normal** (or **Galois**) if any

(hence all) of the following equivalent conditions be satisfied:

A. E is the splitting field of some polynomial with co-efficients in F.

B. $F = \operatorname{Fix}\operatorname{Aut}(E/F)$.

C. $[E : F] = |\operatorname{Aut}(E/F)|$.

D. All automorphisms of $\overline{F}$ that fix F, automatically leave E *set-wise*[1] invariant.

Proving the equivalence of the above four conditions calls for some highly technical machinery and is best reserved for a proper course in Galois Theory.

Let us cogitate a bit on B, which is not as trivially true as might appear. We have, just spelling out the definition,

$$\operatorname{Fix}\operatorname{Aut}(E/F) = \{\, \alpha \in E \mid \forall \sigma \in \operatorname{Aut}(E/F) : \sigma(\alpha) = \alpha \,\}.$$

In words: *These are the elements left fixed by everything that fixes F.* Naturally, F itself is included in this set, so $F \leqslant \operatorname{Fix}\operatorname{Aut}(E/F)$, but *there may be further fixed points.* The condition in B, that $\operatorname{Fix}\operatorname{Aut}(E/F)$ be equal to F, may be phrased: *The field automorphisms that fix F, fix* only *F.*

Example 9. — The field extension $\mathbf{Q} \leqslant \mathbf{Q}(\sqrt{2}, \sqrt{3})$ passes the four tests with flying flags:

A. $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ is the splitting field of the polynomial $(x^2 - 2)(x^2 - 3)$.

B. As can be seen from the lattices in Figure 1 above,

$$\operatorname{Fix}\operatorname{Aut}(\mathbf{Q}(\sqrt{2}, \sqrt{3})/\mathbf{Q}) = \mathbf{Q},$$

since there exist automorphims dislocating both square roots.

C. As may also be gathered from the lattices,

$$[\mathbf{Q}(\sqrt{2}, \sqrt{3}) : \mathbf{Q}] = 4 = |\operatorname{Aut}(\mathbf{Q}(\sqrt{2}, \sqrt{3})/\mathbf{Q})|.$$

D. Any automorphism of $\overline{\mathbf{Q}}$ must either preserve or switch the roots of the two equations $x^2 = 2$ and $x^2 = 3$, so $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ is left invariant.

△

Example 10. — On the other hand, the extension $\mathbf{Q} \leqslant \mathbf{Q}(\sqrt[3]{2})$ fizzles miserably:

[1] This is the *only* place where *set-wise invariance* plays a rôle. In all other instances, we are concerned with automorphisms *fixing* a field, by which term we always mean *element-wise invariance.*

A. $\mathbf{Q}(\sqrt[3]{2})$ is not a splitting field. It is certainly not the splitting field of x^3-2, and therefore, in accordance with Theorem 1, of no other polynomial either.

B. We saw above that

$$\operatorname{Fix}\operatorname{Aut}(\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}) = \operatorname{Fix}\{\iota\} = \mathbf{Q}(\sqrt[3]{2}) \neq \mathbf{Q}.$$

C. We also found that

$$[\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}] = 3 \neq 1 = |\{\iota\}| = |\operatorname{Aut}(\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q})|.$$

D. Finally, the conjugation isomorphism

$$\Psi_{\sqrt[3]{2},\sqrt[3]{2}\zeta} \colon \sqrt[3]{2} \mapsto \sqrt[3]{2}\zeta$$

gives (by the Isomorphism Extension Theorem) an automorphism of $\overline{\mathbf{Q}}$ *not* leaving $\mathbf{Q}(\sqrt[3]{2})$ invariant.

△

§7. Properties of Normal Extensions

Theorem 5. — *Let $F \leqslant E \leqslant K$ be such that $F \leqslant K$ is normal. Then $E \leqslant K$ is also normal.*

Proof. If K is the splitting field of $f(x)$ over F, then K is also the splitting field of $f(x)$ over E. □

Example 11. — On the other hand, $F \leqslant E$ need not be normal. For example, in

$$\mathbf{Q} \leqslant \mathbf{Q}(\sqrt[3]{2}) \leqslant \mathbf{Q}(\sqrt[3]{2}, \sqrt[3]{2}\zeta, \sqrt[3]{2}\zeta^2),$$

the whole extension is normal (it is the splitting field of $x^3 - 2$), but, as we strove to make clear above, not the bottom one. △

Theorem 6. — *Consider an algebraic extension $F \leqslant K \leqslant \overline{F}$.*

- *Every automorphism $\tau \in \operatorname{Aut}(K/F)$ extends (non-uniquely) to an automorphism of $\overline{F}$.*
- *Conversely, if $F \leqslant K$ is normal, then every $\sigma \in \operatorname{Aut}(\overline{F}/F)$ restricts to an automorphism of K.*

Proof.

