# CHAPTER X

## Automorphisms and linear maps of polynomial equations

### 10.1. Introduction.

The purpose of this chapter is to look at the theory of group automorphisms introduced by E. Artin [Ar59], the theory of ring automorphisms provided in the account by Birkhoff and Mac Lane [BM69], and of linear maps, giving an explanation of the behaviour of the solutions of polynomial equations for complex variables and coefficients, and if available, matrices with matrix coefficients. Our proofs are in direct conflict with the universality of the Galois group model assumed by some authors.

Our original intention was to introduce Galois theory, but our point of view is now that this theory is defective. Galois theory claimed to give necessary conditions derived by Ruffini, Galois, Jordan, Hölder and E. Artin for the solvability of complex polynomial equations by radicals, with the sufficiency of these conditions provided by Schreier. It has been developed to a high degree of abstraction including the theories of Jordan-Hölder series and Galois connections. This approach was combined with a theory on the properties of root generators viewed collectively to provide a solution set for possible formulas. These aspects are now put in context to prove they do not provide the correct model for the solution of such equations.

We insist that any direct kind of Galois theory replacement ought to be a theory of algorithms and not states. A full theory is deferred until chapter XI, where the unsolvability of the general quintic and higher degree polynomial equations by radicals and their solution by convergent approximation methods can be found.

We firstly describe the allowable operations within the complex number field, being addition and multiplication by complex numbers and complex conjugation.

After defining ring automorphisms, we develop their concrete representation and then show some of their properties. We show that ring automorphisms are linear reflections, they are not linear transformations except in a trivial case, they are involutions of roots, that is, the application of a ring automorphism twice is the identity transformation, and that the ring automorphism of a root is another root, but when the same automorphism is applied to a different root not equal to these two, in the general case it does not leave the different root fixed. We introduce the idea of discriminants, which can be incorporated within the ring automorphism theory. We provide a geometric picture of the application of automorphisms as rigid transformations of the roots.

We show that in general ring automorphisms, which attach to specific roots, are not described by permutations on roots. From this it follows that ring automorphisms do not bijectively describe the Galois group theory on roots, since multiplicative inner group automorphisms between roots and their images are not in general inner ring root automorphisms, which include addition. The idea of a normal extension, describing the insertion of a new root to a polynomial by an inner group automorphism leaving other roots fixed does not relate directly to polynomial solvability. When a permutation of roots occurs, it is relevant whether or not the remaining roots are fixed. We show that operations on ring automorphisms can be extended to operations available in the same way to multiplicative linear representations. As we will see, however, ring automorphism theory does not always apply to the solution of

complex polynomial equations. For instance, we have seen that the existence of dependent roots can lead to solvable equations violating the Galois model on independent symbols.

Finally, we discuss ring automorphisms for intricate matrix polynomials.

In chapter XI we employ the ideas we have introduced on linear transformations and as an exercise for polynomial transformations to look at the solution of polynomial equations, and show Galois solvability restrictions apply to the case of killing central terms of a polynomial in additive format. This case is not the most general. We now formulate the *unsolvability theorem*, proved in chapter XI, that restrictions apply to polynomial solvability by radicals in the general case.

## 10.2. Allowable complex operations.

The allowable operations on complex roots in a field we will consider are addition, which displaces a root u + iv by a + ib to form (u + a) + i(v + b), subtraction, which can be considered as addition of the additive inverse (-a) + i(-b), multiplication for which

$$(u + iv)(c + id) = (uc – vd) + i(ud + vc),$$

division by a nonzero complex number as multiplication by the multiplicative inverse

$$(c – id)/(c^2 + d^2),$$

where of course, division is always defined for zero algebras, and complex conjugation

$$u + iv \rightarrow u – iv.$$

Complex conjugation is an involution: applied twice it is the identity transformation

$$u + iv \rightarrow u + iv.$$

We can also consider multiplication using complex polar coordinates $u + iv = \rho e^{i\theta}$, where we have used the Euler relation $e^{i\theta} = \cos\theta + i\sin\theta$.

A particular type of transformation applies to rigid mappings, where there is no change of the norm, $\rho^2$.

## 10.3. Polynomial rings.

The theorems that we wish to develop concern the solutions of polynomial equations, and polynomials generate examples of rings.

**Definition 10.3.1**. *A ring is a field, except multiplication may be noncommutative and it may not have division.*

Fields are described in chapter III, section 4, by rules for addition and multiplication. Division by zero is not defined and is excluded for fields, because $(1 \times 0) = (n \times 0)$, so dividing by zero is not unique.

