Galois Theory:
an amateur's account

John Coffey, Cheshire, UK.

2022

Key words: roots of polynomials, solution in radicals, field extension, tower of fields,
splitting field, permutation, automorphism,
Galois group, Galois Correspondence, solvable group,
straight edge and compasses constructions, symmetric polynomials, resolvent

This is my summary of the main ideas and procedures in Galois theory, a branch of algebra which arose from attempts to find formulae which would solve general polynomial equations in one variable, $P(x) = 0$. There is nothing new in this article. My motivation is that I attended a course on this at university many years ago, but never really understood it. The course was given by an enthusiastic but haphazard lecturer who jumped from one topic to another so confusingly that I could not see the mathematical wood for the dense mathematical trees. Some monographs on this are quite turgid and few deal with how to determine the Galois group or how to use knowledge of it to solve a polynomial equation in radicals. This article is my attempt to tell the essentials simply.

A word of warning. Galois theory seems to me to have almost no practical use. Apart from the simple formula for quadratic equations, if you need to know the roots of a polynomial for use in any scientific or engineering calculation, numerical solution to arbitrary precision is most likely to be far better. What the theory does do is answer some deep questions as to why some polynomials have roots which can be expressed in radicals while most do not. It is elegant algebra for those who like elegant algebra.

The article is in four Parts.

1. The first gives some of the history, interesting in itself, plus a heuristic overview of the main ideas behind the theory. Galois theory is at the meeting of field theory and group theory.
2. The second deals with the complementary topics of field extensions and Galois groups, closing with the Galois Correspondence.
3. The third is a partial review of how to find the Galois group of a polynomial without having first to know the algebraic form of its roots, and then how to use this knowledge to solve the given polynomial in radicals where this is possible. This is incomplete.
4. The fourth is an assembly of ten appendices on various detailed aspects of the above topics.

Throughout the text and the appendices I give many examples, but not many proofs. For a rigorous account the reader must look to the standard textbooks and the mathematical literature. I have adopted the further simplification of dealing almost exclusively with polynomials with rational (integer or fractional) coefficients, in the field $\mathbb{Q}$. Most texts deal also with polynomials over finite fields, but that introduces elaborations which are not essential to a basic understanding.

Part I
Ideas which led to Galois theory

1 Brief History

The problem which motivates Galois theory is to find an algorithm or formula which will produce algebraic expressions for all roots of the general polynomial equation in one variable x

$$p(x) = c_n x^n + c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + ... + c_1 x + c_0 = 0 \qquad (1a)$$

where all coefficients c_j are integers in $\mathbb{Z}$. The problem can be restated in terms of fractional (rational) coefficients in $\mathbb{Q}$ by dividing by $c_n \neq 0$ to obtain the monic polynomial (leading coefficient is 1)

$$P(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_1 x + a_0 = 0\ . \qquad (1b)$$

The fundamental theorem of algebra tells us that over the complex numbers $x \in \mathbb{C}$ there are exactly n roots. If $P(x)$ has no rational roots, all its n roots will be distinct. Call these roots $\alpha_j,\ 1 \leq j \leq n$. Finding all roots is equivalent to factorising the polynomial into linear factors only:

$$P(x) = (x-\alpha_1)(x-\alpha_2)....(x-\alpha_{n-1})(x-\alpha_n). \qquad (2)$$

We have here the principal actors in this mathematical drama: the coefficients a_j in the field $\mathbb{Q}$ and the roots α_k. We will be concerned deeply with the interplay between these two sets of numbers. Unless the give polynomial $P(x)$ has roots in $\mathbb{Q}$, its roots will lie in a larger field $\mathbb{S}$ which contains algebraic numbers[1] whose form will be something like $\beta + \sqrt[k]{\gamma}$ where γ might have a similar form, $\delta + \sqrt[m]{\varepsilon}$. The required algorithm must be analytic, expressing the roots as combination of the coefficients using the $+, -, *$ and $\div$ operations together with square, cube and higher roots up to the nth and nested to any depth as may be required. This is called a 'solution in radicals'. There is no resort to numerical search.

The history of this quest is well related in the literature. The ancient civilisations knew how to solve quadratic equations $ax^2 + bx + c = 0$ in radicals. The formula – a solution in square roots familiar to many secondary school students – is

$$\alpha_1 = \frac{-b + \sqrt{b^2 - 4ac}}{2a}, \qquad \alpha_2 = \frac{-b - \sqrt{b^2 - 4ac}}{2a}. \qquad (3a)$$

The formula is derived by the algorithm called 'completing the square' which involves comparing

$$x^2 + \frac{b}{a}x + \frac{c}{a} = x^2 + \frac{b}{a}x + \frac{4ac}{4a^2} \quad \text{with} \quad \left(x + \frac{b}{2a}\right)^2 = x^2 + \frac{b}{a}x + \frac{b^2}{4a^2} \qquad (3b)$$

and my guess is that the ancients used this algorithm rather than the formula. Of course, the ancients would have accepted only positive roots. They thought in terms of whole counting numbers and of the lengths of lines. They knew in effect that the products b^2 and $4ac$ could be understood as the areas of a square and of a rectangle respectively, and that the square root could be extracted as the length of the side of the square with area $b^2 - 4ac$. Appendix 2 shows one construction for finding a square root as a length using only a straight edge and a pair of compasses, and hence of using geometry to solve a quadratic equation which has at least one positive real root.

[1] An algebraic number is a number which is a root of a polynomial equation $P(x) = 0$ whose coefficients are in $\mathbb{Q}$, but which does not factorise over $\mathbb{Q}$: *i.e.* $P(x)$ is irreducible over $\mathbb{Q}$.

Two thousand years later renaissance mathematicians in Italy and France found complicated methods which would solve the general cubic equation in terms of square and cube roots, though there is no corresponding geometrical construction. For example, this is François Viète's formula for the three roots of $x^3 + 2x^2 + 5 = 0$:

$$x \;=\; \tfrac{1}{3}\left\{ \sqrt[3]{\tfrac{1}{2}(-151 + 3\sqrt{2505}\,)} \;+\; \sqrt[3]{\tfrac{1}{2}(-151 - 3\sqrt{2505}\,)} \;-\; 2 \right\}. \qquad (4)$$

The derivation is in Appendix 3. Fairly soon afterwards the quartic equation was solved using a further layer of square roots imposed onto the solution of a related cubic. The scheme in each case was to manipulate the given 4th or 3rd order equation to find a companion equation of one degree lower which must also be satisfied. This lower degree equation could then be solved by a formula which had already been established. Thus the quartic equation implied a complicated cubic, the cubic implied a quadratic, and the quadratic solved by Eq 3. The algorithms found all the roots, real and complex.

Many attempts were then made to find an equivalent formula to crack open the general fifth order equation in terms of 5th roots. Important investigations has been made by Newton and later by Lagrange, but all to no avail. Though some fairly obvious quintic equations such as $x^5 - 3 = 0$ could be solved in radicals (the five roots are $\sqrt[5]{3}$ multiplied by the 5th roots of unity), it seemed that any more general quintic could not. Eventually mathematicians began to suspect that no such formula or equivalent algorithm exists. In the early 19th century Paola Ruffini and Niels Abel separately gave proofs that it is indeed impossible to solve the general quintic. The same applies to polynomials of sixth and higher degree. To be clear, solutions of these higher equations in radicals do not exist; it is not just that an algorithm for finding them does not exist[2]. Finally Evariste Galois, a young hot headed French genius, fired up with romantic jealousy and political zeal, and foolish enough to enter into a duel with pistols which he was most unlikely to win, showed in notes scribbled down before he was shot that the secret of what is solvable in radicals lies in the symmetries of the roots of the polynomial. The year was 1832. To achieve this astounding insight he made major innovations in the embryonic group theory of his day. What a pity he did not have more common sense and self control.

2 Clues and intuitions

We can never know just what was in Galois' mind, except that he was thinking deeply about why some polynomials have roots which can be expressed in radicals while other do not. Finding the roots of $P(x) = 0$ is the same as completely factorising $P(x)$. What properties must the roots have if all the coefficients are simple fractions? Four elementary facts were well understood and may have given Galois the germ of an idea:

1. If the roots can be expressed as radicals – square or higher roots of other combinations of square and higher roots – then their radical terms and factors must cancel when added and multiplied to leave purely rational coefficients. For this to happen the radical parts must be very similar, such as $+\sqrt{2}$ and $-\sqrt{2}$ being the roots of $x^2 - 2$. Indeed, complex roots always occur in conjugate pairs so their imaginary parts cancel.

2. If the numerical values of the roots α_j of a polynomial have been found, direct calculation shows that any fully symmetrical combination of them has an integer or fractional value, never

[2] Later in the 19th century Hermite and others showed that the general quintic can be solved in terms of complicated functions called elliptic modular functions, though hardly anyone would want to do so. In practice solutions are found numerically to almost arbitrary precision. See Appendix 1.

an irrational one. For a quadratic an example of a symmetrical combination is $\alpha_1^2\alpha_2 + \alpha_2^2\alpha_1$ in which both roots have equal status. As a result it does not change value when the indices 1 and 2 are permuted – only the order of writing its terms changes.

3. Some polynomials can be factored in intermediate ways which are less than full linear factorisation in $\mathbb{Q}$. This is most obvious with those quartics which are quadratics in the variable x^2. For instance, $P(x) = x^4 + (2a-n)x^2 + a^2 = (x^2 + a + x\sqrt{n})(x^2 + a - x\sqrt{n})$ for any rational a and n. Here $\sqrt{n}$ or, for $n < 0$, $i\sqrt{|n|}$ has been allowed as a valid term. This hints that the full linear factorisation may be approached in stages by admitting selected non-rational numbers.

4. For any given polynomial some permutations of the roots will leave combinations of the roots, such as $\alpha_1 + \alpha_2$ or $\alpha_1\alpha_3$, unchanged in value whist other permutations will change it. So permutations of the roots fall into two classes – ones which leave such combinations invariant, and ones which change the values. Could the freedom to shuffle roots combined in partially symmetric ways have something to do with their capacity to cancel and fuse into rationals?

To enlarge on these ideas, first the familiar Eq 3a shows that the roots of a quadratic are very alike. Their similarity is the reason why the square root terms cancel under addition and combine in multiplication to leave only rational coefficients. Consider also $x^2 - 2x - 2$ which is irreducible over $\mathbb{Q}$ and has a solution in radicals with roots $1 \pm \sqrt{3}$. Therefore so $x^2 - 2x - 2 = (x - \alpha_1)(x - \alpha_2) = x^2 - (\alpha_1 + \alpha_2) + \alpha_1\alpha_2$. The $\pm\sqrt{3}$ cancel in adding, while in multiplying $(\pm\sqrt{3})^2 = 3$ by which all trace of whether the root was $1 + \sqrt{3}$ or $1 - \sqrt{3}$ has been lost. . Taking this further, if Eq 2 is multiplied out for the case of a 5th degree polynomial, the coefficients are these symmetric combinations of the roots:

$$\begin{array}{ll} \text{of } x^4: & -\alpha_1 - \alpha_2 - \alpha_3 - \alpha_4 - \alpha_5 \\ \text{of } x^3: & \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \ldots + \alpha_2\alpha_3 + \ldots..\alpha_4\alpha_5 \\ \text{of } x^2: & -\alpha_1\alpha_2\alpha_3 - \alpha_1\alpha_2\alpha_4 - \alpha_1\alpha_3\alpha_4 \ldots\ldots - \alpha_3\alpha_4\alpha_5 \\ \text{of } x^1: & \alpha_1\alpha_2\alpha_3\alpha_4 + \alpha_1\alpha_2\alpha_3\alpha_5 + \alpha_1\alpha_2\alpha_4\alpha_5 + \alpha_1\alpha_3\alpha_4\alpha_5 + \alpha_2\alpha_3\alpha_4\alpha_5 \\ \text{of } x^0: & -\alpha_1\alpha_2\alpha_3\alpha_4\alpha_5. \end{array} \qquad (5)$$

Each of these coefficients is called an 'elementary symmetric polynomial' and each evaluates to a rational number. We conclude that there are extremely tight constraints on the possible forms of the roots α to allow all these coefficients to be fractions, through multiple cancellations and fusions of all square, cube and higher roots. The roots have to look very similar for this to happen.

Point 2, on fully symmetrical combinations of roots, emphasises how deep the cancelling properties of the roots goes. Complicated combinations of roots will remain within $\mathbb{Q}$ under permutation of the roots α_j provided these combinations are symmetric in all the roots. Isaac Newton had investigated the elementary symmetric polynomials so it was well known long before Galois that for any polynomial $P(x)$ there is a dual relationship between the roots α_j and the coefficients a_k, such that any symmetrical combination of roots can be transformed into a (generally non-symmetrical) combination of coefficients. The values of the roots does not need to be known for this transformation to be carried out, and an algorithm is given in Appendix 9. This property allows insight into the relations between the roots from the coefficients alone, and is a key to determining a solution to $P(x) = 0$ as explained in Part III.

Turning to Point 3, consider $P(x) = x^4 - 2x^2 + 9$. This can be solved in radicals by writing $P(x) = 0 \;\rightarrow\; (x^2 - 1)^2 = -8$ and its four roots are

$$\alpha_1 = \sqrt{2} + i, \qquad \alpha_2 = \sqrt{2} - i, \qquad \alpha_3 = -\sqrt{2} + i, \qquad \alpha_4 = -\sqrt{2} - i. \qquad (6)$$

Six quadratics can be formed from pairs of these roots:

$(x-\alpha_1)(x-\alpha_2) = x^2-2\sqrt{2}\,x+3, \qquad (x-\alpha_1)(x-\alpha_3) = x^2-2i\,x-3, \qquad (x-\alpha_1)(x-\alpha_4) = x^2-2i\sqrt{2}\,x-1,$

$(x+\alpha_2)(x-\alpha_3) = x^2-2i\sqrt{2}\,x-1, \qquad (x-\alpha_2)(x-\alpha_4) = x^2+2i\,x-3, \qquad (x-\alpha_3)(x-\alpha_4) = x^2+2\sqrt{2}\,x+3.$

These point to three intermediate ways of factorising $P(x)$ into the product of two quadratics:

$(x^2+2\sqrt{2}\,x+3)(x^2-2\sqrt{2}\,x+3), \qquad (x^2+2i\,x-3)(x^2-2i\,x-3), \qquad (x^2+2i\sqrt{2}\,x-1)(x^2-2i\sqrt{2}\,x-1).$

This chimes with the solutions found by Viète and others in the late 16th century (see Appendix 3) in which solution of the cubic requires solution of an associated quadratic, and solution of the quartic requires solutions of a cubic. The lower degree polynomials are nested inside the higher ones.

Consistent with Point 2, direct calculation shows that fully symmetric combinations of all the roots of this same quartic polynomial such as

$$\alpha_1+\alpha_2+\alpha_3+\alpha_4 = 0, \qquad \alpha_1\alpha_2\alpha_3\alpha_4 = 9, \qquad \alpha_1\alpha_2+\alpha_3\alpha_3+\alpha_3\alpha_4+\alpha_4\alpha_1 = 4,$$

$$\alpha_1^2\alpha_2+\alpha_2^2\alpha_1+\alpha_1^2\alpha_3+\alpha_3^2\alpha_1+\alpha_1^2\alpha_4+\alpha_4^2\alpha_1+\alpha_2^2\alpha_3+\alpha_3^2\alpha_2+\alpha_2^2\alpha_4+\alpha_4^2\alpha_2+\alpha_3^2\alpha_4+\alpha_4^2\alpha_3 = 0$$

all evaluate to integers or fractions. Because these symmetrical combinations include *all* the roots, *any* permutation of the roots will leave such combinations unchanged in value, even though the order of the terms will change. However, important structural relations exist amongst pairs of roots and some permutations will leave these unchanged while others will not. This is Point 4 above. Some examples are

$a)\ \alpha_1\alpha_2 = 3, \qquad b)\ \alpha_1+\alpha_4 = 0, \qquad c)\ \alpha_2+\alpha_3 = 0, \qquad d)\ \alpha_1\alpha_3 = -3, \qquad e)\ \alpha_2\alpha_4 = -3.$

If the permutation (12) is applied to the indices, swapping roots 1 and 2, these functions become

$a)\ \alpha_2\alpha_1 = 3, \qquad b)\ \alpha_2+\alpha_4 \neq 0, \qquad c)\ \alpha_1+\alpha_3 \neq 0, \qquad d)\ \alpha_2\alpha_3 \neq -3, \qquad e)\ \alpha_1\alpha_4 \neq -3,$

while the permutation (12)(34) produces

$a)\ \alpha_2\alpha_1 = 3, \qquad b)\ \alpha_2+\alpha_3 = 0, \qquad c)\ \alpha_1+\alpha_4 = 0, \qquad d)\ \alpha_3\alpha_4 = -3, \qquad e)\ \alpha_1\alpha_3 = -3.$

Hence (12)(34) lies within the set of permutations which leave all these combinations unchanged, but (12) does not. Similarly (13)(24) and (14)(23) also lie within the set while (23), (34), (14) and the cyclic (123) and (1234) do not. (12)(34), (13)(24) and (14)(23) together with the identity $I = ()$ form a closed set under concatenation of permutations.