- According to the Isomorphism Extension Theorem, every automorphism $\tau \in \mathrm{Aut}(K/F)$ extends to an isomorphism σ of $\overline{F}$ with an algebraic extension E of F. Consider the inverse $\sigma^{-1}\colon E \to \overline{F}$. Again by the Isomorphism Extension Theorem, σ^{-1} extends to an isomorphism of $\overline{F}$ (which contains E, since $E \geqslant F$ is algebraic), with an algebraic extension of $\overline{F}$. But $\overline{F}$ is algebraically closed and has no algebraic extensions. Therefore σ^{-1} must already be an isomorphism of $\overline{F}$ with itself, i. e., an automorphism.
- By normality, every $\sigma \in \mathrm{Aut}(\overline{F}/F)$ leaves K invariant, and so restricts to an automorphism of K. □

§8. The Galois Correspondence

Theorem 7: The Main Theorem of Galois Theory. — *Let $\mathbf{Q} \leqslant K$ be a finite, normal extension. There is a correspondence between groups and fields, called the* ***Galois correspondence****, depicted as follows:*

$$\left[\begin{array}{c}\textit{Intermediate fields}\\ \mathbf{Q}\leqslant F\leqslant K\end{array}\right] \underset{\mathrm{Fix}\, G \hookleftarrow G}{\overset{F\mapsto \mathrm{Aut}(K/F)}{\rightleftarrows}} \left[\begin{array}{c}\textit{Intermediate groups}\\ \mathrm{Aut}(K/\mathbf{Q})\geqslant G\geqslant\{\iota\}=\mathrm{Aut}(K/K)\end{array}\right]$$

It has the following properties:

1. *The Galois correspondence is a bijection:*

$$\mathrm{Fix}\,\mathrm{Aut}(K/F) = F \qquad \textit{and} \qquad \mathrm{Aut}(K/\mathrm{Fix}\, G) = G.$$

2. *The Galois correspondence reverses order: If the fields F and E correspond to the groups G and H, respectively, then:*

$$F \leqslant E \qquad \textit{if and only if} \qquad G \geqslant H.$$

   Hence the group lattice is the field lattice turned upside-down.

3. *The bottom field $\mathbf{Q}$ corresponds to the full automorphism group* $\mathrm{Aut}(K/\mathbf{Q})$. *The top field K corresponds to the trivial subgroup* $\mathrm{Aut}(K/K) = \{\iota\}$.

4. $[K : F] = |\mathrm{Aut}(K/F)|$.

5. $[F : \mathbf{Q}] = (\mathrm{Aut}(K/\mathbf{Q}) : \mathrm{Aut}(K/F))$.

6. *$F \geqslant \mathbf{Q}$ is a normal field extension if and only if* $\mathrm{Aut}(K/F)$ *is a normal subgroup of* $\mathrm{Aut}(K/\mathbf{Q})$.

7. *When this is the case, there is an isomorphism of groups:*

$$\mathrm{Aut}(F/\mathbf{Q}) \cong \mathrm{Aut}(K/\mathbf{Q})/\mathrm{Aut}(K/F).$$

Proof.

1. The first statement follows from the fact that K is a normal extension also of F.

   As to the second statement, it is clear that $G \leqslant \mathrm{Aut}(K/\operatorname{Fix} G)$. Since the extension $K \geqslant \operatorname{Fix} G$ is finite, it is simple — this follows from the Primitive Element Theorem. Find α such that $K = (\operatorname{Fix} G)(\alpha)$ and let $G = \{\sigma_1, \ldots, \sigma_m\}$.