Consider a finite commutative polynomial in additive format

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0. \qquad (1)$$

**Definition 10.3.2**. *If a number,* c, *can be represented by* f(x) = 0 *in* (1), *where the coefficients* $a_r$ *are integers and* x = c, *it is called algebraic, otherwise it is called transcendental.*

So the roots, $u_1$, $u_2$, … $u_s$ of a polynomial equation may be partitioned into two equivalence classes: those which are algebraic, and those which are transcendental. By the results of chapter VII, these may be encoded in the multiplicative form of a polynomial equation

$$(x - u_1)(x - u_2) \ldots (x - u_s) = 0. \qquad (2)$$

Equation (1) looks very like a finite vector space with vectors $x^n$, $x^{n-1}$, … x, $x^0$, and satisfies the axioms of a vector space. The ideas of linear dependence and independence can be applied to such a polynomial.

When f(x) = 0 and the coefficients $a_r$ belong to a field, so they are algebraic or transcendental, the values of x for which this equation holds are called the zeros of the polynomial, or the roots of the polynomial equation. The vectors $a_nx^n$, $a_{n-1}x^{n-1}$, … $a_1x$, $a_0x^0$ are then linearly dependent, by definition.

When $a_n = 1$ in equation (1) the polynomial is called *monic*. The commutative polynomials of non-negative degree generate a ring $\mathbb{P}$ by addition, subtraction and multiplication. These polynomials are members of $\mathbb{P}$. Not all divisions by polynomials of non-negative degree give a product of polynomials with zero remainder, the interpretation being that there is no complete division, so the polynomial ring $\mathbb{P}$ does not form a field.

We note that this is the case only under the rules we have provided for it. If we were to consider polynomials as in (1) under the condition that terms of arbitrary finite integer degree – positive, negative or zero – are allowed, then finite division is indeed possible. Such polynomials where $(x + a)^{-n}$ is allowed form a field.

A type of Euclidean algorithm for division with remainder also holds. Consider the division

$$\frac{(x-2)(x-1)}{(x-3)} = \frac{x^2 - 3x + 2}{(x-3)} = x + \frac{2}{(x-3)},$$

so we could say

$$x^2 - 3x + 2 = 2 \pmod{(x-3)}. \qquad (2)$$

Multiplication can be formed using a polynomial congruence class, say (x – 3), as in (2), so we keep dividing by, say, (x – 3) until we get a remainder, which could be zero, of degree less than (x – 3).

## 10.4. Ring automorphisms.

**Example 10.4.1**. When we take the complex conjugate of a complex number (a + ic), then we are applying a map $a + ic \rightarrow S(a + ic) = a - ic$. This preserves addition

$$\begin{aligned} S(a + ic + b + id) &= a - ic + b - id \\ &= S(a + ic) + S(b + id) \end{aligned}$$

and also preserves multiplication

$$\begin{aligned} S[(a + ic)(b + id)] &= S[(ab - cd) + i(ad + bc)] \\ &= (ab - cd) - i(ad + bc) \\ &= (a - ic)(b - id) \\ &= S(a + ic)S(b + id). \end{aligned}$$

It is an example of a ring automorphism.

**Definition 10.4.2**. *A ring automorphism* T *of a polynomial is a bijective mapping of its roots*, a, b: a $\leftrightarrow$ T(a) *so that sums and products are preserved*

$$T(a + b) = T(a) + T(b) \quad (1)$$

$$T(ab) = T(a)T(b), \quad (2)$$

(*the bijection implies* T(a) = T(0) *if and only if* a = 0). (3)

**Example 10.4.3**. We see from the definition that the identity map a + ic $\rightarrow$ S′(a + ic) = a + ic is also a ring automorphism.

**Theorem 10.4.4**. *All ring automorphisms of a polynomial ring* $\mathbb{P}$ *form a ring*.

*Proof*. By (1), the sum of two ring automorphisms is also a ring automorphism, and the zero element of the automorphism ring is T(0), since

$$T(0 + 0) = T(0) + T(0),$$

and from the properties of a ring, negative ring automorphisms exist.

From (2) the product of two ring automorphisms is a ring automorphism, where the identity is

$$T(1) = T(1)T(1).$$

That the distributive laws hold follows from the corresponding statements for a ring:

$$a(b + c) = ab + ac,$$

so

$$\begin{aligned} T(a(b + c)) &= T(a)T(b + c) \\ &= T(ab) + T(ac) \\ &= T(a)T(b) + T(a)T(c). \square \end{aligned}$$