From this jigsaw of clues and intuitions we begin to understand that the ability of solve a general irreducible nth degree monic polynomial $P(x) = x^n + ... + a_0 = 0$ in radicals depends on those particular symmetries of its roots $\alpha_j, 1 \leq j \leq n$ which allow the roots to be shuffled around without changing the values of significant polynomial combinations of 2, 3 or only a few roots: that is, they do not change the structural algebraic relations between pairs, triples, *etc.* of the roots. The structural relations will of course depend on the particular coefficients of $P(x)$. The set of particular permutations which preserve algebraic relations amongst the roots form a group called the Galois group. Thus the set $\{I,\ (12)(34),\ (13)(24),\ (14)(23)\ \}$ under concatenation of permutations form the Galois group of $x^4 - 2x^2 + 9$, and it happens to be the Klein 4-group. Galois theory is about identifying this group for each $P(x)$ then using the power of group theory to infer corresponding relations between the algebraic number fields – such as $\mathbb{Q}$ with i or $\sqrt{2}$ or $i\sqrt{2}$ adjoined – in which the roots lie. If it is possible to advance from one number field to a larger one by adding a new radical (i.e. a square root, cube or higher root) until a field in reached in which all the roots of $P(x)$ are contained, then $P(x)$ can be solved in radicals. If not, no such solution exists.

2.1 Spoiler – unsolvable quintics

Because the mathematical trees in Galois theory are quite dense, I will jump ahead and say in a few everyday words why most quintic and higher order equations cannot be solved in radicals. The answer is that there is not structure of number fields which can be built by adding radicals until all the roots of $P(x)$ lie within it. The answer is as profound as why 17 is a prime number and 18 isn't– they just are.

The two solutions of an irreducible quadratic have the form of rational numbers a, b, combined with the roots α of a degree-2 polynomial, such as $a + b\alpha$ where α might be $\sqrt{2}$, $\sqrt{5}$, etc. Label as K the number field composed of all combinations of $\mathbb{Q}$ and α. The solution of a cubic is achieved by appending to K another root β, where β satisfies an polynomial which is irreducible in K. Label this doubly extended number field as L. At each stage we have to 'spice up' the types of available number to achieve combinations which satisfy the higher order polynomial. The quartic is solved by appending yet a further root γ to the cubic. Can this process continue indefinitely? No. For some quintic equations there is no additional root δ available to lift the solution of a quartic to a quintic. δ with the required properties simply does not exist.

Why not? you ask, along with dozens of clever mathematicians up to Abel and Galois. Galois explained the matter by pointing out that the chain or 'tower' of extended number fields $\mathbb{Q}$, K, L, etc. has an exact counterpart in the hierarchy of subgroups of a group $\mathcal{G}$. $\mathcal{G}$ consists of permutations which shuffle all the roots of the given $P(x)$ without disturbing the numbers in the next smaller field. Thus permuting roots γ in L is done without changing any numbers in K. For many quintic equations their group $\mathcal{G}$ is either the full symmetric group S_5 on 5 items with 120 members, or the alternating group A_5 on 5 items with 60 members. A_5 is the smallest 'simple' group, meaning it has no normal subgroups. The normal subgroups correspond with number fields which contain not just the one appended root γ, say, but all companion roots of γ which satisfy the same polynomial as γ, typically $x^5 = u$, $u \in L$. Normal subgroups have cosets which themselves constitute the compound elements of a factor group. If the factor group is cyclic, the corresponding step from one number field to the next can be made by adjoining a new radical δ. If it is not cyclic or at least albelian, there is no equivalent δ. That is the position with most quintic equations. Only a few quintics have groups $\mathcal{G}$ which are smaller than A_5's 60 elements, and these can be solved in radicals because the required normal subgroups and their cyclic factor groups do exist. This means in turn that radicals δ also exist to step up from a smaller number field. So group theory shines a light on field structure. But to say that A_5 is a simple group is much like saying the certain tyoes of quintic cannot be solved in radicals. Numbers are just made that way.

Much of the rest of this article and its Appendices set this story in more formal and precise terms, but the above précis is the kernel of Galois theory.

Part II
The Galois Correspondence

3 Number fields and field extensions

We need some technical preliminaries. Recall that a field is a structure such as the rationals, $\mathbb{Q}$, consisting of elements over which two binary operations, addition and multiplication, are defined. Under both operations the field elements form abelian groups, meaning that the order of combining any two elements a, b does not affect the result: $a + b = b + a$, and $a * b = b * a$. There is a unique identity element for addition denoted 0. There is also a unique multiplicative identity, 1. There are no 'zero divisors' – non-zero numbers which when multiplied together give a product equivalent to zero in the field[3]. Consequently it is possible to divide any chosen element by any other except 0 and the result will be another element in the same field. In this article, therefore, we will be examining certain types of field related to polynomials. Our interest will be mainly in the infinite field $\mathbb{Q}$ and its extensions, though Galois theory does carry over to finite fields $\mathbb{F}_p$ where the number of elements p is prime or a prime prower p^k. The properties of finite fields are explained in the article of factorising polynomials on my web site *www.mathstudio.co.uk*.

Just as groups have subgroups nested within them, so fields have nested subfields. Conversely a smaller field K can be augmented or 'extended' by incorporating with the base field K an algebraic number α which is irrational in K, then forming every possible sum, multiple, power and quotient of numbers within this enlarged set. The idea is illustrated in Figure 1 which shows four levels of nested field with the rationals $\mathbb{Q}$ as the smallest, embedded in $\mathbb{Q}(\alpha_1)$. Note the notation for the field extension of the rationals by α_1.

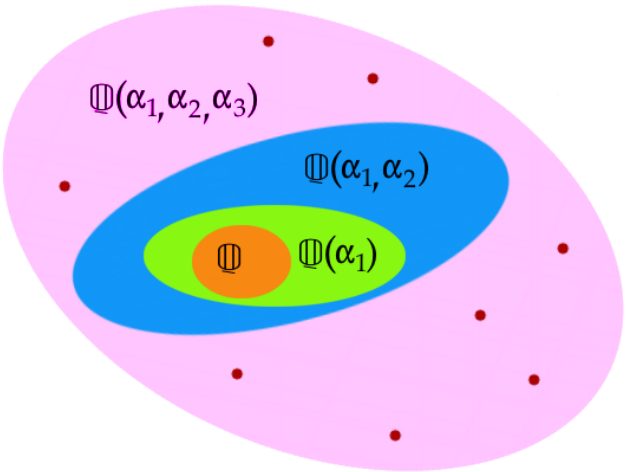

Figure 1: Diagram of field extensions where all roots (red spots) of $P(x)$ are contained in the outer, largest field, here made by adjoining three roots of $P(x)$ to $\mathbb{Q}$.

Any polynomial $P(x)$ has a field $\mathbb{S}$ called its 'splitting field' or 'root field' or 'decomposition field' which is the smallest field in which all its roots lie. It would correspond with the out lilac-coloured field in Figure 1. If the polynomial $x^n + a_{n-1}x^{n-1}....a_1x + a_0$ is irreducible and of degree n, it will have n distinct roots $\alpha_1, \alpha_2, ...\alpha_n$ in $\mathbb{S}$. A crucial concept is that the splitting field of $P(x)$ can

[3] For example, if we take the integers modulus 6, that is 0, 1, 2, 3, 4, 5, then $2 * 3 = 6 \equiv 0 \mod 6$, so both 2 and 3 are zero divisors. Integers mod p for p prime have no zero divisors and so form a finite field.

be built up by successively adjoining one algebraic number at a time to $\mathbb{Q}$, so constructing a chain or 'tower' of intermediate 'field extensions' as in Figure 1:

$$\mathbb{Q} \subset \mathbb{F}_1 \subset \mathbb{F}_2 \subset ..... \subset \mathbb{F}_k ..... \subset \mathbb{S}. \tag{7}$$

The solution of a quartic by first forming a related cubic and then a quadratic is an example of a tower of field extensions.

We say that $P(x)$ is a polynomial 'over the rationals' when the coefficients of $P(x)$ are all fractions. This is written using square brackets as $P(x) \in \mathbb{Q}[x]$ where $\mathbb{Q}[x]$ denotes the set of all possible polynomials with rational coefficients. Coefficients could alternatively come from a finite field $\mathbb{F}_p$. The roots will all lie in the complex numbers $\mathbb{C}$, but $\mathbb{C}$ is a vastly large field. Galois theory is concerned with the smallest field $\mathbb{S}$ which is just large enough to contain all the roots of the given $P(x)$. All roots will be 'algebraic numbers' (numbers which by definition are roots of polynomials with rational coefficients). The field $\mathbb{A}$ of all algebraic numbers is a vanishingly small subfield of $\mathbb{C}$, which is uncountably infinite, though $\mathbb{A}$ is nevertheless infinite – countably infinite. However, much smaller subfields of the algebraic numbers will still contain all the roots of any given $P(x)$. The smallest field $\mathbb{S}$ with this property is P's 'splitting field' in which $P(x)$ will be a product of n linear factors $(x - \alpha_k)$ as in Eq 2.

Any algebraic number α may be a root of many polynomials, but we home in on the unique monic polynomial $M(x)$ of lowest degree for which α is a zero, called its 'minimal polynomial'. Each stage in the tower of field extensions will have its own minimal polynomial, and the algebraical number adjoined to extend the existing subfield will be a root of this minimal polynomial. We have already seen an example of this in §2 with $x^4 - 2x^2 + 9$ following Eq 6. The minimum polynomial of $2i$ is $x^4 + 4$, of $2\sqrt{2}$ is $x^2 - 8$ and of $2i\sqrt{2}$ is $x^2 + 8$.

4 Building the tower of field extensions

This section explains how we determine, stage by stage, the smallest field $\mathbb{S}$ in which all the roots of a given $P(x)$ lie. In Figure 1 the red spots represent the roots $\alpha_1, \alpha_2, ...\alpha_n$ of some nth degree irreducible polynomial $P(x)$ with coefficients in $\mathbb{Q}$. We suppose the outer, largest field to be the splitting field $\mathbb{S}$ of our given $P(x)$. It contains all the roots of $P(x)$ but, as the notation indicates, has been created by adjoining only α_1, α_2 and α_3 to $\mathbb{Q}$ as we are supposing that these three are sufficient to generate the other roots.

4.1 Adjoining irrational numbers to the rationals

Our starting place is the field of rational numbers, $\mathbb{Q}$. Some polynomials with coefficients in $\mathbb{Q}$ such as $10x^3 - 43x^2 + 43x - 12 = (x - 3)(2x - 1)(5x - 4)$ have all their zeros in $\mathbb{Q}$. $\mathbb{Q}$ contains all the roots to represent this polynomial as a unique product of linear factors, so $\mathbb{Q}$ is its 'splitting field', $\mathbb{S}$. Polynomials which have all their coefficients and roots in $\mathbb{Q}$ are solved by factorisation. For ones of small degree this can usually be done by hand with some trial and error. For ones of high degree – perhaps 100 or larger – several algorithms have been implemented in computer algebra packages: algorithms due to Berlekamp, and Cantor and Zassenhaus[4]. From now on we will be concerned mainly with polynomials which are irreducible over $\mathbb{Q}$.

[4] See the article on factorising polynomials on *www.mathstudio.co.uk*

There are various related ways in which a field extension from K to L can be created (see Appendix 4), but the simplest is to adjoin to K at least one algebraic number α which is not already in K. All sums, differences, products, powers and quotients (except by zero) of this new element with elements in the base field K are then formed. For example, adjoining $\sqrt{N}$ to $\mathbb{Q}$, $N \in \mathbb{N}$, creates a field with general element $a + b\sqrt{N}$ where $a, b \in \mathbb{Q}$. The action also adjoins $-\sqrt{N}$ since $(a^2 - b^2N)/(a + b\sqrt{N}) = a - b\sqrt{N}$. The smaller field has equivalent elements in the enveloping field. Thus the mapping of $a \in \mathbb{Q}$ is to the element $a + 0\sqrt{N}$. AS we have already seen, this extended field is written $\mathbb{Q}(\sqrt{N})$. Similarly adjoining $\sqrt[3]{N}$ creates $\mathbb{Q}(\sqrt[3]{N})$ which has general element $a + b\sqrt[3]{N} + c\sqrt[3]{N^2}$ where a, b, $c \in \mathbb{Q}$. Every element in this field has this form. Appendix 3 shows how this particular field is closed under multiplication and division.

Formally, an extension is a homomorphism from a smaller field K to a larger field L by which all elements of K are mapped to a subset of the elements of L. The extension is written as L/K or $L : K$. The convention is to write the larger field to the left of the smaller.

To be specific $P(x) = x^2 - 3$ has the irrational roots $\pm\sqrt{3}$. By adjoining either of these to $\mathbb{Q}$ we build a larger field in which $P(x)$ splits into $(x - \sqrt{3})(x + \sqrt{3})$. These are linear factors so no further factorisation is possible, and $\mathbb{Q}(\sqrt{3})$ is the splitting field. For $x^2 - 3$ adjoining only one irrational root is sufficient because its algebraic conjugate (also called 'associate') is created by taking the reciprocal. The general element in this field extension is $a + b\sqrt{3}$, $a, b \in \mathbb{Q}$. Any and every element in $\mathbb{Q}(\sqrt{3})$, therefore, can be constructed as a linear combination of the base elements 1 and $\sqrt{3}$, using multipliers in $\mathbb{Q}$. This pair forms a basis for this extended field when we regard it as a vector space over $\mathbb{Q}$. As with any vector space the choice of basis vectors is not unique, but the dimension of the space they span is unique[5]. We say that the degree of this field extension from $\mathbb{Q}$ to $\mathbb{Q}(\sqrt{3})$ is 2 because this is the dimension of the vector space. The degree is written $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$. Since only one element has been adjoined, the extension is 'simple'.

Next take $P(x) = x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 - 3) = (x - \sqrt{2})(x + \sqrt{2})(x - \sqrt{3})(x + \sqrt{3})$. This serves our discussion even though it is reducible over $\mathbb{Q}$. Its splitting field has adjoined both $\sqrt{2}$ and $\sqrt{3}$ so is written $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Both have to be adjoined because $\sqrt{3}$ is irrational in $\mathbb{Q}(\sqrt{2})$ and *vice versa*. What is the degree of this extension? The general field element is $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$, a, b, c, $d \in \mathbb{Q}$. The $\sqrt{6}$ is required in the basis because the product $\sqrt{2}.\sqrt{3}$ is an element in the field but cannot be formed as a linear combination of 1, $\sqrt{2}$ and $\sqrt{3}$. So there are four basis vectors and the degree is 4. This is written $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$. The construction of this field can be broken into two stages: i) adjoining $\sqrt{2}$ or $\sqrt{6}$, then ii) adjoining $\sqrt{3}$ (or *vice versa*). The tower to $\mathbb{S}$ is $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ or $\mathbb{Q} \subset \mathbb{Q}(\sqrt{3}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ or $\mathbb{Q} \subset \mathbb{Q}(\sqrt{6}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$. The structure of the field extensions for this polynomial is given in §8, Degree 4, case 1.

In a similar way $x^2 + 3$ does not factor over $\mathbb{Q}(\sqrt{3})$ but does over $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(i\sqrt{3})$. This is a field extension of degree 2 with base vectors 1 and $i\sqrt{3}$. It is a subfield of $\mathbb{Q}(\sqrt{3}, i)$ which has degree 4 and base vectors 1, $\sqrt{3}$, i and $i\sqrt{3}$. The latter is constructed by adjoining $\sqrt{3}$ then adjoining i or *vice versa*. Alternatively it could be built by adjoining $i\sqrt{3}$ then either i or $\sqrt{3}$. The degree of each stage is 2 and the degree after adjoining both is $2 \times 2 = 4$. This is an example of the general rule for the degree of field extensions: if $K \subset L \subset M$, then

$$[M : L]\,[L : K] = [M : K]. \tag{8}$$

Further elements can be adjoined one at a time, each irrational in the smaller field. A cluster of nested field extensions is called a 'tower'. By Eq 8 the degree of the final (largest) extension is the

[5] For instance, the same field extension could be created by adjoining $s = 1 + 2\sqrt{3}$ since $\sqrt{3} = (s - 1)/2$.

product of the degrees over all intermediate levels. Determining the field extensions and splitting field of a given polynomial can be tricky. Some examples are given in Appendix 5.

A field extension can be defined as above by stating explicitly the algebraic numbers adjoined to $\mathbb{Q}$. It can also be defined implicitly by giving its 'minimal polynomial', $M(x)$, introduced at the end of §3. For a given algebraic number, β, $M(x)$ is usually understood to be the unique monic polynomial with smallest degree which has β as one of its roots: $M(\beta) = 0$. Thus $x^2 - 2$ is $M(x)$ for $\pm\sqrt{2}$ and $x^2 + 2x - 1$ is $M(x)$ for $\pm\sqrt{2} - 1$. However in the context of defining a field extension, the definition can be extended to be the unique monic polynomial

- with smallest degree whose roots generate the field of irrational numbers adjoined to $\mathbb{Q}$, and
- where two such irreducible polynomials have the same degree and produce the same root field, $M(x)$ is the one which, when divided into the other, leaves a non-zero remainder.

For example, we take $x^2 - 2$ and not $x^2 + 2x - 1$ to be the minimal polynomial of $\mathbb{Q}(\sqrt{2})$ because, when divided by $x^2 - 2$, the latter leaves a non-zero remainder:

$$x^2 + 2x - 1 \;=\; (x^2 - 2) + (2x + 1).$$

The degree of $\mathbb{S}$ is the degree of its minimal polynomial, which will be n or some multiple of $n \le n!$. Appendix 6 gives examples of the rather tricky task of finding $M(x)$ of a given algebraic number.