   Consider the polynomial

$$f(x) = (x - \sigma_1(\alpha)) \cdots (x - \sigma_m(\alpha)).$$

   For simplicity, take the special case $m = 2$, so that

$$f(x) = (x - \sigma_1(\alpha))(x - \sigma_2(\alpha)) = x^2 - (\sigma_1(\alpha) + \sigma_2(\alpha))x + \sigma_1(\alpha)\sigma_2(\alpha).$$

   The co-efficients belong to $\operatorname{Fix} G$, since they are invariant under the action of G. This is because, for a finite group $G = \{\sigma_1, \ldots, \sigma_m\}$, one has

$$\{\sigma_j\sigma_1, \ldots, \sigma_j\sigma_m\} = \{\sigma_1, \ldots, \sigma_m\}.$$

   For example, in the case $m = 2$:

$$\sigma_j(\sigma_1(\alpha) + \sigma_2(\alpha)) = \sigma_j\sigma_1(\alpha) + \sigma_j\sigma_2(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha)$$

   and

$$\sigma_j(\sigma_1(\alpha)\sigma_2(\alpha)) = \sigma_j\sigma_1(\alpha) \cdot \sigma_j\sigma_2(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha)$$

   Moreover, α is a zero of f, since one $\sigma_j = 1$, and the corresponding factor becomes

$$\alpha - \sigma_j(\alpha) = 0.$$

   It follows that α is algebraic of degree at most m over $\operatorname{Fix} G$, and so

$$\begin{aligned} |\mathrm{Aut}(K/\operatorname{Fix} G)| &= [K : \operatorname{Fix} G] = [(\operatorname{Fix} G)(\alpha) : \operatorname{Fix} G] \\ &= \deg_{\operatorname{Fix} G} \alpha \leqslant m = |G|. \end{aligned}$$

   Consequently, $\mathrm{Aut}(K/\operatorname{Fix} G) = G$.

2. If $F \leqslant E$, then all those automorphisms fixing E will of course also fix the subfield F, and so $\mathrm{Aut}(K/E) \leqslant \mathrm{Aut}(K/F)$.

   Conversely, if $G \geqslant H$, then those elements left fixed by G will also be left unperturbed by the subgroup H; hence $\mathrm{Fix}\, G \leqslant \mathrm{Fix}\, H$.

3. Special case of Item 1.

4. This follows from the fact that the extension $K \geqslant F$ is normal.

5. Since $K \geqslant F, \mathbf{Q}$ are both normal, Item 4 (or the definition of normality) shews that

$$[K : F] = |\mathrm{Aut}(K/F)| \quad \text{and} \quad [K : \mathbf{Q}] = |\mathrm{Aut}(K/\mathbf{Q})|.$$

   The Tower Law then gives:

$$[F : \mathbf{Q}] = \frac{[K : \mathbf{Q}]}{[K : F]} = \frac{|\mathrm{Aut}(K/\mathbf{Q})|}{|\mathrm{Aut}(K/F)|} = (\mathrm{Aut}(K/\mathbf{Q}) : \mathrm{Aut}(K/F)).$$

6. $F \geqslant \mathbf{Q}$ is normal if and only if all automorphisms of $\overline{\mathbf{Q}}$, fixing $\mathbf{Q}$, leave F set-wise invariant. By Theorem 6, this is true if and only if all automorphisms of K, fixing $\mathbf{Q}$, leave F set-wise invariant. We then arrive at the following chain of logical equivalences:

$$\begin{aligned}
&\forall \sigma \in \mathrm{Aut}(K/\mathbf{Q}) : \sigma(F) = F \\
&\leftrightarrow\ \forall \sigma \in \mathrm{Aut}(K/\mathbf{Q}),\ \alpha \in F : \sigma(\alpha) \in F = \mathrm{Fix}\, \mathrm{Aut}(K/F) \\
&\leftrightarrow\ \forall \sigma \in \mathrm{Aut}(K/\mathbf{Q}),\ \alpha \in F,\ \tau \in \mathrm{Aut}(K/F) : \tau\sigma(\alpha) = \sigma(\alpha) \\
&\leftrightarrow\ \forall \sigma \in \mathrm{Aut}(K/\mathbf{Q}),\ \alpha \in F,\ \tau \in \mathrm{Aut}(K/F) : \sigma^{-1}\tau\sigma(\alpha) = \alpha \\
&\leftrightarrow\ \forall \sigma \in \mathrm{Aut}(K/\mathbf{Q}),\ \tau \in \mathrm{Aut}(K/F) : \sigma^{-1}\tau\sigma \in \mathrm{Aut}(K/F) \\
&\leftrightarrow\ \mathrm{Aut}(K/F) \trianglelefteq \mathrm{Aut}(K/\mathbf{Q}),
\end{aligned}$$

   concluding the proof.