**Remark 10.4.5**. If T could act on inverse elements, not generally existing in a polynomial, then inverse ring automorphisms would be present and these would form a field:

$$\begin{aligned} T(1) &= T(a)T(a^{-1}) \\ &= T(a)[T(a)]^{-1}. \end{aligned}$$

**Theorem 10.4.6**. *If two roots* $u_1$ *and* $u_2$ *differ, then so too do their ring automorphisms.*

*Proof*. If $u_1 \neq u_2$ then $(u_1 - u_2) \neq (u_1 - u_1) = 0$, so from (3)

$$T(u_1) - T(u_2) \neq T(0) = 0. \square$$

**Theorem 10.4.7**. *If* u *is a root of a polynomial equation in* x, *so is* T(u).

*Proof*. If $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$, then x is a variable and T applies to it, whilst $a_r$ is a complex coefficient and we will assume in this chapter can be chosen fixed with $T(a_r) = a_r$, so

$$\begin{aligned} T(0) &= 0 \\ &= T(u^n + a_{n-1}u^{n-1} + \ldots + a_0) \\ &= T(u)^n + a_{n-1}T(u)^{n-1} + \ldots + a_1T(u) + a_0. \square \end{aligned}$$

## 10.5. All ring automorphism models are linear reflections.

If firstly we consider linear ring automorphisms, for a linear map

$$U(a + ic) \rightarrow ga + ihc + m,$$

then for this to be a ring automorphism, the definition of U implies

$$U(a + ic) + U(b + id) = U((a + b) + i(c + d)) + m, \quad (1)$$

so the additive condition for a ring automorphism, 10.4.(1), gives

$$m = 0. \quad (2)$$

Also, from equation 10.4.(2) the multiplicative ring automorphism

$$(ga + ihc)(gb + ihd) = g(ab – cd) + ih(cb + ad)$$

thus

$$g^2ab – h^2cd = g(ab – cd) \quad (3)$$

and

$$g(cb + ad) = cb + ad, \quad (4)$$

so that g = 1, which implies from (3) that $h^2 = 1$, that is, $h = \pm 1$. □

In general, if a polynomial ring automorphism were of the form

$$U'(a + ic) = \sum_{j+k=0}^{r} g_{jk}a^j(ic)^k, \quad (5)$$

the definition of U′ and 10.4.(1), imply for the same reasons as equation (2) that

$$g_{00} = 0, \quad (6)$$

thus the summation can start from 1

$$U'(a + ic) = \sum_{j+k=1}^{r} g_{jk}a^j(ic)^k. \quad (7)$$

From the additive ring automorphism equation 10.4.(1)

$$U'(2a + i2c) = 2U'(a + ic), \quad (8)$$

so

$$\sum_{j+k=1}^{r} g_{jk}(2a)^j(i2c)^k = 2\sum_{j+k=1}^{r} g_{jk}a^j(ic)^k, \quad (9)$$

and since this holds for arbitrary a and c, if we assume (9) for r, then for r + 1

$$\sum_{j+k=r+1} g_{jk}(2a)^j(i2c)^k = \sum_{j+k=r+1} 2^{r+1}\, a^j(ic)^k$$

$$= 2\sum_{j+k=r+1} g_{jk}a^j(ic)^k,$$

$$\sum_{j+k=r+1} g_{jk}(2^{r+1} - 2)\, a^j(ic)^k = 0. \quad (10)$$

If $g_{jk}$ does not depend on a or c, this means r + 1 = 1, which is the linear automorphism already encountered. □

## 10.6. Ring automorphisms are multiple.

We have seen in the previous section that a ring automorphism is of the form

$$U(a + ic) = a + ihc, \quad (1)$$

where $h = \pm 1$. Therefore defining $U^2$ by

$$U^2(a + ic) = U[U(a + ic)]$$

$$= U[a + ihc]$$

$$= a + ic, \quad (2)$$

we find that ring automorphisms are involutions; $U^2$ is the identity. □

Since theorem 10.4.7 shows that if u is a root then so is the ring automorphism T(u), this only swaps roots, since $T^2$ is the identity. As we will show in section 9, in general there must be ring automorphisms with many instances.

We can introduce an equivalence class of automorphisms by defining the maps

$$a \to e + if$$

$$c \to s + it$$

so that where by implication we had previously assumed a and c real, these are now complex.

Thus we can form, say, continuous maps

$$a + ic \to (e - t) + i(s + f)$$

We can now treat the automorphism U(a + ic) as the automorphism

$$U''[(e - t) + i(s + f)] = (e - t) + ih(s + f), \quad (3)$$

where U and U″ are identical if f = 0 and t = 0, and are defined distinct otherwise.

We can put U ≡ U″ in the same equivalence class if there is a continuous map with end points U = [e, is] and U″ = [-t, if]. □

## 10.7. Discriminants and antidiscriminants. [Wikipedia]

For the general polynomial

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0, \quad (1)$$

the discriminant, denoted by Δ, is given in terms of the roots by

$$\Delta = a_n^{2n-2} \prod_{j<k} (u_j - u_k)^2$$
$$= (-1)^{\frac{n(n-1)}{2}} a_n^{2n-2} \prod_{j \neq k} (u_j - u_k), \quad (2)$$

where $a_n$ is the leading coefficient and $u_1$, ... $u_n$ are the roots of the polynomial. Δ is the square of the Vandermonde polynomial multiplied by $a_n^{2n-2}$.