A further alternative way to define a field extension is to use the isomorphism between a simple algebraic field extension $L : K$ and the quotient ring of polynomials $K[x]$ by a minimal polynomial[6]. For instance, $\mathbb{Q}(\sqrt{3})$ is isomorphic to $\mathbb{Q}[x]/(x^2 - 3)$ where $\mathbb{Q}[x]$ represents all polynomials in x with coefficients in $\mathbb{Q}$. In this field $x^2 - 3$ is equivalent to 0; the logic is explained in Appendix 4. If instead of $\mathbb{Q}$ we use a finite field $\mathbb{F}_p$ with a prime number p of elements, this quotient will create a larger finite field with p^k elements, k a positive integer. A finite field can have only p or p^k elements so there are fields with 5, 25 and 125 elements, but not 10 or 50.

In later sections we will be using the term 'Galois extension' to describe a particularly well-behaved type of field extension. There are several equivalent definitions of this, but all we need to know at the moment is that L is a Galois extension if it is the splitting field of an irreducible polynomial with coefficients in $\mathbb{Q}$.

To summarise, the splitting field or 'root field' or 'decomposition field' $\mathbb{S}$ of a polynomial $P(x)$ is the smallest field which contains all its roots. Over this field $P(x)$ is a product of purely linear factors. In Galois theory we adjoin one root at a time to the rationals to build a tower of nested simple field extensions $\mathbb{Q} \subset K \subset L \subset \ldots.. \subset Z \subset \mathbb{S} \subset \mathbb{C}$. This is called an 'extension in radicals'. The degree of the extension $[L : K]$ is the dimension of the vector space of the extended field L divided by the dimension of the vector space spanning the smaller field K. The tower law Eq 8 allows the dimension of $\mathbb{S}$ to be calculated by multiplying the degrees of the intermediate extensions.

In practical terms, however, this all seems round the wrong way. We would like Galois theory to help find the roots of $P(x)$, whilst the scheme above infers the splitting field from a *prior* knowledge of the roots. In textbooks the theory is presented this way probably because the simplest examples to establish the theory come from polynomials whose roots are easy to find. I will follow this common path in Part II of this article, comprising §5 to §9. Methods in the reverse direction of using the theory to find the roots are the subject of Part III, §10 to the end.

[6] Note the square brackets [..] to distinguish polynomials from the field extension notation (..)

4.2 Simple extensions and primitive elements

A simple extension is one with only one algebraic number, β say, adjoined to $\mathbb{Q}$ to produce $\mathbb{Q}(\beta)$. $\mathbb{Q}(\sqrt{2},\sqrt{3})$, with its two elements adjoined, looks like a non-simple field extension. However, writing $\beta = \sqrt{2}+\sqrt{3}$, observe that:

$$\beta^3 = 11\sqrt{2}+9\sqrt{3}$$

$$\text{so} \quad \beta^3 - 9\beta = 2\sqrt{2}, \qquad -\beta^3 + 11\beta = 2\sqrt{3}$$

so $\sqrt{2}$ and $\sqrt{3}$ are in the field $\mathbb{Q}(\sqrt{2}+\sqrt{3})$. Also

$$\beta^2 = 5 + 2\sqrt{6} \quad \text{so} \quad \sqrt{6} = \tfrac{1}{2}(\beta^2 - 5)$$

and $\sqrt{6}$ is also in $\mathbb{Q}(\sqrt{2}+\sqrt{3})$. Thus $\mathbb{Q}(\sqrt{2},\sqrt{3}) \equiv \mathbb{Q}(\sqrt{2}+\sqrt{3})$ and the extension is in fact simple and of degree 4. This is confirmed by determining that the minimal polynomial of $\sqrt{2}+\sqrt{3}$ is x^4-10x^2+1.

We have already seen that one set of basis vectors for this field extension is $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$. The equivalent simple extension gives another basis as $\{1,\beta,\beta^2,\beta^3\}$, $\beta = \sqrt{2}+\sqrt{3}$. Each number in any simple field extension $\mathbb{Q}(\beta)$ can be constructed as a linear combination of 1, β and its linearly independent powers. β is called a 'primitive element' of the field extension. Some examples are given in Appendix 9.

The same algebraic number field can be generated by the roots of more than one polynomial. Consider for example that the above field, $\mathbb{Q}(\sqrt{2},\sqrt{3})$ can be generated by powers of any of these:

$$\sqrt{2}+\sqrt{3}: \text{ minimal polynomial } x^4-10x^2+1, \quad \text{roots } \pm\sqrt{2}\pm\sqrt{3} = \pm\sqrt{5\pm2\sqrt{6}}.$$

$$2\sqrt{2}+\sqrt{3}: \text{ minimal polynomial } x^4-22x^2+25, \quad \text{roots } \pm2\sqrt{2}\pm\sqrt{3} = \pm\sqrt{11\pm4\sqrt{6}}.$$

$$\sqrt{2}+2\sqrt{3}: \text{ minimal polynomial } x^4-28x^2+100, \quad \text{roots } \pm\sqrt{2}\pm2\sqrt{3} = \pm\sqrt{14\pm4\sqrt{6}}.$$

It is often the case that a linear combination of algebraic elements will produce a primitive element and an equivalent simple extension. Thus $\mathbb{Q}(\alpha_1,\alpha_2,...,\alpha_k) \equiv \mathbb{Q}(\alpha_1+h_2\alpha_2+...+h_k\alpha_k)$, $h_j \in \mathbb{Q}$.

There is an important general fact here: for any polynomial P with coefficients in a base field K but irreducible over K, the number of ways in which K can be extended to the splitting field $\mathbb{S}$ of P is the degree [L:K]. Thus if $P = x^2-2$, $\mathbb{Q}$ can be extended to either $\mathbb{Q}(+\sqrt{2})$ or $\mathbb{Q}(-\sqrt{2})$, two isomorphic forms of $\mathbb{S}$, and similarly for the quartic equations just quoted.

5 The tower of groups

5.1 The Galois group $\mathcal{G}$

The essence of Galois theory is that the splitting field of $P(x)$ has an exact counterpart in a particular group $\mathcal{G}$ of permutations of the roots of $P(x)$. Moreover, every subfield in the tower of extensions from $\mathbb{Q}$ to $\mathbb{S}$ has a unique group counterpart in the subgroups of $\mathcal{G}$. This pairing of subfields and subgroups is called the 'Galois Correspondence' and was the crucial insight that Evariste Galois had before getting himself shot. Though this group of permutations, called the Galois group, was introduced in §2, we need now to examine it in some detail.

Suppose K is a field, either $\mathbb{Q}$ or a field extension of $\mathbb{Q}$, and suppose an irrational number β_1 not in K is adjoined to K to produce a further extended field L so $L = K(\beta_1)$. β_1 will be a root

of its minimal polynomial $M(x)$. If $M(x)$ has degree m, there will be $m-1$ other roots of $M(x)$ which will also lie in L. Therefore $L = K(\beta_1) = K(\beta_1, \beta_2, \beta_3, ..., \beta_m)$. Some of these other $m-1$ roots may be primitive elements and so could equally well generate the field L. The elements of the Galois group of the extension $L : K$ are those permutations of the m roots which preserve the structural relations between the roots and as a result leave the field K unchanged. This means that shuffling the roots within $\mathcal{G}$ still allows all the cancellation and fusion of radicals necessary for those numbers which are in K only not to be affected. Some examples of these were given at the end of §2.

In this article permutations are written in cycle notation. Thus (12) means 'swap elements 1 and 2' and (134) means element 1 goes to the position of 3, element 3 to the position occupied by 4, and 4 to that occupied by 1. (12)(23) is read from right to left, so 2 goes to 3, 3 goes first to 2 then to 1, and 1 goes to 2. The combined effect is (123).

Each permutation of roots is also called a 'field automorphism' because the set of roots is being mapped onto itself under the permutation transformation. The relevant permutations are those which involve only the algebraic numbers in the outer field L and do not disturb K. This subset of all automorphisms of the roots has all the properties of a group. This is because:

- permutations can be combined by simply carrying out one then the next; the group operation is concatenation,
- there is an identity permutation $I = () = (1)(2)(3)...(n)$,
- each permutation has a unique inverse,
- the set of permutations forming $\mathbb{HG}$ is closed.

History has named this group the Galois group $\mathcal{G}$ of $P(x)$.

The reader may know the concepts of homomorphism and isomorphism of algebraic structures. We have two sets, A and B, of elements $a_j \in A$, $b_k \in B$ where the indices j, k run over several or even many values. A joining, multiplication or concatenation operation $\circ$ applies between elements of A and a similar operation $*$ applies within B. A homomorphism θ maps elements of A to elements of B in such a way that the relations between elements carry over from A to B. This means that the result of composing two elements and mapping them from A to B is the same whether the joining operation is applied first in the space of A or later in that of B. Symbolically

$$\text{if } \theta(a_1) = b_1 \text{ and } \theta(a_2) = b_2, \quad \text{then } \theta(a_1 \circ a_2) = \theta(a_1) * \theta(a_2) = b_1 * b_2.$$

In addition $\theta(I) = e$ where I is the identity element in A and e the identity in B.

In a general homomorphism several elements of A could be sent to the identity e. We then say that the homomorphism is 'not faithful' because a distortion has occurred and information in A has been lost in the transfer to B. The section of A which is lost by being mapped to e (*i.e.* obliterated) is called the 'kernel' of the homomorphism. An isomorphism is a homomorphism which is faithful: it is a bijection, meaning every element of A maps to a separate distinct element of B and none is left over. Only I maps to e. With an isomorphism there is a reverse operation θ^{-1} which uniquely maps each element $b \in B$ back to its corresponding $a \in A$.

An automorphism is an isomorphism where the sets A and B, and hence the operations $\circ$ and *, are the same. An automorphism θ maps an algebraic structure to itself. It permutes the

elements by mapping a_j to a_k in such a way that $\theta(a_j \circ a_k) = \theta(a_j) \circ \theta(a_k)$. Clearly the identity I must map to itself and this implies that inverses of elements map to the corresponding inverses, since

$$\text{if } \theta(a) = b, \text{ then } \theta(I) = \theta(a.a^{-1}) = \theta(a)\theta(a^{-1}) = b.b^{-1} = I.$$

Also an element of general order m can map only to another element of order m. An automorphism is essentially a relabelling of the elements of an algebraic structure.

The subgroup structure of the Galois group maps to the subfield structure of $\mathbb{S}$ by the Galois Correspondence such that Eq 7

$$\mathbb{Q} \subset \mathbb{F}_1 \subset \mathbb{F}_2 \subset ..... \subset \mathbb{F}_k ..... \subset \mathbb{S}. \qquad \textit{copy of } (7)$$

has the dual chain of subgroups

$$\mathcal{G} \supset \mathcal{H}_1 \supset \mathcal{H}_2 \supset ..... \supset \mathcal{H}_k ..... \supset I, \qquad (9)$$

where I is the identity element, shorthand for the cyclic group C_1 of one element. Note that $\mathbb{Q}$ is matched with $\mathcal{G}$ and I with $\mathbb{S}$; the reason is explained later. In any practical application we would hope to identify the finite group $\mathcal{G}$ from the coefficients of $P(x)$ and use the known properties of $\mathcal{G}$ to determine the chains of subgroups as in Eq 9. Then this would specify the splitting field $\mathbb{S}$ and the corresponding subfields in Eq 7. Finally and hopefully a pathway from $\mathbb{Q}$ to $\mathbb{S}$ can be found to allow the roots of $P(x)$ to be expressed explicitly in terms of radicals involving the coefficients of P. Alternatively, if no such pathway exists, that should also be plain from knowledge of $\mathcal{G}$. That is where this article is heading.

5.2 Soluble polynomials

Though series of nested groups and nested fields have been shown at Eqs 7 and 9, we need to explain normal series and composition series. Given a group G, a subgroup series is an ordered set of subgroups from the single identity element in C_1 to G such that one proper subgroup fits inside the next: $\{I\} = G_0 \subset G_1 \subset G_2 \subset G_3 \subset ..... \subset G_{k-1} \subset G_k = G$. Such a series would correspond to a stepwise ascending path through a subgroup lattice. Normal and composition series are subgroup series with particular additional features.

- In a normal series, every G_j is a normal subgroup of the next one, G_{j+1} (though not necessarily normal in G or in G_{j+2}). $\{I\} = G_0 \lhd G_1 \lhd G_2 \lhd G_3 \lhd ..... \lhd G_{k-1} \lhd G_k = G$.
- In a composition series every quotient group G_{j+1}/G_j is a simple group, that is, one with no normal subgroups. The quotient groups are called composition factors of the series.

Now we can state what is perhaps the principal result of this article. There are two equivalent statements:

1. A polynomial is solvable in radicals if and only if its Galois group includes a normal series with the additional property that every factor group G_{j+1}/G_j in the series is abelian.
2. A polynomial is solvable in radicals if and only if its Galois group includes a composition series in which all composition factors G_{j+1}/G_j are cyclic groups of prime order, C_p.

These are the conditions under which the field extension from the fields corresponding to G_j and G_{j+1} can be made by adjoining a single new radical. For a solution of $P(x)$ in radicals the chain of subgroups can be formed only from normal subgroups of $\mathcal{G}$. This allows quotient groups to be

formed and all these quotient groups must be abelian. By the Correspondence Theorem each field extension must be normal – that is, include all the roots of its minimal polynomial.

A few examples will illustrate the matter.

- $x^2 - 3$: This is soluble with roots $\pm\sqrt{3}$. The single field extension $\mathbb{Q}(\sqrt{3})$ contains both roots (*i.e.* is normal) and is of degree 2. The Galois group of $\mathbb{Q}$-automorphisms also has degree 2 so is C_2. C_2 has the trivial normal subgroup $\{I\} = C_1$ so a factor group C_2/C_1 can be formed. This is also C_2 which is abelian, indeed cyclic. So by the central theorem of soluble polynomials, $x^2 - 3$ should be soluble, which indeed it is.

- Suppose a polynomial can be shown[7] to have Galois group C_{12} – is it soluble in radicals? We look for normal subgroups and their quotient groups to see if they are abelian. We have several choices. First $\{I\} = C_1$ is a normal subgroup and $C_{12}/C_1 = C_{12}$ which is an abelian quotient groups, so straight away that polynomial is soluble in radicals. Of course finding the set of solutions might be difficult since the theorem we are using is an existence theorem, not a method for constructing the roots. We might get further if the solution were broken into manageable stages by a tower of subfields. So we note that

$$C_1 \lhd C_2 \lhd C_4 \lhd C_{12} \qquad \text{and} \qquad C_1 \lhd C_3 \lhd C_6 \lhd C_{12}$$

  point to two towers of field extensions since the quotient factors in these series are respectively

$$\frac{C_2}{C_1} = C_2,\ \frac{C_4}{C_2} = C_2,\ \frac{C_{12}}{C_4} = C_3 \qquad \text{and} \qquad \frac{C_3}{C_1} = C_3,\ \frac{C_6}{C_3} = C_2,\ \frac{C_{12}}{C_6} = C_2,$$

  all of which are abelian, indeed cyclic. Note in passing an example here of the Jordon-Hölder theorem in that there are two maximal normal series which are isomorphic, with the same number of terms (4) and same orders of their composition factors (2, 2 and 3).

- Suppose the polynomial $P(x)$ can be shown to have Galois group A_5, the alternating group on 5 items, a group of order 60. It is well known that not only is A_5 non-abelian, but it is the smallest non-abelian simple group. The fact that it has no normal subgroup except C_1 means that the only factor group which can be formed is $A_5/C_1 = A_5$ itself. As this is not abelian, by the Galois correspondence there is no corresponding field extension of $\mathbb{Q}$ in which the roots of $P(x)$ lie. Galois himself pointed out that many quintic polynomials have automorphism groups which are A_5 or S_5 and that is the reason why these quintics have no solutions in radicals.

6 Examples of Galois correspondence

It is appropriate at this juncture to illustrate the theory with several worked examples of increasing complexity. We will attempt to find the roots of various polynomials in radicals and use them to show the fields in which they lie, the corresponding Galois group. From this we will determine the invariant fields of the various subgroups. In my limited experience, identifying the field extensions which correspond to a particular subgroup of $\mathcal{G}$ can be quite challenging. We will also find the factor groups and their corresponding field extensions in radicals.

Note how in all cases the degree of the splitting field $\mathbb{S}$ is equal to the order of the Galois group $\mathcal{G}$. We have already remarked that the degree of the extension $\mathbb{Q} : \mathbb{S}$ equals the number of ways the extension from $\mathbb{Q}$ to $\mathbb{S}$ can be made. If each stage j in the tower of field extensions is a

[7] Finding the Galois group can be difficult!

simple extension by adjoining a root α_j whose degree in n_j, there will be n_j automorphisms of α_j and its conjugate roots of the intermediate minimal polynomial corresponding to the extension. So at each intermediate stage of the tower of fields the degree of extension will be the same as the order of the intermediate Galois group. There is therefore a tower law for the order of intermediate Galois groups between $\mathbb{Q}$ and $\mathbb{S}$ which mirrors the tower law for field extensions, Eq 8 and the total degree $n = n_1 n_2 .... n_k$.

6.1 Examples of increasing complexity

Degree 1 : Start with the rational field, $\mathbb{Q}$. Polynomials such as $10x^3 - 43x^2 + 43x - 12 = (x - 3)(2x - 1)(5x - 4)$ have all their zeros in $\mathbb{Q}$. Here $\mathbb{S} = \mathbb{Q}$ and no field extension is required. As already explained, the only automorphism of this is the identity. The vector space group is spanned by the single base vector 1, and the Galois group trivially has order 1. It is $C_1 = \{I\}$, the cyclic group with one element.