7. Define an homomorphism

$$\xi\colon\ \mathrm{Aut}(K/\mathbf{Q}) \to \mathrm{Aut}(F/\mathbf{Q}), \quad \sigma \mapsto \sigma\big|_F.$$

   It is onto because of Theorem 6, and the kernel is simply $\mathrm{Aut}(K/F)$. By the Fundamental Homomorphism Theorem,

$$\mathrm{Aut}(K/\mathbf{Q})/\mathrm{Aut}(K/F) = \mathrm{Aut}(K/\mathbf{Q})/\mathrm{Ker}\, \varphi \cong \mathrm{Im}\, \varphi = \mathrm{Aut}(F/\mathbf{Q}).$$

□

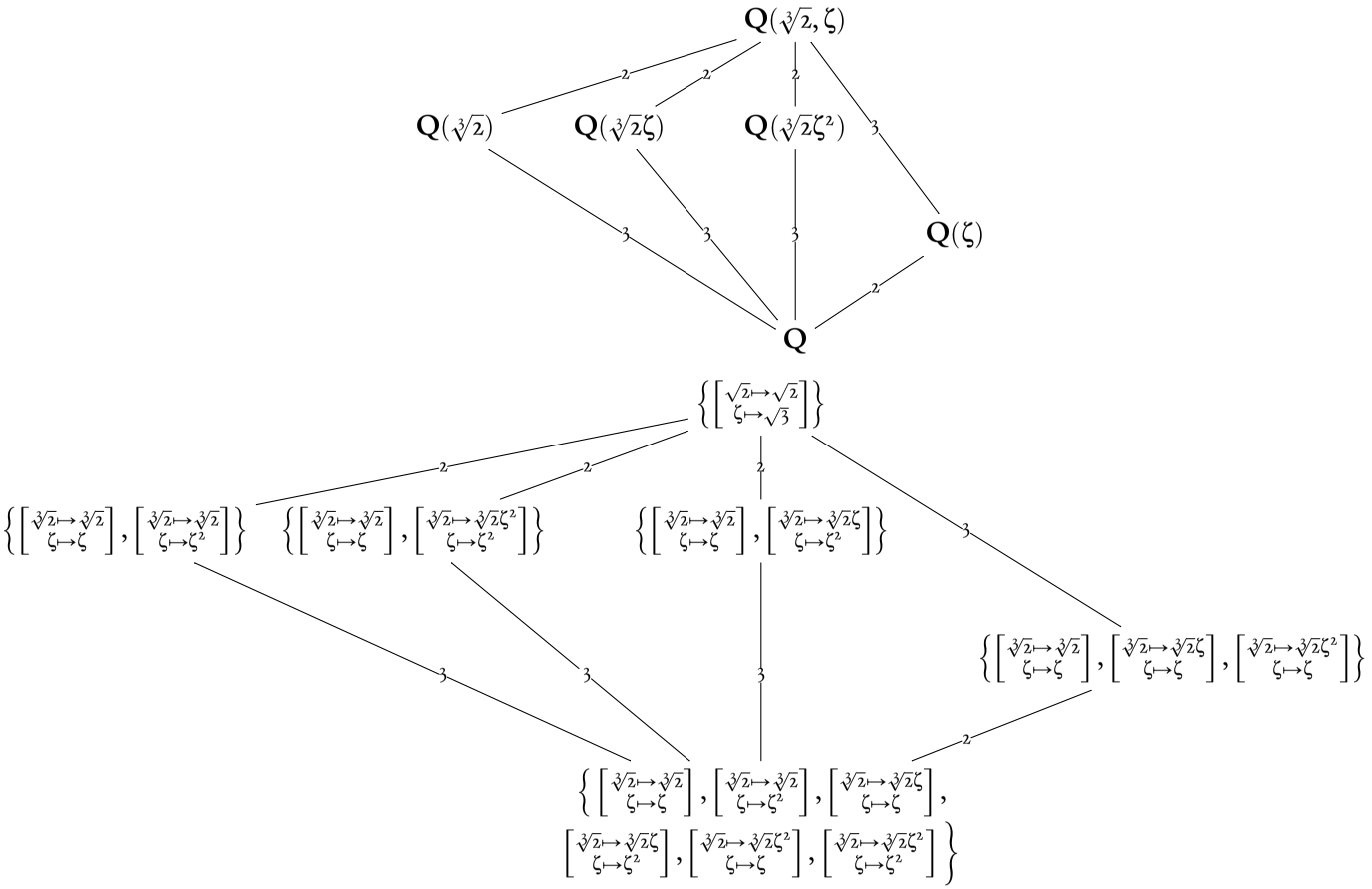


Figure 2: Galois Correspondence for the Field Extension $\mathbf{Q} \leqslant \mathbf{Q}(\sqrt[3]{2},\zeta)$.