Since the discriminant is a symmetric function of its roots, it can also be expressed in terms of the coefficients of the polynomial. These coefficients are what is known as the elementary symmetric polynomials in the roots, given in chapter IX, section 2.

Expressing the discriminant in terms of the roots makes its key property clear, namely that it vanishes if and only if there is a repeated root, but this only enables it to be calculated by factoring the polynomial. Hence a formula in terms of the coefficients allows the nature of the roots to be determined without factoring.

For a, b and c in the quadratic equation

$$ax^2 + bx + c = 0 \quad (3)$$

the discriminant satisfies

$$\Delta = b^2 - 4ac, \quad (4)$$

where if Δ > 0 the quadratic has two real roots, if Δ = 0 it has real duplicate roots, whereas for Δ < 0 both roots of the polynomial equation are complex conjugates.

The discriminant of the cubic polynomial equation

$$ax^3 + bx^2 + cx + d = 0 \quad (5)$$

is

$$\Delta = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd, \quad (6)$$

so that for the monic (a = 1) cubic polynomial without quadratic term, $x^3 + cx + d = 0$, this is

$$\Delta = -4c^3 - 27d^2,$$

and for the quartic

$$ax^4 + bx^3 + cx^2 + dx + e = 0, \quad (7)$$

its discriminant is

$$\Delta = 256a^3e^3 - 192a^2bde^2 - 128a^2c^2e^2 + 144a^2cd^2e - 27a^2d^4 + 144\,ab^2ce^2$$
$$- 6ab^2d^2e - 80abc^2de + 18abcd^3 + 16ac^4e - 4ac^3d^2 - 27b^4e^2 + 18b^3cde$$
$$- 4b^3d^3 - 4b^2c^3e + b^2c^2d^2. \quad (8)$$

In a homogeneous polynomial all nonzero terms have the same degree. The discriminants above are homogenous polynomials in the coefficients, respectively of degree 2, 4 and 6, and are also homogeneous in term of the roots, of respective degrees 2, 6 and 12.

For a polynomial of degree n in real coefficients, we have

- $\Delta > 0$: for some integer k such that $0 \le k \le \frac{n}{4}$, there are 2k pairs of complex conjugate roots and n – 4k real roots, all different.
- $\Delta < 0$: for some integer k such that $0 \le k \le \frac{n-2}{4}$, , there are 2k + 1 pairs of complex conjugate roots and n – 4k – 2 real roots, all different.
- $\Delta = 0$: at least 2 roots coincide, which may be either real or not real. □

For the polynomial (1), if we consider from the coefficients the two row vectors

$$\begin{bmatrix} a_n & a_{n-1} & \dots & a_0 & 0 \\ 0 & a_n & \dots & a_1 & a_0 \end{bmatrix} = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix}, \tag{9}$$

then these are linearly independent, since no nonzero combination of one row with the other will give zero; the first element is $a_n \neq 0$ for the first row and 0 for the second, so if a linear combination $bv_1 + cv_2 = 0$, then b = c = 0, which defines linear independence.

Now consider the formal derivative of (1), which we introduced in chapter VIII section 11, and will write here as

$$f'(x) = na_nx^{n-1} + (n-1)a_{n-1}x^{n-2} + \dots + a_1, \tag{10}$$

where we saw that if f(x) = 0 contains duplicate roots $(x + u)^2$, then f′(x) = 0 contains a copy of one of them. We have seen that if (1) contains the duplicate roots $(x + a)^2$ then (10) contains the root (x + a).

Since (10) has (n – 1) terms at maximum with no $a_0$ value, but where (9) contains $a_0$, for the same reason the vectors

$$\begin{bmatrix} a_n & a_{n-1} & \dots & a_0 & 0 \\ 0 & \dots & na_{n-1} & \dots & a_1 \end{bmatrix} = \begin{bmatrix} v_1 \\ u_1 \end{bmatrix}, \tag{11}$$

are linearly independent when f′(x) has no roots in common with f(x).

Thus the (2n – 1) × (2n – 1) *Sylvester matrix*, shown below for n = 4

$$\begin{bmatrix} a_4 & a_3 & a_2 & a_1 & a_0 & 0 & 0 \\ 0 & a_4 & a_3 & a_2 & a_1 & a_0 & 0 \\ 0 & 0 & a_4 & a_3 & a_2 & a_1 & 0 \\ 0 & 0 & 0 & a_4 & a_3 & a_2 & a_1 \\ 4a_4 & 3a_3 & 2a_2 & a_1 & 0 & 0 & 0 \\ 0 & 4a_4 & 3a_3 & 2a_2 & a_1 & 0 & 0 \\ 0 & 0 & 4a_4 & 3a_3 & 2a_2 & a_1 & 0 \\ 0 & 0 & 0 & 4a_4 & 3a_3 & 2a_2 & a_1 \end{bmatrix}$$

contains linearly independent rows if and only if there are no duplicate roots in f(x).