Degree 2 : The irreducible $P(x) = x^2 - 2$ splits into $(x - \sqrt{2})(x + \sqrt{2})$ in $\mathbb{Q}(\sqrt{2})$. The field is spanned by vectors 1 and $\sqrt{2}$. There can be only $2! = 2$ permutations of the two roots: the identity, and interchanging $+\sqrt{2}$ with $-\sqrt{2}$. Neither of these disturbs $x^2 - 2$. The two elements of the Galois group are therefore I and s where s swaps the two roots. $\mathcal{G}$ is the cyclic group C_2. Which field elements remain constant when the identity permutation is applied? It is all of them, so the fixed field of I is the whole group. Which field remains unchanged when s is applied to $a \pm b\sqrt{2}$? It is $a \in \mathbb{Q}$. So the fixed field of s is $\mathbb{Q}$. In the latiice diagrams the cyclic group C_2 is paired with $\mathbb{Q}$, and the splitting field $\mathbb{Q}(\sqrt{2})$ with I as shown in Figure 2.

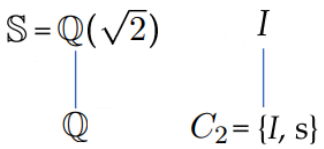

Figure 2: Matched lattice diagrams of fields and automorphism group of $x^2 - 2$.

Degree 4, Case 1 : Consider next $x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 - 3)$ and its splitting field $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \equiv \mathbb{Q}(\sqrt{2} + \sqrt{3})$. In §4.1 it was shown that this extension has degree 4. Which permutations of the roots are field automorphisms? Clearly $\pm\sqrt{2}$ are conjugates as are $\pm\sqrt{3}$. Even though the four roots can be permuted in $4! = 24$ ways, there are only three allowable permutations apart from the identity :

1. s_1: swap $\sqrt{2}$ and $-\sqrt{2}$ leaving $\sqrt{3}$ and $-\sqrt{3}$ unmoved; fixed field $\mathbb{Q}(\sqrt{3})$.
2. s_2: swap $\sqrt{3}$ and $-\sqrt{3}$ leaving $\sqrt{2}$ and $-\sqrt{2}$ unmoved, fixed field $\mathbb{Q}(\sqrt{2})$.
3. s_3: swap both $\sqrt{2}$, $-\sqrt{2}$ and $\sqrt{3}$, $-\sqrt{3}$; fixed field $\mathbb{Q}(\sqrt{6})$.

To be clear $\sqrt{3}$ cannot be swapped with $\sqrt{2}$ unless $-\sqrt{3}$ is also swapped with $-\sqrt{2}$. The Galois group is $C_2 \times C_2$, also called the V_4 or Klein 4-group, the symmetry group of a non-square rectangle for which the operations are reflection plus rotation by 180°. The subgroups and the corresponding tower of field extensions are shown by the lattice diagrams in Figure 3. The degree at every link marked by a blue line is 2.

The group lattice clearly implies that the tower of field extensions from $\mathbb{Q}$ could be formed by any of these three approaches shown in the central diagram:

1. adjoin $\sqrt{2}$ then $\sqrt{3}$,

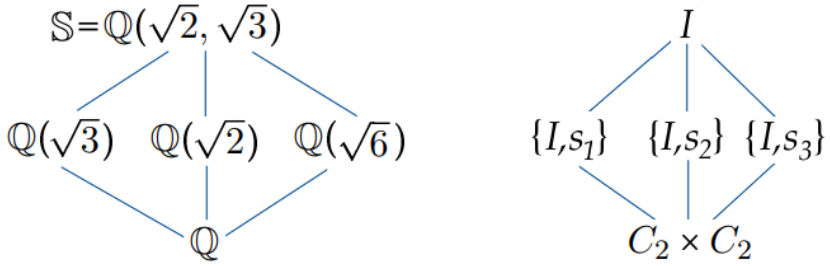

Figure 3: Structure of field extensions of $(x^2-2)(x^2-3)$ and their corresponding subgroups.

2. adjoin $\sqrt{3}$ then $\sqrt{2}$,
3. adjoin $\sqrt{6}$ then either $\sqrt{2}$ or $\sqrt{3}$.

The Klein 4-group is abelian and so are its three non-trivial subgroups. The normal series $\mathbb{Q} \lhd \mathbb{Q}(\sqrt{3}) \lhd \mathbb{Q}(\sqrt{3},\sqrt{2})$ has quotients $\mathbb{Q}(\sqrt{3})/\mathbb{Q} \equiv C_2$ and $\mathbb{S}/\mathbb{Q}(\sqrt{3}) \equiv C_2$. This is consistent with Galois theory on the conditions for a solution in radicals.

In §4.2 it was shown that $\mathbb{Q}(\sqrt{2},\sqrt{3})$ is isomorphic to the simple extension $\mathbb{Q}(\sqrt{2}+\sqrt{3})$, so a slightly alternative view is obtained by examining the minimal polynomial of $\sqrt{2}+\sqrt{3}$ which is x^4-10x^2+1. Label its four roots as

$$\alpha_1 = \sqrt{2}+\sqrt{3}, \qquad \alpha_2 = -\sqrt{2}+\sqrt{3}, \qquad \alpha_3 = -\sqrt{2}-\sqrt{3}, \qquad \alpha_4 = \sqrt{2}-\sqrt{3}.$$

Note the complete equivalence of these four: any one can be generator of all the algebraic numbers in the field extension $\mathbb{Q}(\alpha_j)$. Many sets of vectors can define a basis: for instance $\{I,\alpha_1,\alpha_1^2,\alpha_1^3\}$, $\{I,\alpha_1,\alpha_2,\alpha_1\alpha_2\}$, or $\{I,\sqrt{2},\sqrt{3},\sqrt{6}\}$. 24 permutations of these roots are possible, but only 4 preserve algebraic relations such as $\alpha_1+\alpha_3 = \alpha_2+\alpha_4 = 0$ and $\alpha_1^2 = \alpha_3^2$. The operation s swaps $\sqrt{2}$ for $-\sqrt{2}$ and *vice versa*, and t swaps the sign of $\sqrt{3}$. Thus s interchanges α_1 with α_2 and α_4 with α_3, so can be notated as the permutation (12)(34). Similarly t interchanges α_1 with α_4, α_2 with α_3 and so is (14)(23). The product of these is (13)(24). This negates α_1, turning it into α_3 but leaves $\alpha_1^2 = \alpha_3^2 = 5+2\sqrt{6}$, and also $\alpha_2^2 = \alpha_4^2 = 5-2\sqrt{6}$. This is consistent with $\alpha_1\alpha_2 = \alpha_3\alpha_4 = 1$. The fixed fields can now be identified as

$$s = (12)(34) \text{ fixes } \sqrt{3}, \qquad t = (14)(23) \text{ fixes } \sqrt{2}, \qquad st = (13)(24) \text{ fixes } \sqrt{6}\,.$$

Degree 4, Case 2 : Another polynomial with the Klein 4-Galois group is $P(x) = x^4+1$. This is irreducible over $\mathbb{Q}$, but factors over $\mathbb{Q}(i)$ as $(x^2+i)(x^2-i)$. This factors further over $\mathbb{C}$ as

$$(x-\sqrt{i})(x+\sqrt{i})(x-\sqrt{-i})(x+\sqrt{-i}) \quad \text{where} \quad \sqrt{i} = \frac{1+i}{\sqrt{2}}, \ \sqrt{-i} = i\sqrt{i} = \frac{-1+i}{\sqrt{2}}. \tag{9a}$$

The roots are marked as red spots in Figure 4. Writing $\beta = \sqrt{i}$ and using $\beta^3 = \sqrt{-i}$ Eq 9a becomes

$$(x-\beta)(x+\beta)(x-\beta^3)(x+\beta^3). \tag{9b}$$

These roots reside in the field extension $\mathbb{Q}(\beta) = \mathbb{Q}(i,\sqrt{2})$. Basis vectors for this can be either $\{1,\beta,\beta^2,\beta^3\}$ or $\{1,\sqrt{2},i,i\sqrt{2}\}$. The linear factorisation is similar to that of $(x^2-2)(x^2-3)$ above with β taking the role of $\sqrt{2}$ and β^3 that of $\sqrt{3}$. The spitting field is therefore $\mathbb{Q}(i,\sqrt{2}) \equiv \mathbb{Q}(\sqrt{2}+i)$ and the Galois group is $C_2 \times C_2$ as in Figure 3. An alternative way of writing the factorisation in Eq 9a, b is

$$(x-\beta)(x-\beta^5)(x-\beta^3)(x-\beta^7). \tag{9c}$$

The automorphisms of $\mathbb{S}$ can be notated in several ways and are

1. $s_0 : \beta \to \beta$, the identity,
2. $s_1 : \beta \to \beta^3$, or $\frac{1}{\sqrt{2}}(1+i) \to \frac{1}{\sqrt{2}}(-1+i)$, or (13)(57)
3. $s_2 : \beta \to \beta^5$, or $\beta \to -\beta$ or $\frac{1}{\sqrt{2}}(1+i) \to \frac{-1}{\sqrt{2}}(1+i)$, or (15)(37),
4. $s_3 = s_1 s_2 = s_2 s_1 : \beta \to \beta^7$, or $\frac{1}{\sqrt{2}}(1+i) \to \frac{1}{\sqrt{2}}(1-i)$. This takes β^3 to $\beta^{21} \equiv \beta^5 \mod 8$. In permutation notation it is (17)(35).

One test that these are genuine automorphisms is to observe that β^7 is the complex conjugate of β so that their sum $\beta + \beta^7 \in \mathbb{Q}$, and similarly $\beta^3 + \beta^5 \in \mathbb{Q}$.

$$\text{If } \beta \to \beta^3, \quad \beta + \beta^7 \to \beta^3 + \beta^{21} \equiv \beta^3 + \beta^5 \in \mathbb{Q}, \text{ and } \beta^3 + \beta^5 \to \beta^9 + \beta^{15} \equiv \beta + \beta^7 \in \mathbb{Q},$$

$$\text{If } \beta \to \beta^5, \quad \beta + \beta^7 \to \beta^5 + \beta^{35} \equiv \beta^5 + \beta^3 \in \mathbb{Q}, \text{ and } \beta^3 + \beta^5 \to \beta^{15} + \beta^{25} \equiv \beta^7 + \beta \in \mathbb{Q}.$$

$s_1^2(\beta) = \beta$ and $s_2^2(\beta) = \beta^9 \equiv \beta \mod 8$ so both these operations have degree 2, as does s_3. The three C_2 subgroups respectively have elements $\{I, s_1\}$, $\{I, s_2\}$, $\{I, s_3\}$.

The corresponding intermediate field extensions contain those algebraic numbers fixed by each of these permutations.

- s_3 is complex conjugation so the fixed field is $\mathbb{R}$ and in particular $\mathbb{Q}(\sqrt{2})$.
- s_1 takes β^3 to β and swaps β^5 with β^7 so reversing the sign of each real part. It is reflection in the imaginary axis and therefore leaves either i or $i\sqrt{2}$ invariant. To see which, check the action of s_1 on a general algebraic number composed from the base vectors;

  $$n = a_0 + a_1\beta + a_2\beta^2 + a_3\beta^3 \to a_0 + a_1 i\beta - a_2\beta^2 + a_3\beta$$

  so if n is invariant, $a_2 = 0$ and $a_1 = a_3$, making $n = a_0 + a_1\beta(1+i) = a_0 + a_1(1+i)^2/\sqrt{2} = a_0 + a_1 i\sqrt{2}$. So the fixed field of s_1 is $\mathbb{Q}(i\sqrt{2})$.
- s_2 takes $n = a_0 + a_1\beta + a_2\beta^2 + a_3\beta^3 \to a_0 - a_1\beta + a_2\beta^2 - a_3\beta^3$. The fixed number is $a_0 + a_2 i$ and the fixed field $\mathbb{Q}(i)$.

The route taken to build the tower in the analysis just used is $\mathbb{Q} \subset \mathbb{Q}(i) \subset \mathbb{Q}(i, \sqrt{2})$. However, the lattice diagram states that the tower can be built by first adjoining $\sqrt{2}$ or $i\sqrt{2}$ rather than i.

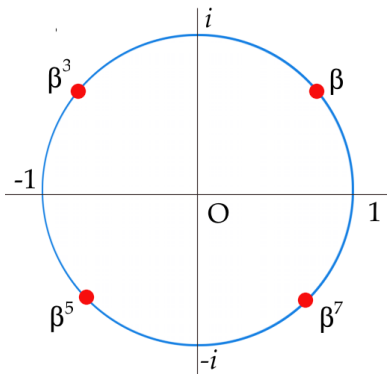

Figure 4: The complex roots of $x^4 + 1$.

There must be factorisations of x^4+1 in these fields, and indeed they are found by noting that $x^4+1=(x^4\pm 2x^2+1)\mp 2x^2$. The three intermediate factorisations are

$$(x^2-1+i\sqrt{2}x)(x^2-1-i\sqrt{2}x),\quad (x^2+1+\sqrt{2}x)(x^2+1-\sqrt{2}x),\quad (x^2+i)(x^2-i).$$

These field extensions have minimal polynomials x^2+2, x^2-2 and x^2+1 respectively.

This is a suitable place to mention again the 'primitive element' of a field. It is an algebraic number V from which is it possible to generate all numbers in the field as a linear combination of V and its powers. A basis for the field which contains the roots of x^4+1 is $\{1,\sqrt{2},i,i\sqrt{2}\}$. This is $\mathbb{Q}(\sqrt{2},i)\equiv\mathbb{Q}(\sqrt{2}+i)$ and $V=\sqrt{2}+i$ turns out to be a primitive element because

$$1=\tfrac{1}{9}(2V^2-V^4),\qquad \sqrt{2}=\tfrac{1}{6}(5V-V^3),\qquad i=\tfrac{1}{6}(V+V^3),\qquad i\sqrt{2}=\tfrac{1}{18}(7V^2+V^4).$$

The numbers $\pm\sqrt{2}\pm i$ are the roots of x^4-2x^2+9 which therefore is the minimal polynomial for the splitting field.

Degree 6 : $P(x)=x^3-N$ for $N>0$, N not a cube. Its three roots are

$$\alpha_1=\beta,\qquad \alpha_2=\omega\beta,\qquad \alpha_3=\omega^2\beta,\qquad \beta=\sqrt[3]{N},\quad \omega=\exp(2\pi i/3)$$

where β is the real cube root of N. $\mathbb{S}=\mathbb{Q}(\omega,\beta)$. The roots create a field which requires 6 base vectors to represent it:

$$\{1,\qquad \beta,\qquad \beta^2,\qquad \omega,\qquad \omega\beta,\qquad \omega\beta\ \}.$$

The general field element is a linear combination of these plus ω^2, $\omega^2\beta$, $\omega^2\beta^2$. It is not necessary, however, to include these last three elements in the basis because $\omega^2=-1-\omega$, a linear combination. The roots can be shuffled into of $3!=6$ permutations, and the Galois group $\mathcal{G}$ is S_3, the symmetric group on 3 items which is also D_3, the dihedral group for an equilateral triangle. It comprises these permutations of the indices

$$I,\quad (123),\quad (132),\quad (12),\quad (13),\quad (23).$$

Note that $\alpha_1^2=\alpha_2\alpha_3$ and all six permutations above respect this. The subgroups are {I}, {I, (123), (132)}, {I,(23)} and other two of order 2.

An alternative presentation of $\mathcal{G}$ is in terms of the 'words' s and t as $<s^3,t^2,ts=s^2t>$ where

- $s(\beta)=\omega\beta$ effects an anticlockwise rotation of β, $\omega\beta$ and $\omega^2\beta$ each through 120° and
- $t(\omega)=\omega^2$ which is complex conjugation.

The effect of s on β^2 must be reckoned as a homomorphism, so $s(\beta^2)=(s(\beta))^2=\omega^2\beta^2$. This leads to a neat way to find the fixed fields. Write the essential field elements, including those in ω^2, in an array A where each element is recorded as its power of ω. The identity array A is modified by each automorphism and it is easy to spot which elements have not changed. Thus 0 represents $\beta\omega^0$ and $st(\omega\beta)=s(\omega^2\beta)=\omega^3\beta=\beta$. Below are the six arrays with the fixed elements highlighted in blue.

$I(A)$:

	1	β	β^2
1	0	0	0
ω	1	1	1
ω^2	2	2	2

,

$s(A)$:

	1	β	β^2
1	0	1	2
ω	1	2	0
ω^2	2	0	1

,

$s^2(A)$:

	1	β	β^2
1	0	2	1
ω	1	0	2
ω^2	2	1	0

$$t(A):\ \begin{matrix}0&0&0\\2&2&2\\1&1&1\end{matrix},\qquad st(A):\ \begin{matrix}0&1&2\\2&0&1\\1&2&0\end{matrix},\qquad s^2t(A):\ \begin{matrix}0&2&1\\2&1&0\\1&0&2\end{matrix}$$

From this we can read off the invariant fields:

$$I:\ \mathcal{G},\qquad s,s^2:\ \mathbb{Q}(\omega),\qquad t:\ \mathbb{Q}(\beta)=\mathbb{Q}(\alpha_1),\qquad st:\ \mathbb{Q}(\omega^2\beta)=\mathbb{Q}(\alpha_3),\qquad s^2t:\ \mathbb{Q}(\omega\beta)=\mathbb{Q}(\alpha_2)\,.$$

The correspondence between the permutation and word presentations of $\mathcal{G}$ is

$$\begin{matrix}I&(123)&(132)&(23)&(13)&(12)\\I&s&s^2&t&st&s^2t\end{matrix}$$

The single subgroup of order 3 is the 'derived' or 'commutator' subgroup. Calling this $\mathcal{N}$, it is a normal subgroup and so it and its cosets form a quotient group $\mathcal{G}/\mathcal{N}$ of order $6/3=2$, isomorphic to the abelian cyclic group C_2. This fact is highly significant in Galois theory because, as has been stressed, the criterion for a polynomial to have roots in radicals is that there be a series of derived cyclic (or at least abelian) groups descending from $\mathcal{G}$ of $P(x)$ to I.