Example 12. — Figure 2 displays the Galois correspondence for the field extension $\mathbf{Q} \leqslant \mathbf{Q}(\sqrt[3]{2}, \zeta)$, which is normal, being the splitting field of $x^3 - 2$. Once the full Galois group $\mathrm{Aut}(\mathbf{Q}(\sqrt[3]{2}, \zeta)/\mathbf{Q}) \cong S_3$ is known, one proceeds to discover the intermediate fields through their corresponding subgroups of S_3. By the Main Theorem, *all* intermediate fields arise in this way. Observe that this transforms a potentially infinite problem into a *finite* one.

The reader will perceive the little numerals with which the diagram has been decorated. For field extensions, they indicate the respective *degrees*; for group extensions, they specify the *index* of the subgroups in their respective supergroups. That corresponding figures be equal is in concordance with Items 4 and 5 of the Main Theorem.

There is one further point we wish to dwell upon. The only normal subgroup of S_3 is, it will be recalled, the three-element subgroup A_3. By Item 6 of the Main Theorem, this corresponds to the normal field extension $\mathbf{Q} \leqslant \mathbf{Q}(\zeta)$. By Item 7, an isomorphism will then be expected:

$$\mathrm{Aut}(\mathbf{Q}(\zeta)/\mathbf{Q}) \cong \mathrm{Aut}(\mathbf{Q}(\sqrt[3]{2}, \zeta)/\mathbf{Q})/\mathrm{Aut}(\mathbf{Q}(\sqrt[3]{2}, \zeta)/\mathbf{Q}(\zeta)) \cong S_3/A_3 \cong \mathbf{Z}_2.$$

△

§9. Solution by Radicals

The great triumph of Galois Theory is its ability to successfully demonstrate the impossibility of solving algebraical equations beyond the quartic in terms of radicals. In order to acquire a feeling for what this means, let us look at a few concrete examples.

Example 13. — The equation $x^2 + px + q = 0$ has the solution

$$x = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}.$$

Now, let us assume the co-efficients p and q to be rational. The roots are not necessarily so, but will live in what is called a *quadratic extension* of the co-efficient field, namely

$$\mathbf{Q}\left(\sqrt{\frac{p^2}{4} - q}\right).$$

This field is obtained from $\mathbf{Q}$ after adjoining (at most) a single element, the square root of a rational number. (It is conceivable that this element is indeed rational, in which case the field extension is, of course, trivial.)

Hence, the fact that both solutions are expressible by means of the four arithmetic operations, coupled with a single root extraction, may, in the language of Field Theory, be phrased: *Given a quadratic equation, there exists an extension of the base field, obtained by adjoining a square root, containing both solutions.* △

Example 14. — Our old friend, the cubical equation $x^3 - 2 = 0$, has the solutions

$$x_1 = \sqrt[3]{2}, \quad x_2 = \sqrt[3]{2}\zeta, \quad x_3 = \sqrt[3]{2}\zeta^2,$$

with $\zeta = \frac{1}{2} + \frac{1}{2}\sqrt{3}i$, as always, denoting a third root of unity. These are all contained in the top field of the tower

$$\mathbf{Q} \leqslant \mathbf{Q}(\sqrt[3]{2}) \leqslant \mathbf{Q}(\sqrt[3]{2}, \sqrt{3}i).$$

Once again, *each new field has been concocted from the preceding one through the adjunction of a single square or cube root.* △

Illuminated by these insights, we formally define what it means for a polynomial to be soluble in radicals.

Definition 7. — Suppose there exists a tower of fields

$$F = E_0 \leqslant E_1 \leqslant \cdots \leqslant E_m = E$$

with the following property: Each $E_k = E_{k-1}(\alpha_k)$ for some element α_k, a (positive) power of which belongs to E_{k-1}. Then $F \leqslant E$ is called a **radical extension**.