A determinant is zero if and only if it contains linearly dependent rows. Thus the Sylvester matrix has zero determinant if and only if the polynomial f(x) has duplicate roots. This determinant is known as the *resultant*, denoted by R(f, f′). Since the resultant vanishes if and only if the discriminant is zero, that is, when a term $(u_1 - u_1)$ exists in the discriminant, and the degree of the resultant is one more than the degree of the discriminant, the two differ only by a factor, and the two are equal up to a factor of degree one.

$$\Delta(f) = (-1)^{\frac{1}{2}n(n-1)} \frac{1}{a_n} R(f, f'). \square \qquad (12)$$

A question we raise is does the Sylvester matrix (for duplicates) relate to another matrix (for antiduplicates)? In like manner to the discriminant, which we now denote by $\Delta^+$, we can introduce the antidiscriminant $\Delta^-$, satisfying

$$\Delta^- = a_n^{2n-2} \prod_{j<k} (u_j + u_k)^2,$$
$$= a_n^{2n-2} \prod_{j \neq k} (u_j + u_k),$$

which vanishes if there is any antiduplicate root, $u_j = -u_k$, so

$$\Delta^+\Delta^- = a_n^{4n-4} \prod_{j<k} (u_j^2 - u_k^2)^2,$$

and the symbol

$$\Delta^h = a_n^{2n-2} \prod_{j<k} (u_j + hu_k)^2,$$

vanishes if $u_j + hu_k = 0$. $\square$

## 10.8. Ring automorphisms and linear maps are usually different.

We can prove that a linear substitution of the variable x, called a Tschirnhaus transformation, which we will denote by T′, does not usually form a ring automorphism. Let

$$T': x \rightarrow gx + m,$$

where g and m belong to a field, be a linear transformation.

**Theorem 10.8.1**. T′ *is not a ring automorphism unless* g = 1 *and* m = 0.

*Proof*.

$$T'(x + x) = g(2x) + m \neq T'(x) + T'(x)$$

and

$$T'(xx) = g(x^2) + m \neq (gx + m)(gx + m) = T'(x)T'(x). \square$$

We can extend theorem 10.8.1 to consider the map

$$a + ic \rightarrow g(a + ihc) + m. \square$$

Since a ring automorphism is a symmetry operation, we are justified in calling a Tschirnhaus transformation a symmetry breaking operation.

For monic polynomials, the products factorise as terms like (x – u). Here u is a fixed element of a field and x is a variable, of which there is only one type. Thus if we apply the linear substitution x = y + m with m fixed (this would hold when the transformation is non-linear) we can view this two ways, firstly as a re-labeling of the variable x where the automorphism idea applies, and secondly as a transformation of u, which is no longer a fixed element. In the first interpretation we allow ring automorphisms, and in the second, we do not.

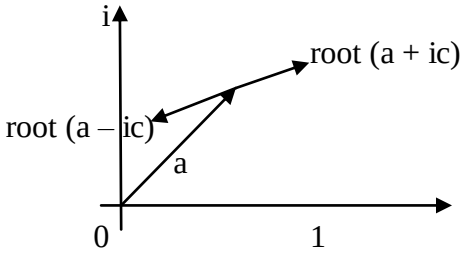
The second way, the transformation $(x - u) \rightarrow (x - u + m)$, makes available a method for solution of polynomial equations. Nevertheless, we have seen in chapter VII, section 8, that solutions of complex polynomials exist, so if the solution is accessible there exists a state as well as a transformation where the roots are detected by an automorphism under re-labeling

of x. Conversely, a solution by radicals is inaccessible if and only if no ring automorphism can describe it.

Since we have found that the Tschirnhaus substitution is a trivial ring automorphism, it follows that polynomial recursion on adding further linear transformations to a polynomial in x so that y = x + h and z = y + h′ does not alter the solvability question if it is determined by automorphisms. Related questions will be studied in chapter XI, where we discuss varieties.

## 10.9. The geometric ring automorphism model.

We have described a ring automorphism as a map U: a + ic $\rightarrow$ a – ic, where a and c are complex in the general case, and $U^2$ is the identity. The pair of roots this describes can be pictured in the Argand diagram

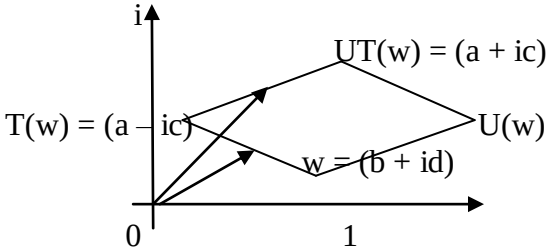



Any pair of roots can be pictured in this way. For two roots in the Argand diagram, draw the connecting lines between them. Then the value a is the complex vector between 0 and the midpoint of the two roots and the value ±ic is the vector from the tip of a to one of the roots.