Note, however, that the fixed field of $\mathcal{N}$ is $\mathbb{Q}(\omega)$ in which a typical element is $a+b\omega+c\omega^2$. This involves all three roots of $x^3-1=0$, a cyclotomic polynomial which factorises as $(x-1)(x^2+x+1)$. A field which contains all roots of a polynomial is called 'normal' and always corresponds in the lattice diagrams with a normal subgroup, that is, one which is conjugate to itself through having its left and right cosets set-wise equal. Now $x^2+x+1=0$ has roots $\frac{1}{2}(-1\pm i\sqrt{3})=\{\omega,\ \omega^2\}$. The degree of the extension $\mathbb{Q}(\omega):\mathbb{Q}$ is therefore 2, not 3 as might be supposed at first sight. Thus $\mathbb{Q}(\omega)$ is the splitting field of both x^2+x+1 and x^3-1. Note that the extension from $\mathbb{Q}$ can be made in two ways, by adjoining either ω or $\omega^2=\omega^*$. By definition all splitting fields are normal. The further extension to $\mathbb{S}$ is made by adjoining β which has degree 3, giving the overall degree of $2\times3=6$. In contrast none of the degree-2 extensions $\mathbb{Q}(\beta)$, $\mathbb{Q}(\omega\beta)$, $\mathbb{Q}(\omega^2\beta)$ contains all the roots of their minimal polynomial. For instance the typical element of $\mathbb{Q}(\omega\beta)$ is $a+b\omega\beta+c\omega^2\beta^2$ and $\omega^2\beta$ is missing. The intermediate factorisation of x^3-N in $\mathbb{Q}(\beta)$ is $(x-\beta)(x^2+\beta x+\beta^2)$.

Degrees 3, 5, 9, *etc.* : This type of field extension and Galois group arises as a subfield and subgroup of a cyclotomic polynomial x^p-1, p prime. 'Cyclotomic' means 'circle cutting ' and describes the roots of these polynomials dividing the unit circle into p equal arcs[8]. Take the case of $p=11$. The roots are unity plus ten others at $\exp(2\pi ki/11)$, $1\le k\le10$ around the unit circle. Label these ω^k. Now add the five complex conjugate pairs $C_1=\omega+\omega^{10}$, $C_2=\omega^2+\omega^9$, $C_3=\omega^3+\omega^8$, $C_4=\omega^4+\omega^7$, $C_5=\omega^5+\omega^6$. These are five real numbers which form a subfield $\mathbb{Q}(\cos(2\pi/11))$ of the Galois group of $x^{11}-1$. Note that $1+2\sum_1^5\cos(2\pi k/11)=0$, showing a linear dependence of one of the cosine terms. Using this, a basis for the subfield is $\{1,\cos(2\pi/11),...,\cos(8\pi/11)\}$. The degree of the extension is 5. The subfield's minimal polynomial is $32x^5+16x^4-32x^3-12x^2+6x+1$ and has roots $\cos(n\pi/11)$, $n=2,4,6,8,10$. Any one of these could be adjoined to $\mathbb{Q}$ to generate the splitting field. This is another example of a fact we have noted before: that the number of ways of extending a base field to the splitting field is the degree of the extension. The automorphisms are $\omega\to\omega^j$, $1\le j\le5$ and the Galois group is isomorphic to C_5.

Degree 8 : $P(x)=x^4-3$. This has two real roots, $\pm\rho$, and two complex conjugates, $\pm i\rho$, where ρ is the positive real value of $\sqrt[4]{3}\approx1\cdot316$.

$$\alpha_1=+\rho,\qquad \alpha_2=+i\rho,\qquad \alpha_3=-\rho,\qquad \alpha_4=-i\rho,$$

[8] There is a description of cyclotomic polynomials over $\mathbb{Q}$ and over finite fields in Appendix 3 of my article on factorising polynomials on *www.mathstudio.co.uk*.

where they have been labelled anticlockwise from the positive real axis. It is clear that the splitting field $\mathbb{S}$ is $\mathbb{Q}(\rho,i) = \mathbb{Q}(\rho+i)$ with base vectors $\{1,\rho,\rho^2,\rho^3,i,i\rho,i\rho^2,i\rho^3\}$. There are 4! = 24 permutations of the roots, but only some preserve the algebraic relations amongst them, such as $\alpha_1+\alpha_3 = \alpha_2+\alpha_4 = 0$. There are three obvious automorphisms by which the roots are permuted:

- s_1 : sign reversal : $\rho \leftrightarrow -\rho$. The permutation is (13).
- s_2 : complex conjugation: $i \leftrightarrow -i$. The permutation is (24).
- s_3 : rotate all roots through 90° anticlockwise, equivalent to $\rho \to i\rho$. The cycle is (1234).

These three are enough to generate a $\mathbb{Q}$-automorphism group of 8 elements. It has five elements of order 2 and two of order 4 so is the dihedral group D_4, the symmetries of a square. Once we know that the group is D_4, it is also known that it can be generated from just two basic permutations:

1. r: rotation by 90° (s_3 above): $\rho \to i\rho$, i unchanged,
2. $c = s_2$: complex conjugation (s_2 above): ρ unchanged, $i \to -i$.

subject to $cr = r^3c$. Then sign reversal is $s_1 = r^2$. The correspondence between the permutation and word presentations of the Galois group is

I	r	r^2	r^3	c	rc	r^2c	r^3c
I	(1234)	(13)(24)	(1432)	(24)	(12)(34)	(13)	(14)(23)

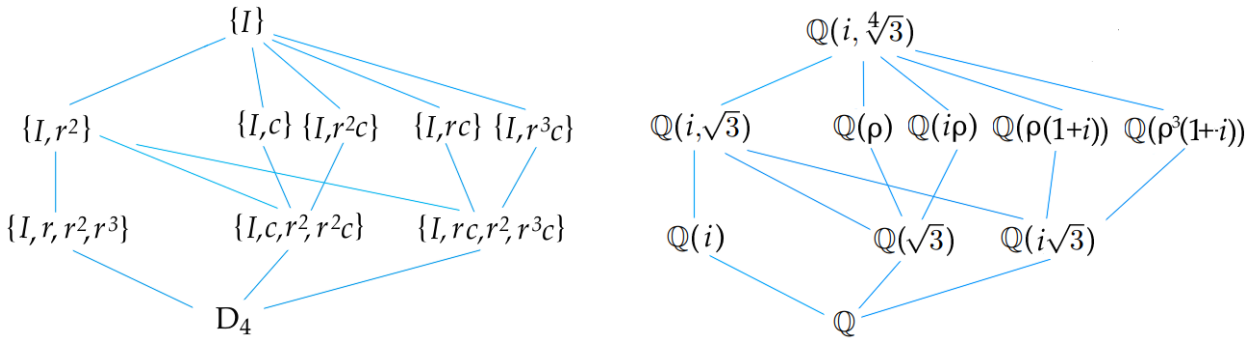

Figure 5: Lattice structures of the Galois group and field extensions of $x^4 - 3$.

The group lattice is drawn in the left panel of Figure 5 and the corresponding invariant fields on the right. The fixed fields of these automorphisms are found by seeing what remains unchanged when they act on an arbitrary linear combination x of the basis vectors or a typical field element. For example, the element $a_0 + a_1\rho + a_2\rho^2 + \ldots$ *etc.* is mapped as follows:

Coefficients :	a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	fixed
I :	1	ρ	ρ^2	ρ^3	i	$i\rho$	$i\rho^2$	$i\rho^3$:	$\mathbb{S} = \mathbb{Q}(i,\rho)$
$r : \rho \to i\rho$:	1	$i\rho$	$-\rho^2$	$-i\rho^3$	i	$-\rho$	$-i\rho^2$	ρ^3 :	$\mathbb{Q}(i)$
$r^2 : \rho \to -\rho$:	1	$-\rho$	ρ^2	$-\rho^3$	i	$-i\rho$	$i\rho^2$	$-i\rho^3$:	$\mathbb{Q}(\sqrt{3},i)$
$r^3 : \rho \to -i\rho$:	1	$-i\rho$	$-\rho^2$	$i\rho^3$	i	ρ	$-i\rho^2$	$-\rho^3$:	$\mathbb{Q}(i)$
$c : i \to -i$:	1	ρ	ρ^2	ρ^3	$-i$	$-i\rho$	$-i\rho^2$	$-i\rho^3$:	$\mathbb{Q}(\rho)$
rc :	1	$i\rho$	$-\rho^2$	$-i\rho^3$	$-i$	ρ	$i\rho^2$	$-\rho^3$:	$\mathbb{Q}(\rho(1+i))$
r^2c :	1	$-\rho$	ρ^2	$-\rho^3$	$-i$	$i\rho$	$-i\rho^2$	$i\rho^3$:	$\mathbb{Q}(i\rho)$
r^3c :	1	$-i\rho$	$-\rho^2$	$i\rho^3$	$-i$	$-\rho$	$i\rho^2$	ρ^3 :	$\mathbb{Q}(\rho^3(1+i))$

The invariants under the subgroup $\{I, rc\}$ are rather more tricky to identify. $rc(x) = x$ if $a_5 = a_1$, then $\rho + i\rho$ is constant and so is $i\rho^2 = \rho^2(1+i)^2/2$. Here are factorisations in some of these field extensions:

- in $\mathbb{Q}(\sqrt{3})$: $x^4 - 3 = (x^2 - \sqrt{3})(x^2 + \sqrt{3})$,
- in $\mathbb{Q}(\rho)$: $x^4 - 3 = (x - \rho)(x + \rho)(x^2 + \sqrt{3})$,
- in $\mathbb{Q}(i\rho)$: $x^4 - 3 = (x - i\rho)(x + i\rho)(x^2 - \sqrt{3})$.
- in $\mathbb{Q}(i, \rho)$: $x^4 - 3 = (x - \rho)(x + \rho)(x - i\rho)(x + i\rho)$.

The derived (commutator) subgroup is $\{I, r^2\}$ and its three cosets are $\{r, r^3\}$, $\{c, r^2c\}$ and $\{rc, r^3c\}$. These four sets form the compound elements of the abelian factor group $\mathcal{G}/\{I, r^2\}$.

Degree 20 : $x^5 - 1$ and $x^5 - 3$. I am dealing with both of these soluble quintics because they are superficiality similar, but their Galois groups are very different. $x^5 - 1$ is reducible over the rationals, factoring as $(x-1)(x^4 + x^3 + x^2 + x + 1)$. Its solutions are the five 5th roots of unity: $1, \omega, \omega^2, \omega^3, \omega^4$ where $\omega = \exp(2\pi i/5)$. If the roots are plotted on the Argand diagram, they lie at the vertices of a regular pentagon with unit radius, the blue spots in Figure 6.

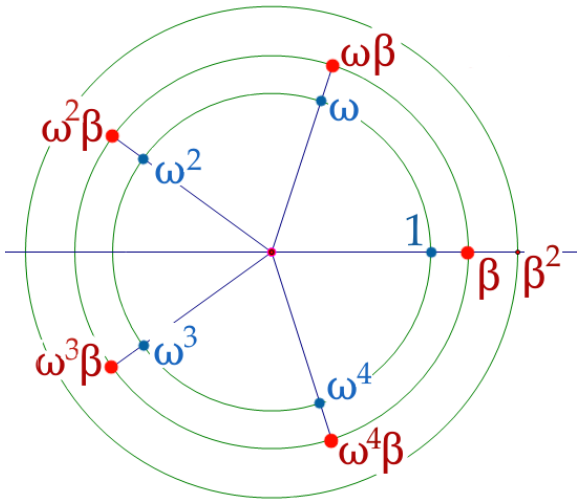

Figure 6: Roots of $x^5 - 1$ and $x^5 - 3$ plus part of its splitting field $\mathbb{Q}(\beta, \omega)$.

The Galois group of $x^5 - 1$ consists of automorphisms which send one complex root to another. The possibilities are $\tau_0(\omega) = \omega$, $\tau_1(\omega) = \omega^2$, $\tau_2(\omega) = \omega^3$, $\tau_3(\omega) = \omega^4$. Geometrically, each of these is a rotation anticlockwise through a multiple of $2\pi/5$ radians. They form a cyclic group $\mathcal{G} = C_4$ generated by τ_1 or τ_2 since $\tau_1^2(\omega) = \omega^2$, $\tau_1^3(\omega) = \omega^8 \equiv \omega^3$, $\tau_1^4(\omega) = \omega^{16} \equiv \omega \mod 5$. Note that ω is invariant under τ_1^4. The splitting field $\mathbb{S}$ is $\mathbb{Q}(\omega)$. It has a subfield $\mathbb{Q}(\sqrt{5})$ corresponding to the subgroup $C_2 = \{I, \tau_1^2\}$. The $\sqrt{5}$ arises from $\omega + \omega^4$ and $\omega^2 + \omega^3$ both being invariant under τ_1^2, and $\cos 72° = (\sqrt{5} - 1)/4$. A more thorough analysis of the automorphism group of the regular pentagon is given in Appendix 8.

Figure 6 also shows, as red spots on the middle circle, the roots of $x^5 - 3$ at $\beta = \sqrt[5]{3} \approx 1 \cdot 246$, $\omega\beta$, $\omega^2\beta$, $\omega^3\beta$, $\omega^4\beta$. The splitting field of $x^5 - 3$ is $\mathbb{Q}(\beta, \omega)$ and other elements in this field lie on the circle radius β^2 shown, plus those on two more circles with radii β^3, β^4, not shown. We can expect the field extensions $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\omega)$ to be subfields in the splitting field $\mathbb{S}$ of $x^5 - 3$. The

roots themselves do not form a group because, for instance, β^2, is not a root even though it is in $\mathbb{S}$. However, the roots do have the symmetries of the group D_{10}, the dihedral group of a pentagon with radius β, and ω representing rotation by $72° = 2\pi/5$ radians. D_{10} has 10 elements: 5 rotations by 72° around the origin and a reflection in the real axis. An analysis of D_{10} is given at the end of Appendix 8.

We now need to identify the automorphisms of $\mathbb{S}$ and its subfields which leave $\mathbb{Q}$ unchanged. Because $\omega^4 = -\omega^3 - \omega^2 - \omega - 1$, $\mathbb{S}$ has the 20 base vectors

$$\begin{array}{ccccc} 1 & \beta & \beta^2 & \beta^3 & \beta^4 \\ \omega & \omega\beta & \omega\beta^2 & \omega\beta^3 & \omega\beta^4 \\ \omega^2 & \omega^2\beta & \omega^2\beta^2 & \omega^2\beta^3 & \omega^2\beta^4 \\ \omega^3 & \omega^3\beta & \omega^3\beta^2 & \omega^3\beta^3 & \omega^3\beta^4. \end{array} \qquad (8)$$

The automorphism group can be generated by two elements s and t where s, order 5, takes $\beta \to \omega\beta$ and t, order 4, takes $\omega \to \omega^2$, and $ts = s^2t$. (t has the role of τ_1 above.) Its 20 elements are $\{I, s, s^2, s^3, s^4, t, st, st^2, ..., s^2t, ...s^4t^3\}$. The required invariant subfields are obtained by applying these automorphisms to an arbitrary linear combination of the 20 base vectors.

In practice, in calculating these $\mathbb{Q}$-invariant fields, it is useful to include the extra elements in ω^4. Neither s nor t maps β to a higher power of β, so the effect of all combinations of s and t can be summarised by the power to which ω is raised for each field element. A couple of examples should illustrate the method. As with the case Degree 6 above, the basis field vectors are conveniently written in an array and to the right is the array of powers of ω. When operated upon by automorphism st the elements are shuffled so that their indices are in the right hand array. The numbers in bold match between the initial array and the array for st. This means that these elements are invariant under the automorphism. All are members of the field generated by $\omega\beta^4$ or equivalently by $\omega^4\beta$.

$$\begin{array}{ccccc} 1 & \beta & \beta^2 & \beta^3 & \beta^4 \\ \omega & \omega\beta & \omega\beta^2 & \omega\beta^3 & \omega\beta^4 \\ \omega^2 & \omega^2\beta & \omega^2\beta^2 & \omega^2\beta^3 & \omega^2\beta^4 \\ \omega^3 & \omega^3\beta & \omega^3\beta^2 & \omega^3\beta^3 & \omega^3\beta^4 \\ \omega^4 & \omega^4\beta & \omega^4\beta^2 & \omega^4\beta^3 & \omega^4\beta^4 \end{array} \equiv \begin{array}{ccccc} 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & \mathbf{1} \\ 2 & 2 & 2 & \mathbf{2} & 2 \\ 3 & 3 & \mathbf{3} & 3 & 3 \\ 4 & \mathbf{4} & 4 & 4 & 4 \end{array}, \quad st(...): \begin{array}{ccccc} 0 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 0 & \mathbf{1} \\ 4 & 0 & 1 & \mathbf{2} & 3 \\ 1 & 2 & \mathbf{3} & 4 & 0 \\ 3 & \mathbf{4} & 0 & 1 & 2 \end{array}$$

Below are the equivalent arrays for automorphisms t^2 and st^2. With t^2 two points to note are that i) the top line of 0s is retained and ii) the indices 1 and 4 have swapped over. This swapping means that $\omega \leftrightarrow \omega^4$, and similarly $\omega^2 \leftrightarrow \omega^3$. Consequently the sum of each of these pairs is invariant under t^2. Now $\omega + \omega^4 = 2\cos(2\pi/5)$ while $\omega^2 + \omega^3 = -1 - \omega - \omega^4$. Since $\cos(2\pi/5) = (\sqrt{5}-1)/4$, the fixed field of t^2 is $\mathbb{Q}(\beta, \sqrt{5})$.

$$t^2(...): \begin{array}{ccccc} 0 & 0 & 0 & 0 & 0 \\ 4 & 4 & 4 & 4 & 4 \\ 3 & 3 & 3 & 3 & 3 \\ 2 & 2 & 2 & 2 & 2 \\ 1 & 1 & 1 & 1 & 1 \end{array}, \quad st^2(...): \begin{array}{ccccc} 0 & 1 & 2 & 3 & 4 \\ 4 & 0 & \mathbf{1} & 2 & 3 \\ 3 & 4 & 0 & 1 & \mathbf{2} \\ 2 & \mathbf{3} & 4 & 0 & 1 \\ 1 & 2 & 3 & \mathbf{4} & 0 \end{array}$$

With automorphism st^2 the fixing of $\omega + \omega^4$ is retained and in addition, as the numbers in bold show, the field of $\mathbb{Q}(\omega^3\beta)$ is fixed. The combined restrictions mean that the fixed field of st^2 is $\mathbb{Q}(\omega^3\beta, \sqrt{5})$. The full lattice of the Galois group and its corresponding fixed fields are shown in Figure 7.