Definition 8. — The equation $f(x) = 0$, where $f(x) \in F[x]$, is **soluble in radicals** if the solutions are all contained in a radical extension E of F (E will thus contain the splitting field of $f(x)$).

Definition 9. — Let $f(x)$ be a rational polynomial. Its **Galois group** is the group $\mathrm{Aut}(K/\mathbf{Q})$, where K is the splitting field of $f(x)$.

Example 15. — In the preceding definition we find associated, to each polynomial, a whole Galois Correspondence of intermediate fields and automorphism groups. For instance, Figure 1 displays the Galois Correspondence for the polynomial $(x^2 - 2)(x^2 - 3)$, and Figure 2 that of $x^3 - 2$. △

Theorem 8. — *A rational polynomial equation is soluble in radicals if and only if its Galois group is soluble.*

Proof. We shall not endeavour a complete proof, but content ourselves with a vague indication of why the result is true. Consider a radical extension $E \leqslant E(\alpha)$, where $\alpha^n \in E$. Assuming that the bottom field E contains all n'th roots of unity, denoted by $1, \zeta, \ldots, \zeta^{n-1}$, we shall shew that the automorphism group $\mathrm{Aut}(E(\alpha)/E)$ is *cyclic*.

This simplification is of course crude in the extreme, and by no means sufficient to verify the general result of the theorem. It does, however, bespeak that *radical field extensions*, under the Galois Correspondence, give rise to *cyclic factor groups* — which would hint at a soluble group.

The minimal polynomial of α over E divides $x^n - \alpha^n$. This implies $\sigma(\alpha) = \zeta^q\alpha$ for some $q \in \mathbf{Z}$. We may thus define

$$\mu\colon\ \mathrm{Aut}(E(\alpha)/E) \to \mathbf{Z}_n$$

by letting

$$\mu(\sigma) = q \ \leftrightarrow\ \sigma(\alpha) = \zeta^q\alpha.$$

We now shew μ has the homomorphism property. Suppose $\tau(\alpha) = \zeta^p\alpha$, so that $\mu(\tau) = p$. The root of unity $\zeta^p \in E$ and will remain fixed by σ, whence

$$\sigma(\tau(\alpha)) = \sigma(\zeta^p\alpha) = \sigma(\zeta^p)\sigma(\alpha) = \zeta^p\zeta^q\alpha.$$

Consequently,

$$\mu(\sigma\tau) = p + q = \mu(\sigma) + \mu(\tau),$$

and μ is an homomorphism.

Since $\mathrm{Ker}\,\mu = \{1\}$, it is one-to-one, and so provides an embedding of $\mathrm{Aut}(E(\alpha)/E)$ into $\mathbf{Z}_n$. Hence the group is cyclic, as desired. □

Theorem 9: Abel's Impossibility Theorem. — *There exist algebraical equations of any degree beyond the quartic which are insoluble in radicals.*

Proof. The argument runs as follows:

1. Shew A_n is a simple group when $n \geqslant 5$.

2. The ramification is that S_n is insoluble when $n \geqslant 5$. For it has a composition series

   $$\{1\} \trianglelefteq A_n \trianglelefteq S_n,$$

   with simple composition factors $A_n/\{1\} \cong A_n$ and $S_n/A_n \cong \mathbf{Z}_2$. Since A_n is not abelian, the group S_n is not soluble.

3. The hard part consists in exhibiting a polynomial $f(x)$ of degree n having Galois group S_n. Referring to Theorem 8, the equation $f(x) = 0$ will then be insoluble in radicals. □

One must be careful not to misconstrue the statement of the Impossibility Theorem. It does *not* state that quintical equations *never* be soluble. For instance, the equations $x^5 = 0$ and $x^5 = 1$ are both perfectly soluble in radicals.

What it *does* state, is that the quintic is insoluble *in general*, which is to say that there *exist* quintics whose solutions cannot be expressed in radicals. As a concrete example, one may proffer the inconspicuous

$$x^5 - x - 1 = 0,$$

which has Galois group precisely S_5. Since there even exist *particular* equations whose roots cannot be expressed in radicals, there is, *a fortiori*, no closed formula calculating the roots of a *general* quintic in terms of its co-efficients.

As a last point, we remark that "most" equations of degree n have Galois group S_n, and so "most" quintics are insoluble in radicals.