For three roots, define one of the previous roots, say a – ic, and the new root b + id. Then the construction proceeds as before, this time on the vector [(a + b) + i(d – c)]/2. If T is this new ring automorphism, then we can define for the root w at b + id, the ring automorphism T(w) = a – ic, and then form UT(w) = a + ic.

A ring automorphism T(w) of a root w transfers the root to another root, but does not in general keep roots outside of this pair fixed. If we apply an automorphism U distinct from T to the root T(w), then UT(w) is a ring automorphism, but U acts on T(w) and not w, so that U(w) is not a root automorphism.

Note that, although in general U(w) = U(b + id) is not a root, we can define U(b + id) from the following parallelogram:




Then from the properties of the parallelogram, we have

$$UT(w) = TU(w),$$

and so

$$U^{-1}UT(w) = T(w)$$
$$= U^{-1}TU(w).$$

The ring automorphism $U^{-1}TU$ is known as an inner ring automorphism. □

## 10.10. Isolated and combined ring automorphisms.

**Definition 10.10.1.** An *isolated ring automorphism* acts on a pair of roots

$$(x + a)(x + b) = 0 \quad (1)$$

maintaining their invariance under the automorphism. It is thus equivalent to a permutation of two roots in multiplicative format.

**Definition 10.10.2.** A generally complex symbol has *real* (respectively *imaginary*) *status* if it has the same properties under a ring automorphism as a real (respectively imaginary) symbol.

Writing x as y + iz, and treating a and b as symbols with real status, we have

$$y + iz + a = 0 \quad (2)$$

under the automorophism

$$y + iz \rightarrow y - iz \quad (3)$$

is the same as

$$y - iz + b = 0, \quad (4)$$

that is on adding (2) and (4)

$$y = (a + b)/2 \quad (5)$$

and

$$iz = (a - b)/2. \quad (6)$$

Alternatively, we can treat x as a symbol with real status and introduce the roots

$$(x + c + id)(x + e + if) = 0 \quad (7)$$

so that under an isolated automorphism, this is the same as

$$(x + c - id)(x + e - if) = 0. \quad (8)$$

Another way of putting this is that under the permutation of roots, (7) and (8) imply

$$x + c + id = x + e - if, \quad (9)$$

so that on identifying parts with real and imaginary status

$$(e - c) = i(d + f) = 0. \square \quad (10)$$

For isolated transformations, we now relate these ideas to the theory of varieties. Note that if we can solve (1) we can also solve

$$(x + wa)(x + wb) = 0, \quad (11)$$

and since the two solutions are linear in x, a and b, any root which is valid for (1), say

$$x = -a,$$

is also valid in (11) for

$$x = -wa,$$

and to generalise, for any expression involving a and b combined, say in the function f(a, b) satisfying

$$x = f(a, b)$$

from the analogue of (1), it has the solution

$$x = wf(a, b)$$

under a transformation to the analogue of (11). $\square$

Let us consider the expression (1) under the linear substitutions

$$x = u + p \quad (12)$$

$$a = gu + q \quad (13)$$

$$b = hu + r, \quad (14)$$

then one of the roots is

$$(u + p) + gu + q = 0, \quad (15)$$

satisfying

$$u = -(p + q)/(1 + g). \tag{16}$$

For $p = 0$, $g = h = 1$, (1) becomes

$$u = -q/2 \text{ or } -r/2, \tag{17}$$

since using expressions like (15)

$$(2u + q)(2u + r) = 0.$$

Then as an automorphism (5) and (6) become under

$$u = y + iz, \tag{18}$$

the allocations

$$y = (u + q + u + r)/2 = u + (q + r)/2, \tag{19}$$

$$iz = (u + q - u - r)/2 = (q - r)/2, \tag{20}$$

and this is the form for a linear transformation of an isolated ring automorphism. □

**Definition 10.10.3.** A *combined ring automorphism* is a multiplicative sequence of isolated ring automorphisms, each isolated isomorphism of which is independent of the others.

**Notation 10.10.4.** We use the symbol i for the first imaginary part of a variable occurring in the first isolated ring automorphism in the sequence, and $i'$, $i''$ etc. for later ones.

Thus in our notation

$$i^2 = i'^2 = \ldots \text{ etc.}, = -1 \tag{21}$$

and

$$ii' = -1 \tag{22}$$

for all combinations. This notation allows us to keep track of the independent automorphisms occurring in a combined ring automorphism.

We wish to consider combined automorphisms in a simple case. We will first consider the quartic polynomial equation, and we will compare the same quartic polynomial written in standard form, and expanded out as containing terms in combined format.