$x^5 - 3$ can be factored in these subfields. As examples

1. in $\mathbb{Q}(\beta): (x - \beta)(x^4 + \beta x^3 + \beta^2 x^2 + \beta^3 x + \beta^4)$,

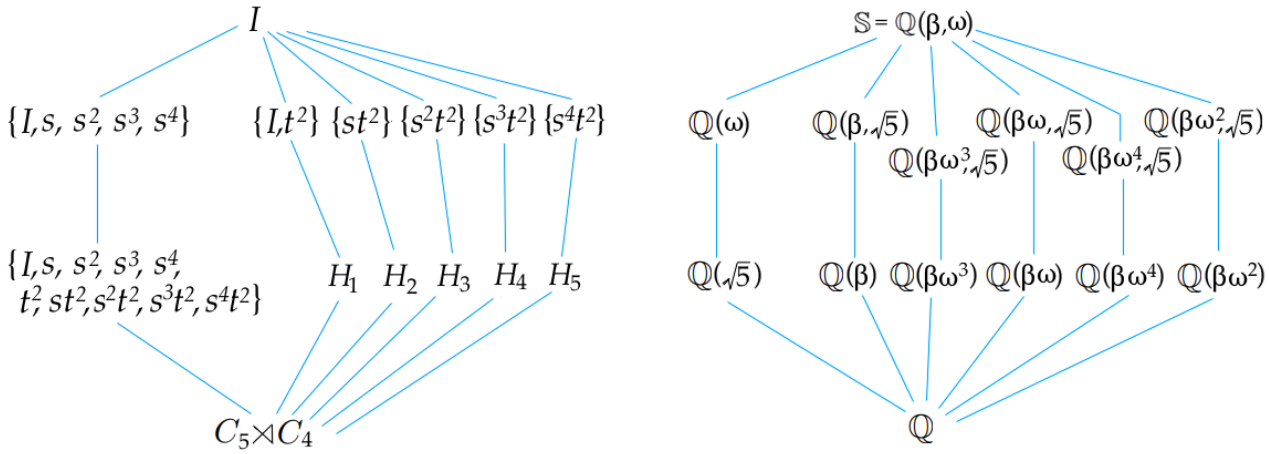

Figure 7: Structure of the group $H_{20} = C_5 \rtimes C_4$ of automorphisms of a pentagon and corresponding field extension for $x^5 - 3$. $\beta = \sqrt[5]{3}$, $\omega = \exp(2\pi i/5)$.

2. in $\mathbb{Q}(\beta, \cos\left(\frac{2\pi}{5}\right))$: $(x-\beta)(x^2 - 2\beta x\cos\left(\frac{2\pi}{5}\right) + \beta^2)(x^2 - 2\beta x\left(2\cos^2\left(\frac{2\pi}{5}\right) - 1\right) + \beta^2)$

The commutator (derived) subgroup is $\{I = s^5, s, s^2, s^3, s^4\} = C_5$ and the corresponding normal fixed field is $\mathbb{Q}(\omega)$. The quotient group has order $20/5 = 4$ with elements represented by I, t, t^2, t^3 so is cyclic, C_4.

Looking at this lattice it might seem that there are three paths upwards from I to H_{20}, but to be of use each subgroup must be normal in the one above it. C_2 is not normal in D_{10}, nor is C_4 normal in H_{20}, so the only acceptable path is $I \to C_5 \to D_{10} \to H_{20}$. The quotient groups are C_5, C_2, C_2, each of which is abelian. Hence the strategy for building a tower of field extensions runs in the opposite direction, first to adjoin a degree 2 algebraic number, then another degree 2 one, and finally one of degree 5 : $\mathbb{Q} \subset \mathbb{Q}(\cos(2\pi/5)) \subset \mathbb{Q}(\eta) \subset \mathbb{Q}(\eta, \sqrt[5]{3})$, $\eta = \exp(2\pi i/5)$.

6.2 The cubic using Galois concepts

Appendix 3 recounts the solution of the general cubic devised by Viète, and opens by showing that a general cubic can be transformed into the standard form $P(x) = x^3 + c_1 x + c_0 = 0$. Here we find its Galois group using symmetry concepts that Galois must have had.

The polynomial has three roots, one real, so its Galois group must be either the symmetric group S_3 or its only subgroup of order 3, the cyclic C_3. Consider the fixed fields of these. For S_3 it can only be $\mathbb{Q}$. C_3 has more potential, so we invent some polynomials in the roots α_1, α_2, α_3 which would be invariant under the group $C_3 = \{I, (123), 132)\}$. Two obvious ones are

$$A = \alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1\,, \qquad B = \alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2.$$

Thus $(123)A = (132)A = A$ while $(12)A = B$. Therefore $A + B$ is invariant under S_3.

The next step is to evaluate A and B in terms of the coefficients. The cubic has been transformed so that $c_2x^2 = 0$ which is a large simplification. Recall that $\alpha_1 + \alpha_2 + \alpha_3 = c_2 = 0$, $c_1 = -\alpha_1^2 - \alpha_1\alpha_2 - \alpha_2^2$ and $c_0 = \alpha_1\alpha_2(\alpha_1 + \alpha_2)$. It is fairly easy to show that $A+B = 3c_0$ and $AB = c_1^3 + 9c_0^2$. Now A and B will be the two solutions of a quadratic equation in u if $(u - A)(u - B) = 0$. This

expands as

$$u^2 - (A+B)u + AB \;=\; u^2 - 3c_0u + (c_1^3 + 9c_0^2) \quad \text{with roots} \quad 2u = 3c_0 \pm \sqrt{-4c_1^3 - 27c_0^2}.$$

We can take A as having the positive root, B the negative. It is now clear why $A+B$ is invariant under S_3 – it is merely the rational number $3c_0$. The discriminant is $-4c_1^3 - 27c_0^2$. This also happens to be the discriminant of the reduced cubic $P(x)$. If this is positive both A and B will be real, if zero they will be equal, and if negative they will be complex conjugates. Supposing $x^3 + c_1x + c_0$ to be irreducible over $\mathbb{Q}$, if A and B are rational, the Galois group $\mathcal{G}$ is C_3; if not, it is S_3. So if the discriminant of a cubic is a perfect square, its Galois group is $C_3 = A_3$, the alternating group. Examples of this seem hard to find; one quoted by Ian Stewart in his book on Galois theory is $x^3 - 3x \pm 1$.

7 Algebraic basis of Galois theory

The previous sections have steadily built a picture of Galois theory both through appeal to intuition prompted by basis facts about polynomials, and from several worked examples. It is now time to state the main theorems of Galois theory in a more formal way, including defining further terms. This section therefore summarises much of the ground covered in textbooks on Galois theory.

7.1 Review of significant concepts

Let us take stock of the technicalities met so far:

- a field extension $L : K$ made by adjoining one or more algebraic numbers α_j to field K so $L = K(\alpha_1, \alpha_2, ..., \alpha_k)$. The general member of L will be a linear combination or all elements of K plus the α_j, their products and powers, with weighting coefficients in K.

- a field extension can be regarded as a vector space in that it can be represented by a set of base vectors such that every field element is a linear combination of them. The degree of the extension $L : K$ is the minimum number of base vectors required.

- a simple extension, made by adjoining a single primitive element β to K so $L = K(\beta)$. In many cases a linear combination of roots $\beta = b_1\alpha_1 + b_2\alpha_2, ..., b_k\alpha_k$, $b_j \in \mathbb{Q}$, will create a primitive element. All numbers in field L can be written as a linear combination of β and its powers using coefficients in K.

- the minimal polynomial of an algebraic number α, the polynomial of lowest degree which has α as a root.

- the splitting field, $\mathbb{S}$ of $P(x)$, the smallest algebraic number field in which all the roots of $P(x) = 0$ lie and hence the smallest field in which $P(x)$ factorises into purely linear factors.

- K-automorphisms of a field extension $L = K(\alpha_1)$ which are those permutations of the roots $\alpha_1, \alpha_2, ..., \alpha_k$ of the minimal polynomial of α_1 which maintain the structural relations amongst the roots, such as, say, $\alpha_1\alpha_3 = \alpha_2\alpha_4 = 0$. These permutations leave unchanged all numbers in the field K, and in particular the coefficients of $P(x)$ and of *all* other polynomials which have the same algebraic numbers in their roots.

- the Galois group $\mathcal{G}$ of $P(x)$ which is the group of Q-automorphisms where the group operation is concatenation of permutations. The order of $\mathcal{G}$ equals the degree of the extension $\mathbb{S} : \mathbb{Q}$ and equals the number of ways in which $\mathbb{Q}$ can be extended to $\mathbb{S}$.

- the Galois Correspondence by which there is a one-to-one map between $\mathcal{G}$ and its subgroups and $\mathbb{S}$ and its subfields. The lattice diagrams depicting these are inverted with respect to each other in the sense that the group identity I corresponds with the splitting field and $\mathcal{G}$ corresponds with the base field $\mathbb{Q}$.

- the derived (commutator) subgroup $\mathcal{N}$ of $\mathcal{G}$ which is normal, and gives rise to an abelian quotient group $\mathcal{G}/\mathcal{N}$. It is matched in the Galois Correspondence to a 'normal' field extension, where a normal extension is one which contains all the roots of its own minimal polynomial. More will be explained about this below.

- normal and composition series of subgroups, where the quotient of adjacent members is an abelian (often cyclic) factor group which in turn corresponds with an field extension by adjoining a new radical.

The following subsections revisit and expand upon some of these technicalities and introduce new ones.

7.2 Properties of the Galois group

The Galois group $\mathcal{G}$ of $P(x)$ can be defined in two equivalent ways:

1. as the group of permutations of the roots which maintains all algebraic relations between the roots,

2. as the group of automorphisms of the splitting field $\mathbb{S}$ of the polynomial which leave the base field $\mathbb{Q}$ unchanged.

To avoid any doubt, the Galois group is a group of field automorphisms. The roots of the polynomial themselves do not form a group, only a set with some symmetries. The group operations we are talking about are permutations of the roots, or equivalently, permutations of elements in $\mathbb{S}$. It is also important to grasp that Galois theory reckons with invariants under group actions, not with those field elements which do swap places.

Textbooks discuss Galois extensions and groups in more general contexts than just between the fields $\mathbb{Q}$ and $\mathbb{S}$. Subgroups and subfields, including finite fields, can also have the essential properties of being 'Galois' because each subfield could be the splitting field of a polynomial of lower degree than the given one. These texts write generally of a K-automorphism as a field automorphism of L, for $K \subset L$, which leaves all numbers in K unchanged. The Galois group of the extension $L : K$ is then this group of K-automorphisms. The notation is

$$\mathcal{G} = \mathrm{Gal(L : K)} = \mathrm{Aut}(L| \text{ leaving invariant all elements of } K).$$

If at times distinctions between general field extensions and $\mathbb{S} : \mathbb{Q}$ are not clearly made, bear in mind that in this article deals almost entirely with polynomials over $\mathbb{Q}$ and their splitting fields. For any particular automorphism θ its 'fixed field' is the subfield left unchanged by θ.

Galois groups G have some general properties which can be useful in identifying them from limited information.

1. For a polynomial $P(x)$ of degree n, its Galois group is either S_n, the symmetric group on n elements, or a subgroup of S_n.

2. All Galois groups are transitive. This means that any and every element a of G can be expressed in terms of any and every other element b and a third element in the same group, c : $a = bc$ or $a = cb$.

3. The discriminant Δ of the polynomial tells whether G is A_n, the alternating group on n elements, or a subgroups of A_n. Δ is defined as the product of all the differences between pairs of roots, $\prod(\alpha_i - \alpha_j)$, $\alpha_i \neq \alpha_j$. If Δ is a perfect square, then G is either A_n or one of its subgroups. Δ can be calculated from the coefficients of $P(x)$ without knowledge of the roots (see Appendix 12).

4. Thanks to a remarkable theorem by Dedekind, the types of permutations of which G is composed can be found by factorising $P(x)$ modulo a prime p. Though $P(x)$ is irreducible over $\mathbb{Q}$, it will factorise in some prime number fields. If the degrees of the polynomial factors are d_1, d_2, ... d_k, their sum will be n, so $[d_1, d_2, ..., d_k]$ is a partition of n. The theorem states that the Galois group will have a conjugacy class whose disjoint cycles contain d_1, d_2, ..., d_k elements respectively. For instance, if n is 5 and $P(x)$ factorises modulo p as $(x^2...)(x^3...)$ so that $d_1 = 2$, $d_2 = 3$, then G contains a conjugacy class of elements with permutation type $(ab)(cde)$. Hence, factorising $P(x)$ modulo a modest number primes p will show most, if not all, of the permutation types in G.

5. Armed with the above information, on consulting tables of transitive subgroups of S_n such as the one on the final page of this document, the nature of G can become apparent, at least for small n, less than about 8 or 9. Examples of this are given in Appendix 12.

7.3 Normal and separable

These terms appear in textbooks on Galois theory.
Normal extension: Suppose $L = K(\alpha)$. 'Normal' just means that all the roots of the minimal polynomial of α lie in L. Textbooks express this as: a field extension $L : K$, $K \subset L$, is called 'normal over K' if whenever an irreducible polynomial in the ring $K[x]$ has one root in L, it also has all its other roots in L:

"One root in, all roots in".

In other words, if $P(x)$ has coefficients in K and is irreducible in K, but has one root in the extension field L, then it will split completely into linear factors in L. The term can be applied to each level in a tower of extensions, so $M : L$, $L : K$ and $K : \mathbb{Q}$ might be three normal extensions in the tower.

$\mathbb{Q}(\sqrt{2})$ is a normal extension of $\mathbb{Q}$ because it is the splitting field of the minimal polynomial $x^2 - 2$ and of the general irreducible polynomial $x^2 - 2ax + a^2 - 2b^2$, $a, b \in \mathbb{Q}$. On the other hand $L = \mathbb{Q}(\sqrt[3]{2})$ is not normal because the irreducible polynomial $x^3 - 2$ has only the real root $\sqrt[3]{2}$ in L, the other two being complex conjugates, $\frac{\sqrt[3]{2}}{2}(-1 \pm i\sqrt{3})$. A further extension adjoining $i\sqrt{3}$ is necessary to form the splitting field. Any splitting field $\mathbb{S}$ is normal by definition, but its subfields need not be so.

The word 'normal extension' is borrowed from group theory and draws parallels with a normal subgroup. The definition of normal was applied to a field extension because the Galois correspondence matches normal subgroups with normal field extensions.

Separable polynomial : A polynomial of degree n is separable if all its n roots are distinct; that is, it has no multiple (coincident) roots. Textbooks on Galois theory contain chapters on separability,

and to my mind make an unnecessary fuss about it since it comes into play only where the field has characteristic[9] p, a prime. The principal fields $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ all have characteristic 0 so are separable and no problem arises. So unless you are dealing with a finite field, you do not have to be concerned about separability.

A polynomial with $(x-\alpha_1)^2$ as a factor, $\alpha_1 \in L$, is not separable. This leads to a simple test of separability which can be applied to irreducible polynomials $P(x)$ over a finite field: see whether $P(x)$ and its derivative $P'(x)$ are coprime, since if $P(x)$ does have a factor $(x-\alpha_1)^2$, $P'(x)$ will also have $x-\alpha_1$ as a factor. Then the greatest common divisor of (P, P') will be $x-\alpha_1$, not 1.

In the case where the coefficients are in $\mathbb{Q}$, the splitting field $\mathbb{S}$ is separable if the polynomial is irreducible over $\mathbb{Q}$. Irreducible polynomials over $\mathbb{Q}$ never have multiple roots[10]. Their roots are either distinct reals or in complex conjugate pairs. Each real root must have an algebraic conjugate so that when added singly, in product pairs, in triple products, etc. and finally multiplied all together, every coefficient is rational. Duplicating any one factor would prevent cancellation and fusion of the surds.

7.4 Galois extensions

A field extension[11] is called 'Galois' if it has the property of being the splitting field $\mathbb{S}$ of an irreducible polynomial over $\mathbb{Q}$. In other words, if $P(x)$ is the polynomial under consideration and $\mathbb{S}$ its splitting field, then $\mathbb{S} : \mathbb{Q}$ is the overarching Galois extension. However, in a tower of field extensions building from up $\mathbb{Q}$ any field L will be the Galois extension $L : K$ of the embedded field K if L is the splitting field of any polynomial which has coefficients in K and has no roots in K. So the Galois concept applies to the whole tower of extensions and to each stage within it.

It is worth stressing again the paradoxical point about the correspondence between field extensions and automorphism groups – the upside-down correspondence between the field and group lattice diagrams. The Galois correspondence looks at what stays fixed in the base field under a field automorphism, not at what is moved. A large automorphism group contains many permutations so most roots α_j will be moved around and the fixed field will be small – perhaps just the identity. Conversely, a small automorphism group has small capacity to permute field elements, so most stay fixed. Since large field extensions will have the more automorphisms, large field extensions are paired with small group actions and *vice versa*. In particular the identity automorphism group $I \equiv C_1$ does not permute any elements and has the maximum fixed field, which is the whole of $\mathbb{S}$. In contrast the fixed field of the full Galois group is only $\mathbb{Q}$ since all the algebraic numbers in the extensions of $\mathbb{Q}$ are shuffled by $\mathcal{G}$. For these reasons the lattice diagrams of field extensions and of subgroups of $\mathcal{G}$ in §5 are upside down with respect to each other.

There are alternative definitions of a Galois extension $L : K$, all of which mean that is it 'well behaved':

1. L is both 'normal' and 'separable' over K. This means that if $P(x)$ is a polynomial over K, all

[9] The characteristic of a ring or field is defined as follows. Take copies of the multiplicative identity 1 and add them together and see if their sum ever equals 0, the additive identity. If they do, the ring or field is said to have characteristic N where N is the smallest number of 1s needed. If no sum ever equals 0, the characteristic is 0 (on ∞ in some older books).

[10] There is a different condition if K is a finite field since then $\mathbb{S}$ might not be separable even where the polynomial is irreducible because some numbers can have value equivalent to 0.

[11] Recall that extensions are written as $L : K$ or as L/K.

of its roots lie in L (normal condition) and all these roots are distinct (separable condition). Then $P(x)$ has n distinct roots in L where n is the degree of P.

2. L is the splitting field of a separable polynomial over K.

3. $[L : K] = |\mathcal{G}| = |\text{Gal}(L : K)|$: the degree of the field extension is equal to the order of the Galois group, that is, the number of automorphisms which leave the base field K unchanged. It happens that for any field extension, $|\mathcal{G}| \leq [L : K]$. Therefore requiring equality makes $\mathcal{G}$ as large as possible, meaning that L is as symmetric as is possible – the roots within L are as similar as possible.

4. Define $L^{\mathcal{G}}$ to be the set of elements of L which remain fixed when $\mathcal{G}$ operates on the set L. Then the equality $L^{\mathcal{G}} = K$ defines $\mathcal{G}$ to be the Galois group of the extension $L : K$.

7.5 The Correspondence Theorem

We already understand what this states. Here I will state it in general terms so that it applies to $\mathbb{Q}$ and to finite fields. However for most of the examples in this article $K = \mathbb{Q}$ and $M = \mathbb{S}$, the splitting field of $P(x)$ which is irreducible over $\mathbb{Q}$.

Consider the tower of field extensions $K \subset L_1 \subset L_2 \subset L_3 \subset M$ and the nested subgroups $I \subset H_3 \subset H_2 \subset H_1 \subset \mathcal{G}$. (Note the order-reversal.) The correspondence states that :

- there is a 1-1 correspondence between the intermediate fields L_j and the subgroups H_j of the Galois group $\mathcal{G}$,
- the correspondence is such that the sub-field L_j corresponds to the group of automorphisms $\text{Gal}(L_{j+1} : L_j)$ – that is, the permutations of L_{j+1} which leave elements of L_j invariant. (NOT the automorphisms of L_j which fix L_{j-1}),
- the subgroup H_j corresponds with the set of elements of L_{j+1} which are fixed by H_j, written $L_{j+1}^{H_j}$.
- to each normal subgroup of the Galois group corresponds a normal field extension. The order of the normal subgroup is equal to the degree of the normal field extension.

In case the subscripts are confusing I will write this again for a tower of three. Consider the field extensions $K \subset L \subset M$ and the nested subgroups $I \subset \mathcal{H} \subset \mathcal{G}$. M is not necessarily the splitting field of a given $P(x)$, but if not it will be the splitting field of some irreducible polynomial of lower degree. Then

1. there is a 1-1 correspondence between the intermediate field L and the subgroup $\mathcal{H}$ of the Galois group $\mathcal{G}$, $I \subset \mathcal{H} \subset \mathcal{G}$, $\mathcal{G} = \text{Gal}(M : L)$.

2. the correspondence is such that the subfield L corresponds to $\text{Gal}(M : L)$ – this is, the automorphisms of M which fix elements of L. (NOT the automorphisms of L which fix K), and

3. the subgroup $\mathcal{H}$ corresponds with the set of elements of M which remain unchanged by the action of $\mathcal{H}$, written $M^{\mathcal{H}}$.

Items 2 and 3 above are inverses of each other. Consequently if $L = \text{Gal}(M : L)$, then $M^{Gal(M:L)} = L$. Conversely $\mathcal{H} \to M^{\mathcal{H}}$ implies that $\text{Gal}(M : M^{\mathcal{H}}) = \mathcal{H}$.

The proof of this powerful theorem involves proving that the sizes of $\mathcal{H}$ and L are the same. The size of subgroup $\mathcal{H}$ is its order, and the size of L is taken to be the index of L in M, $[M : L]$. With this definition the size of L will equal the size of $\mathrm{Gal}(M : L)$. The proof, which I will not go into, involves proving two equalities:

1. that the order of $\mathcal{H}$ equals the index of $M^{\mathcal{H}}$ in M : $|\mathcal{H}| = [M : M^{\mathcal{H}}]$,
2. that the size of L equals the order of the Galois group of M/L : $[M : L] = |\mathrm{Gal}(M : L)|$.

8 Soluble groups, soluble polynomials

We have come at length to perhaps the main application of Galois theory, to determining which polynomials can be solved in radicals, and for these, how it can be done. It is useful to review some definitions and concepts from group theory.

8.1 Review of group theory concepts

Abelian group : A group is abelian is all its elements commute one with another: $ab = ba$ for all $a, b \in G$. All cyclic groups C_n are abelian, and all the subgroups of C_n are normal. There is an important theorem that *all* finite abelian groups can be constructed as direct products of cyclic subgroups. Stated precisely, let G be a finite group of order n with the property that, for every prime p which divides n, the Sylow p-group of G is normal[12]. Suppose also that p_1, p_2, p_3, ... p_k are the distinct primes which divide n, and let P_j denote the Sylow p_j-subgroup of g, $1 \leq j \leq k$. Then G is the direct product $P_1 \times P_2 \times ..... P_k$. So every finite abelian group is the direct product of its Sylow p-subgroups. For example, $C_{12} \simeq C_3 \times C_4$ and $C_{18} \simeq C_2 \times C_9$.

Normal and derived or commutator subgroup : A normal subgroup $\mathcal{N} \subset \mathcal{G}$ is one whose left and right cosets are set-wise identical. This can also be expressed by saying that a normal subgroup is its own conjugate. Its cosets are its conjugacy classes. Because of this its cosets are well defined. A group formed from all elements $ghg^{-1}h^{-1}$ using all $g, h \in \mathcal{G}$ is called the 'commutator' or 'derived' subgroup, and is a subgroup of every normal subgroup of $\mathcal{G}$. In an abelian group the commutator subgroup, written $[\mathcal{G}, \mathcal{G}]$, is just the identity $\{I\}$, so the larger the order of $[\mathcal{G}, \mathcal{G}]$, the further $\mathcal{G}$ is from being abelian. A 'perfect group' has $[\mathcal{G}, G] = \mathcal{G}$ itself and so is totally non-abelian.

A 'simple' group has no normal subgroups except, trivially, $\{I\}$ and itself. All cyclic groups of prime order C_p are both simple and abelian. They are therefore elementary and primary. More complicated group can in many cases be built from an assembly of these.

Quotient group : Let G be a group and N one of its normal subgroups. Its cosets are unambiguous and together they have the properties of a group, $\hat{G}$ with elements. The compound elements of $\hat{G}$ therefore each contain $|G|/|N|$ single elements of G. The cosets are equivalence classes, and each can be represented by any of the elements within it. Cosets are composed together by compounding any of their representative members and identifying the coset- product with the coset to which the product of elements belongs. The kernel of the mapping $G \to \hat{G}$ is N.; that is, N behaves as the identity of the quotient group and therefore contains I, the identity of G. The group $\hat{G}$ of compound elements is called the quotient or factor group of G by N and written $\hat{G} = G/N$.

[12] If G is a finite group with $n = Ap^m$ elements, p prime, $p \nmid A$, a Sylow p-subgroup of G is one with p^m elements – the highest power of p which divides n. In general A will be a product of other primes and each of these will have a Sylow p-subgroup.

As an example, let G be A_4, the alternating group on 4 items. It has $4!/2 = 12$ elements and is generated by the seed permutations (123) and (12)(34). It has a normal subgroup N with elements $\{I$, (12)(34), (13)(24), (14)(23)$\}$. The factor group A_4/N has three elements consisting of the three cosets of N, each of which has four members. N is one of these cosets and takes the role of the identity. The other two are

$$\{(123), (134), (142), (243)\} \quad \text{and} \quad \{(124), (132), (143), (234)\}.$$

These three cosets are isomorphic to the cyclic group C_3 of three elements, making $A_4/N \simeq C_3$. All elements have order 3. Also multiplication respects the cosets – for example (123)(123) in the second coset =(132) in the third, and (12)(34).(142) = (134).

Cyclic groups are often written as the quotient of the integers $\mathbb{Z}$ by $N\mathbb{Z}$, the latter meaning N, $2N$, $3N$, etc. Thus $\mathbb{Z}/5\mathbb{Z}$ is the integers modulo 5. These are a group of equivalence classes (also called residue classes) with representative values 0, 1, 2, 3, 4 and addition as the group operation. Some authors write $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ to emphasise that these are a representation of five equivalence classes. The group is isomorphic to C_5. Where the group operation is required to be multiplication, the value 0 must be excluded. The modified quotient group has members 1, 2, 3, 4 and is written $(\mathbb{Z}/5\mathbb{Z})^*$, the * meaning that 0 is omitted.

Normal and composition series : Given a group G, a subgroup series is an ordered set of subgroups from the single identity element in C_1 to G such that one proper subgroup fits inside the next: $\{I\} = G_0 \subset G_1 \subset G_2 \subset G_3 \subset ..... \subset G_{k-1} \subset G_k = G$. Such a series would correspond to a stepwise ascending path through a subgroup lattice. Normal and composition series are subgroup series with particular additional features.

- In a normal series, every G_j is a normal subgroup of the next one, G_{j+1} (though not necessarily normal in G or in G_{j+2}). $\{I\} = G_0 \lhd G_1 \lhd G_2 \lhd G_3 \lhd ..... \lhd G_{k-1} \lhd G_k = G$.
- In a composition series every quotient group G_{j+1}/G_j is a simple group, that is, one with no normal subgroups. The quotient groups are called composition factors of the series.

There is no need for a normal series to include all possible normal subgroups; there could be other intermediate normal subgroups which are not included. However in a composition series all intermediate subgroups are included, since if one, G_j say, were missed out, then G_{j+1}/G_{j-1} would not be simple – it would have G_j/G_{j-1} as a normal subgroup. The series is said to have maximal length. The Jordan-Hölder theorem states that if G has more than one composition series, all are isomorphic.

Conjugates : This term applies both to the roots of a polynomial and to elements of a group. There is a link through the Galois correspondence. In a field two algebraic numbers are conjugates if they are both roots the same polynomial. A normal field extension contains all the roots – all the conjugates – of some minimal polynomial. Thus $\mathbb{Q}(\sqrt[3]{2})$ is not normal because the conjugate roots $\omega\sqrt[3]{2}$ and $\omega^2\sqrt[3]{2}$ are not included, ω being a complex cube root of unity. In contrast $\mathbb{Q}(\omega, \sqrt[3]{2})$ is normal (but not $\mathbb{Q}(\omega\sqrt[3]{2})$!).

In groups, elements a and $b \in G$ are conjugate is there exists another element $q \in G$ such that $aq = qb$ or $b = q^{-1}aq$. This will happen if they lie in the left and right cosets of some subgroup N and N is normal so that left and right cosets are identical. In simpler words, they are conjugates if they are in the same coset of some normal subgroup N of G. Hence the conjugacy classes of G are cosets of one or more normal subgroups. As such they form one or more factor groups of G. A normal subgroup is also known as an invariant one because it is invariant under the conjugation operation

$q^{-1}...q$. This operation maps each $a \in G$ to some b and so shuffles the members of G. This is therefore an automorphism of G through conjugation. Such permutations are called 'inner automorphisms' and the set of inner automorphisms forms the group $\mathrm{Inn}(G)$.

The correspondence between normal field extensions and normal subgroups is that the factor group G/N by a normal subgroup N has compound elements which are the conjugacy classes of N, and a normal field extension contains all conjugates roots of some irreducible polynomial.

Transitive group : The orbit of a group element g is the set of other elements which can be reached from g by multiplying g by all other elements h_j. If the orbit of any one element encompasses the whole group, the group is 'transitive'. In general the orbits of elements will in general have different lengths and will partition the elements of G into one or more disjoint parts. If there is only one orbit in the group, the group is transitive. Clearly all cyclic groups are transitive. Transitive groups are subgroups of S_n, the symmetric group on n items. For example S_3 is transitive; the combinations below show how (12) can be reached from any of the other permutations:

$$(12) = (1)(12) = (123)(23) = (23)(132) = (13)(123) = (132)(13).$$

All Galois groups are transitive because they have elements which map any root of $P(x)$ into any other of its roots. This can be a clue to identifying candidate Galois groups when the order is known.

Dedekind's theorem : This has been stated elsewhere in this article, but is so remarkable that it is worth repeating. Let $P(x)$ have degree n and be irreducible over $\mathbb{Q}$. Take the prime p, ensure that it does not divide the discriminant of P, and factorise P mod p into a product of irreducibles, $F_1.F_2.....F_k$. Let d_j be the degree of F_j so $d_1 + d_2 + ... + d_k = n$. Then the Galois group of P contains a permutation which is the product of cycles of lengths d_1, d_2, ... d_k.

9 Solution via a resolvent polynomial of $P(x)$

Suppose the splitting field of some $P(x)$ is a simple extension of the rationals: $\mathbb{S} = \mathbb{Q}(\zeta)$. ζ is a primitive element of $\mathbb{S}$, and ζ together with its powers furnish a complete set of basis vectors for $\mathbb{S}$. Bear in mind that in general the roots of $P(x)$ will be only a small subset of the algebraic numbers in $\mathbb{S}$. There will be a minimal polynomial which ζ satisfies which we call $R(x)$, $R(\zeta) = 0$. This is given the name of the 'resolvent polynomial' of $P(x)$. It plays an important role in an algorithm for determining the Galois group of any give irreducible polynomial over $\mathbb{Q}$ without having first to find its roots.

The primitive element is discussed in §4.2 and at the end of Appendix 7. The 'primitive element theorem' states that the splitting field of any irreducible polynomial $P(x)$ with coefficients in $\mathbb{Q}$ can be written as a simple extension of $\mathbb{Q}$ with a primitive element as the adjoined algebraic number. In §2 I showed that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$, and indeed a more general linear combination $\mathbb{Q}(\sqrt{2} + m\sqrt{3})$, $m \in \mathbb{Z}$ would also serve. The resolvent polynomial is formed by considering such a linear combination V of roots α_j of the given $P(x)$: $V = m_1\alpha_1 + m_2\alpha_2 + ... + m_n\alpha_n$, and seeing what happens to V under all $n!$ permutations of the roots. The aim is to choose the set m_j so that the value of V is different for every permutation for then the splitting field of $P(x)$ is $\mathbb{Q}(V)$. The set m_j is usually found by a systematic trial-and-error search.

Some justification is needed for the assertion that $\mathbb{Q}(V)$ is the splitting field of $P(x)$ provided that $V(\alpha_1, \alpha_2, ...\alpha_n)$ takes $n!$ different values under the permutations of S_n. The splitting field is

clearly $\mathbb{S} = \mathbb{Q}(\alpha_1, \alpha_2, ...\alpha_n)$. As an arbitrary weighted sum of these roots, $V = m_1\alpha_1 + m_2\alpha_2 + ... + m_n\alpha_n$ must lie within $\mathbb{S}$. Call V_1 the value of V with the initial values of the m_h, and V_k the value of V under the permutation σ_k of the roots, so $V_1 = \{I\}V$ and $V_k = \sigma_k V = \sigma_k V_1$.

Appendix 9 contains a theorem by Lagrange which states that two polynomials $H(u)$ and $K(u)$ can be defined so that any two arbitrary polynomials, Q, R in the roots α_j of $P(x)$ have the relationship $Q_k.K(R_k) = H(R_k)$ where the subscript k denotes one of the $n!$ permutations of the n roots. A condition of the theorem is that the permutations σ_k giving Q_k, R_k all be distinct, so Q and R must have no internal symmetries.