Consider the complex polynomial equation

$$x^n + p_{n-1}x^{n-1} + \ldots + p_1x + p_0 = 0, \tag{23}$$

As an example, we will choose $n = 4$ and put (23) in combined automorphism form

$$(z + a + ib)(z + c + id)(z + e + i'f)(z + g + i'h) = 0. \tag{24}$$

On expanding out, the $z^3$ coefficient is

$$(a + c + e + g + i(b + d) + i'(f + h)) = p_3 = 0, \tag{25}$$

where we have chosen to make a Tschirnhaus substitution so that $p_3 = 0$. Thus equating real and imaginary status parts

$$g = -a - c - e \tag{26}$$

$$d = -b \tag{27}$$

$$h = -f. \tag{28}$$

We will resubstitute these values in (24), to obtain

$$(z + a + ib)(z + c - ib)(z + e + i'f)(z - a - c - e - i'f) = 0, \tag{29}$$

so

$$(z^2 + (a + c)z + ac - b^2 + ib(c - a)) \times(z^2 - (a + c)z - e^2 - e(a + c) - f^2 - i'f(a + c + 2e)) = 0, \tag{30}$$

and equation (30) may be split into two similar results, the first being

$$z^2 + (a + c)z + ac - b^2 + ib(c - a) = 0. \tag{31}$$

Now if this remains invariant under the automporphism i → -i on (31), then we obtain

$$z^2 + (a + c)z + ac – b^2 = 0, \quad (32)$$

$$b(c – a) = 0. \quad (33)$$

which gives with c = a or b = 0, the standard quadratic equation in real status symbols, in a form which is solvable for coefficients in (23) under substitutions.

Hence, applying this to a general polynomial of degree 2n, in which a polynomial of degree 2n – 1 can be embedded

**Theorem 10.11.5.** *Transformations available under multiplicative representations of roots are not enhanced by the incorporation of combined ring automorphisms*. □

## 10.11. Group automorphisms and inner automorphisms.

For groups, the isomorphism G → G, $x \leftrightarrow g^{-1}xg = h(x)$ is called an *inner automorphism*, since it satisfies the group automorphism axiom

$$h(xy) = h(x)h(y). \ \square$$

A group automorphism which is not inner is *outer*. As pointed out by J.S. Milne [Mi14], the group automorphism model can be extended to include outer automorphisms.

Concerning the representation of a polynomial in multiplicative format, this is always solvable, the group of permutations of these roots is called the symmetric group, and the polynomial remains solvable on introducing new roots, which can be represented by features of the symmetric group. Thus under this model, a ‘solvable group’ or its transformations does not represent a ‘solvable polynomial’, since they can also be represented by ‘unsolvable groups’. Thus the Galois model of the solvability mapping from groups to polynomials requires justification from elsewhere.

We have seen that ring automorphisms are commutative, and thus in the general case cannot be represented by permutations. Further, the group automorphism idea must extend to that of ring automorphisms, otherwise if addition is irrelevant to the group structure, a polynomial in multiplicative format cannot be transformed to a polynomial in additive format.

We cannot claim in general that if we add the extra distributive axioms

$$a(b + c) = ab + ac$$

to the axioms for a multiplicative group, even if that group describes some of the properties of a polynomial in multiplicative format, then unsolvability criterions derived in that way are unaffected by the introduction of the distributive rules, since there is the possibility that the theory augmented with addition might alter these criterions.

If we say the permutation structure of a group automorphism has nothing to do with addition or multiplication, are we to assume that the roots of a quintic equation permute the formulas expressed with the variable x as each of the roots? Then the permutation of formulas gives no method for obtaining solutions, nor does this change when we consider that a property of the alternating group on five letters is that it has no nontrivial normal subgroups.

**Theorem 10.11.1.** *There exist successive ring automorphisms which do not correspond to any permutation of roots*.

These successive ring automorphisms are not combined ring automorphisms in the sense we have used these terms, since combined automorphisms act on isolated pairs which permute independently of one another, but successive ring automorphisms may not.

*Proof*. Consider four roots, A, B, C and D. Apply a ring automorphism to A and B, so that A becomes B and B becomes A. Now apply a ring automorphism between B and C, then A is displaced in general to a non-root A′. Then applying the same process with D replacing A, then D is displaced to a non-root D′. Apply the ring automorphism to A′ and D′, then all roots are displaced in general to non-roots. □

## 10.12. Solutions of polynomial equations.

The deconstruction of Galois theory, which contains within it a theory of groups based on the permutation of roots, has now taken place in this chapter. This analysis has depended on the theoretical understanding of automorphisms begun by E. Artin [Ar59], and a further account given by Birkhoff and Mac Lane [BM69]. Our point of view is this. Viewed as a theory of groups, Galois theory is correct. Viewed as a theory of rings, in particular as a solvability model for polynomial rings, it fails; we have proved formally that a commutative polynomial equation remains commutative under ring automorphisms, and further that the only instances of such automorphisms are themselves commutative.

This insight is similar to the observation, as we have proved in chapter III, that Wedderburn's little theorem states that all finite division rings are commutative, and thus noncommutative algebra has no part to play in the implementation of such rings.

Galois *representation* theory is used in a number of important areas of mathematics: the proof of Fermat's last theorem, the proof of the Weil conjectures, and in the classification of finite groups, but it can be made independent of the Galois *solvability* theory discussed here.

Features of the various models of solutions by radicals are itemised below.

| | **Variety** | **Ring automorphism** | **Galois** |
|---|---|---|---|
| **Transformation type** | all | ring automorphism<br>(a) isolated<br>(b) combined | group automorphism |
| **Solution method** | (1) Bring-Jerrard comparison<br>(2) killing central terms | ring automorphism | false |
| **Polynomial solvability** | (1) ineffective<br>(2) restricted to degree $\leq 4$ | known for degree 2 | restricted to degree $\leq 4$ |
| **Dependent roots** | incorporated | duplicate roots are identity involutions | defective (inseparable extensions) |
| **Linear transformations** | allowed | usually violated | usually violated |

**Table 10.12.1**. *Theories of complex polynomial equations*.

We will be unable to prove a direct refutation of Galois theory by the solution of equations it deems impossible to construct, but we are able to replace all of noncommutative Galois theory by a commutative theory where unsolvability is based on insufficiency of the number of parameters needed to provide a solution, for instance by killing central terms of a polynomial in additive format. We investigate issues of solvability further in chapter XI, where we show this intuition is in fact correct. The proof of the unsolvability theorem for polynomials using radicals is also obtained and convergent matrix QR algorithms for the solution of real polynomials of arbitrary degree are studied.

## 10.13. Intricate ring automorphisms.

An example of a ring is a matrix ring, which may not be multiplicatively commutative. We restrict discussion to intricate automorphisms.

Let U be an automorphism of the intricate number $a + ib + \alpha c + \phi d$, so that

$$U(a + ib + \alpha c + \phi d) = ga + ihb + \alpha jc + \phi kd + m. \quad (1)$$

We will first consider a limited example, where $a = b = c = d = 1$. The additive nature of the automorphism implies for artbitrary g, h, j and k that $m = 0$.

For multiplication

$$U[(a + ib + \alpha c + \phi d)^2] = U(a + ib + \alpha c + \phi d)U(a + ib + \alpha c + \phi d), \quad (2)$$

so that for the real component of the automorphism

$$g^2 - h^2 + j^2 + k^2 = 2g, \quad (3)$$

and for the imaginary i component

$$hg = h, \quad (4)$$

so $g = 1$, and this is also implied by considering the actual and phantom parts. Thus

$$-h^2 + j^2 + k^2 = 1,$$

or in the more general case

$$-h^2b^2 + j^2c^2 + k^2d^2 = -b^2 + c^2 + d^2,$$

which can only be satisfied for arbitrary b, c and d when

$$h^2 = 1,\ j^2 = 1 \text{ and } k^2 = 1,$$

so

$$h = \pm 1,\ j = \pm 1 \text{ and } k = \pm 1. \quad (5)$$

If we consider the intricate number $p + iq + \alpha r + \phi t$, and the multiplicative automorphism

$$U[(a + ib + \alpha c + \phi d)(p + iq + \alpha r + \phi)t] = U(a + ib + \alpha c + \phi d)U(p + iq + \alpha r + \phi t), \quad (6)$$

then on equating intricate parts, for instance

$$i(hgbp + hgaq + jkct - kjdr) = i(hbp + haq + hct - hdr)$$

so that

$$jk = h, \quad (7)$$

where similar considerations for the actual and phantom parts gives

$$hk = j,$$
$$hj = k,$$

we obtain

$$hjk = 1. \ \square \quad (8)$$

## 10.14. Exercises.

(A) Let $\omega_5$ be the fifth root of unity. Show that the mappings

$\omega_5 \leftrightarrow \omega_5^3$

$\omega_5^2 \leftrightarrow \omega_5^4$

$1 \leftrightarrow 1$

do not collectively form an automorphism.

(B) Show that a complex ring automorphism splits a pair of solutions into a ‘real’ part with the same properties as if it were real, and a ‘complex’ part with the same properties as if it were complex.

Show that a complex polynomial equation can be separated out into ‘real’ and ‘complex’ equations, which we have described as equating real and complex parts, so that there is a solution to a polynomial equation using ring automorphisms if there is a solution equating real and complex parts.

(C) To restate part of chapter IX, section 13, solve the general quadratic equation in additive format by equating to zero the real and imaginary parts of roots expressed in terms of a variable $(x + iy)$.