In this theorem let $Q(\alpha_1, \alpha_2, ...\alpha_n) = \alpha_j$ for some j, $1 \le j \le n$, and let $R(\alpha_1, \alpha_2, ...\alpha_n) = V(\alpha_1, \alpha_2, ...\alpha_n)$. Lagrange's theorem states that $H(u)$ and $K(u)$ can be found so that $\alpha_j K(V_j) = H(V_j)$. Moreover, the coefficients of $H(u)$ and $K(u)$ are rational numbers which can be calculated in terms of symmetric polynomials and hence determined from the coefficients of $P(x)$ without knowing the values of its roots α_j. If $\alpha_j K(V_j) = H(V_j)$ is rearranged as $\alpha_j = H(V_j)/K(V_j)$ we see that $\alpha_j \in \mathbb{Q}(V_j) = \mathbb{Q}(V)$. This is true for every j so $\mathbb{Q}(\alpha_1, \alpha_2, ...\alpha_n) \in \mathbb{Q}(V)$. Since we have already seen that $\mathbb{Q}(V) \in \mathbb{Q}(\alpha_1, \alpha_2, ...\alpha_n)$, it follows that $\mathbb{Q}(V) \equiv \mathbb{Q}(\alpha_1, \alpha_2, ...\alpha_n)$ provided all permutations give different values of V : $V_j \ne V_k$ for $j \ne k$.

So the task is to find values of the integer weightings m which give distinct values of V under all $n!$ permutations of the roots α of the given $P(x)$. An example for a 4th degree polynomial might be $\alpha_1 - \alpha_2 + 2\alpha_3 - 2\alpha_4$, though of course this would need testing under all 24 permutations. (In fact there is a theorem that you can take $m_1 = 0$.) When we have a valid V, we have a generator for the splitting field of $P(x)$.

The literature advises that the practical way forwards is to start with the small integer values of m, alternating in sign as above, and vary them by ± 1 until an independent set of V_j is found. My guess is that if the m_j are all different, the chance of any two V_j being the same is very small. For a chosen set of m_j we form

$$\phi(u) = \prod_{1 \le j \le n!} (u - V_j).$$

A specific check for double roots in $\phi(u)$ is to differentiate it and use computational software to shown that gcd of $(\phi(u), d\phi(u)/du)$ is 1, since any double root α_k would produce a linear factor $u - \alpha_k$ as gcd. $\phi(u)$ may or may not be irreducible over $\mathbb{Q}$. If it is, it is the required resolvent polynomial of $P(x)$. If not, then any of its irreducible factor polynomials will be a resolvent polynomial of $P(x)$.

9.1 A worked example: $P(x) = x^3 - x^2 + 2x - 3$

This cubic is irreducible over the rationals. We start by assuming a linear combination of roots for V and seeing whether all permutations of it under S_3 are different. Try $m_1 = 0$, $m_2 = 1$, $m_2 = -1$ so

$$\begin{array}{llll} V_1 = (I)V = \alpha_2 - \alpha_3 & & V_4 = (12)V = \alpha_1 - \alpha_3 \\ V_2 = (123)V = \alpha_1 - \alpha_2 & & V_5 = (13)V = \alpha_2 - \alpha_1 \\ V_3 = (132)V = \alpha_3 - \alpha_1 & & V_6 = (23)V = \alpha_3 - \alpha_2\,. \end{array}$$

These are all different so this is probably a suitable choice for V. Pressing on we form $\phi(u) = (u - V_1)(u - V_2)....(u - V_6)$. This is a 6th degree polynomial in u, but the odd powers of u have coefficients 0. Now we do not know the values of the roots, but since each coefficient of $\phi(u)$ is symmetric in the roots α_j of $P(x)$, it so can be transformed into an expression in the coefficients of

$P(x)$. For this I use the algorithm in Appendix 9. I will not write out all coefficients because some are long, but

$$\text{coefficient of } u^4: \qquad 2(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 - \alpha_1^2 - \alpha_2^2 - \alpha_3^2) = 10.$$

The product polynomial is $u^6 + 10u^4 + 25u^2 + 175$ and, because it is irreducible, it is a resolvent. Its roots, of course, are $\alpha_2 - \alpha_3$, $\alpha_1 - \alpha_3$, *etc.* combining roots of the original cubic. A different resolvent will result from a different set of m_j. For instance, the set $\{1, -1, 2\}$ produces $u^6 - 4u^5 + 30u^4 - 20u^3 + 105u^2 + 416u + 1831$ whilst the set $\{1, 2, 3\}$ produces $u^6 - 12u^5 + 70u^4 - 240u^3 + 505u^2 - 612u + 499$, both of which are irreducible.

The reader may well ask how converting a cubic into a 6th order polynomial can be counted as progress, but the roots of any of these resolvents is guaranteed to be a basis for the splitting field $\mathbb{S}$ of $P(x)$. Moreover, we are guaranteed that its Galois group has order 6. It cannot be the cyclic C_6 so must be $S_3 = D_3$, the symmetric group on 3 elements which is also the dihedral group of a triangle. This conclusion has been reached without having any knowledge of the values of the roots.

By coincidence in the particular case of $m_1 = 0$, $m_2 = 1$, $m_2 = -1$ above, each V_h has the form $\alpha_i - \alpha_j$ and each has a companion which is the negative of this. Then the constant term in $\phi(u) = (u-V_1)(u-V_2)....(u-V_6)$ is $(\alpha_1-\alpha_2)^2(\alpha_2-\alpha_3)^2(\alpha_3-\alpha_1)^2$ which happens to be the discriminant Δ of $P(x)$. Its value here is $-175 = -5^2.7$. In §6.2 I showed that if Δ is a perfect square, the Galois group of $P(x)$ will be A_3, the alternating group, or one of its subgroups, but if Δ is not a perfect square, the Galois group is S_3, the symmetric group. This observation is consistent with $\phi(u)$ having degree 6.

10 Methods for determining the Galois group

The literature makes it clear that there is no single algorithm which is effective at determining the Galois group of a arbitrary $P(x)$, or of finding the field extensions which build to its splitting field. A resolvent polynomial will give the order of the Galois group, and that narrows the possibilities considerably. Moreover, if $P(x)$ is irreducible as assumed in this article, then the Galois group is 'transitive' as explained in §8 (any element can be reached from any other element by combination with a third element: $g_k = g_i.g_j$ for all j, k). Therefore the Galois group of a polynomial of degree n must be either S_n or one of its transitive subgroups. For small n there are only a few such subgroups and all have been documented. The following are transitive subgroups of S_n:

- $S_2 = C_2$,
- $S_3 = D_6$: $C_3 = A_3$,
- S_4: C_4, $C_2 \times C_2$, D_8 (dihedral, order 8), A_4 (order 12),
- S_5: C_5, D_{10} (dihedral, order 10), $\mathrm{Hol}(C_5)$=$C_5 \rtimes C_4$ (order 20), A_5 (order 60),
- S_6: C_5, S_3, D_{12}, A_4, $C_3 \times S_3$ (order 18), $C_2 \times A_4$ (order 24), S_4, A_5 S_5, A_6 and some others.

So if we have a quintic polynomial and its resolvent polynomial is $u^{20} + ...$, we know that its Galois group is $\mathrm{Hol}(C_5)$=$C_5 \rtimes C_4$.

Even when the Galois group of a general $P(x)$ has been identified, there can be considerable challenge in deducing the algebraic numbers which must be adjoined to $\mathbb{Q}$ to create its splitting field $\mathbb{S}$. However, in the following example the splitting field is readily found:

Example 1 : $P(x) = x^4 + 1$ was examined in §6 and its splitting field readily shown to be $\mathbb{Q}(i, \sqrt{2})$. We form the product polynomial $\phi(u)$ first using $m_1 = 0$, $m_2 = 1$, $m_3 = -1$ and obtain the following polynomial with degree 4!:

$$u^{24} - 80u^{20} + 7520u^{16} - 1107200u^{12} + 49475840u^8 - 344489984u^4 + 655360000$$

$$= (u^4 + 12u^2 + 100)(u^4 - 12u^2 + 100)(u^2 + 8)^2(u^2 - 8)^2(u^2 + 2)^2(u^2 - 2)^2.$$

There are two factors of degree 4 and eight of degree 2. The Galois group has degree 4. The solutions of $u^2 \pm 2 = 0$ give the intermediate field $\mathbb{Q}(\sqrt{2})$. Noting that $(1+2i)(1-2i) = 5$, $u^4 + 12u^2 + 100$ factors into a product of $u \pm (1 \pm 2i)\sqrt{2}$, it is clear that $\mathbb{S}$ is $\mathbb{Q}(i, \sqrt{2})$. If $m_1 = 1$, $m_2 = -1$, $m_3 = 2$ were used instead, the product polynomial would be

$$u^{24} - 880u^{20} + 417120u^6 - 130489600u^{12} + 17820279040u^8 - 136404393984u^4 + 268738560000$$

$$= (u^4 + 32u^2 + 400)(u^4 - 32u^2 + 400)(u^2 + 18)^2(u^2 - 18)^2(u^2 + 2)^2(u^2 - 2)^2$$

where $(1 + 3i)(1 - 3i) = 10$. This gives the same splitting field. The ability to factorise these polynomials of high degree is die to the developments of the Berlekampe and Cantor-Zassenhaus algorithms which are described in my article on factorisation in *www.mathstudio.co.uk*.

Example 2 : $P(x) = x^3 - x^2 + 2x - 3$ was our example in §9.1 above where $\phi(u)$ was found to be any of three polynomials depending on the choices of the multipliers m_1, m_2, m_3. Progress requires that $\phi(u)$ be factorised in fields which are extension of the rationals. The constant terms 1831 and 499 in two of the polynomials are not promising starting places because they are both prime, but the more symmetric choice of $m_1 = 0$, $m_2 = 1$, $m_3 = -1$ produces a constant term of $175 = 5^2.7$, so we might try two very similar cubic factors $(u^3 + au^2 + bu + i5\sqrt{7})(u^3 + cu^2 + du - i5\sqrt{7})$. This is fruitful since by equating coefficients we find $a = c = 0$, $b = d = 5$, so

$$u^6 + 10u^4 + 25u^2 + 175 \;=\; (u^3 + 5u + 5i\sqrt{7})(u^3 + 5u - 5i\sqrt{7}).$$

This is not the full splitting field, but we have at least achieved a partial factorisation in $\mathbb{Q}(i\sqrt{7})$. This factors further if $\sqrt{5}$ is adjoined:

Example 3 : $P(x) = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$. When it comes to following the above approach for a quintic or higher degree polynomial, a major problem is the vast amount of computation required to deal with the product polynomial $\phi(u)$ of degree $n!$. Even using Mathematica I made very slow progress finding the coefficients of this quintic. With the set m_j of $\{0, 1, -1, 2, -2\}$ the first few are

$$u^{120} - 1320u^{118} - 344\,086\,490\,u^{114} - 23\,196\,476\,162\,970\,u^{110} - 638\,303\,259\,949\,198\,360\,u^{106} - ...$$

and these later coefficients will be ludicrously large. I have used a different approach to gain evidence that this polynomial is in fact soluble in radical and its Galois group is the cyclic C_5. The roots involve the five fifth roots of unity and a fifth roots of a very complicated complex expression. The solution in radicals is so involved that hardly anyone would be concerned to see it written down. This seems a general point: that solutions in radicals are immensely involved and of no practical use.

11 Summary: a further worked example

To close this Part of the article is seems sensible to gather together and reinforce the concepts so far by working through another example, one that is not trivial.

Example: $P(x) = x^4 - 4x^3 + 4x^2 + 12x + 5$.

First note that the substitution $x \to x+1$ converts this to $x^4 - 2x^2 + 12x + 18$. The prime 2 divides all coefficients except the first, and 2^2 does not divide the constant term. By Eisenstein's criterion this is irreducible over $\mathbb{Q}$ and so is $P(x)$. Also the $\gcd(P, P') = 1$ so the $P(x)$ has no repeated roots, that is, it is separable over $\mathbb{Q}$.

11.1 Finding the roots

It is not necessary to find the roots of $P(x)$ to find its Galois group, but if they can be found without too much effort it does make things significantly easier later on. There is a complicated formula to solve a general quartic in radicals, but let us try a direct approach. Since any complex roots must occur in conjugate pairs, try to factorise $P(x)$ over the field $\mathbb{Q}(i)$ by seeing if coefficients can be found as follows:

$$P(x) = [x^2 + (r_1 + ir_2)x + (s_1 + is_2)]\,[x^2 + (r_1 - ir_2)x + (s_1 - is_2)].$$

Multiplying this out and equating coefficients to $P(x)$,

$$r_1 = -2, \qquad s_1 = -\tfrac{1}{2}\,r_2^2, \qquad s_2 = \frac{6 - r_2^2}{r_2}$$

and r_2^2 satisfies a cubic equation

$$(r_2^2)^3 + 4(r_2^2)^2 - 68r_2^2 + 144 = 0.$$

This has three solutions for r_2 and their negatives[13]:

$$\text{Solution 1: } r_2 = 2, \quad s_1 = -2, \quad s_2 = 1,$$

$$\text{Solution 2: } r_2 = \sqrt{2\sqrt{13} - 4)}, \quad s_1 = -\sqrt{13} + 2, \quad s_2 = 2\sqrt{\sqrt{13} - 3},$$

$$\text{Solution 3: } r_2 = i\sqrt{2\sqrt{13} + 4)}, \quad s_1 = \sqrt{13} + 2, \quad s_2 = -2i\sqrt{\sqrt{13} + 3}.$$

These give three distinct factorisations of $P(x)$ in intermediate fields. Solution 1 gives

$$P(x) = [x^2 - 2(1-i)x - (2-i)]\,[x^2 - 2(1+i)x - (2+i)]. \tag{10}$$

This is in the field extension $\mathbb{Q}(i)$ as intended. Having reduced the quartic to two similar quadratics, a linear decomposition is readily found:

$$x^2 - 2(1-i)x - (2-i) = 0 \text{ when } x = 1 - i \pm \sqrt{2 - 3i}, \quad x^2 - 2(1+i)x - (2+i) = 0 \text{ when } x = 1 + i \pm \sqrt{2 + 3i}.$$

These are the four roots of $P(x) = 0$. Their numerical values are $2\cdot674 \pm 1\cdot896i$, $-0\cdot674 \pm 0\cdot104i$. In working with these it is convenient to introduce some simplifying notation:

$$B = \sqrt{2 + 3i} = A + i\hat{A}, \qquad B^* = \sqrt{2 - 3i} = A - i\hat{A}, \qquad A = \sqrt{\tfrac{\sqrt{13}}{2} + 1}, \quad \hat{A} = \sqrt{\tfrac{\sqrt{13}}{2} - 1}, \quad A\hat{A} = \tfrac{3}{2}.$$

[13] Note that $(\sqrt{13} - 1)\sqrt{\sqrt{13} - 2} = (5 - \sqrt{13})\sqrt{\sqrt{13} + 2}$ as the square of each is $18\sqrt{13} - 54$.

where * denotes the complex conjugate. Label the roots in anticlockwise order around the origin:

$$\alpha_1 = 1 + i + A + i\hat{A}, \quad \alpha_2 = 1 + i - A - i\hat{A}, \quad \alpha_3 = 1 - i - A + i\hat{A}, \quad \alpha_4 = 1 - i + A - i\hat{A}, \qquad (11)$$

so $\alpha_4 = \alpha_1^*$, $\alpha_3 = \alpha_2^*$. The roots are algebraic numbers in the splitting field $\mathbb{Q}(i, A)$.

Solutions 2 and 3 yield two more factorisations in intermediate fields. Solution 2 gives quadratic factors in $\mathbb{Q}(i\hat{A})$ and Solution 3 ones in $\mathbb{Q}(A)$, the latter being over the real numbers. To be specific, the quadratic factorisation with Solution 3 is the rather unwieldy

$$P(x) \;=\; [x^2 - 2(A+1)x + C]\,[x^2 + 2(A-1)x + \hat{C}]$$

$$C \;=\; 2 + \sqrt{13} + 2\sqrt{3 + \sqrt{13}}, \qquad \hat{C} = 2 + \sqrt{13} - 2\sqrt{3 + \sqrt{13}}].$$

It happens that $C = \alpha_1\alpha_4$, $\hat{C} = \alpha_2\alpha_3$. The solution to $x^2 - 2(A+1)x + C = 0$ is $x = 1 \pm i + \sqrt{2 \pm 3i}$ (*i.e.* $\alpha_1 = 1 + i + B$, $\alpha_4 = 1 - i + \hat{B}$) in agreement with Solution 1.

From this we can be sure that the splitting field $\mathbb{S}$ has degree 8. Sets of 8 linearly independent basis vectors can be written in terms of A or B

$$\{\ 1,\ \ i,\ \ \sqrt{13},\ \ i\sqrt{13},\ \ \ A,\ \ iA,\ \ \hat{A},\ \ i\hat{A}\ \}, \qquad (12a)$$

$$\{\ 1,\ \ i,\ \ \sqrt{13},\ \ i\sqrt{13},\ \ B,\ \ iB,\ \ B^*,\ \ iB^*\ \}. \qquad (12b)$$

11.2 Roots using the resolvent

Further confirmation of the degree of $\mathbb{S}$ comes from the 'resolvent' of $P(x)$. This was explained in §9, but in essence we form a linear combination of the roots $V = m_1\alpha_1 + m_2\alpha_2 + m_3\alpha_3 + m_4\alpha_4$. This can be done symbolically, without having to know their values. Now operate on V with all $n! = 4! = 24$ possible permutations of the roots α_j. Let V_j denote the result of the permutation σ_j on V, and form the product

$$\phi(u) \;=\; \prod_{1\le j\le 24} (u - V_j), \qquad V_j = \sigma_j(V). \qquad (13)$$

Expand this into a polynomial of degree 24 in u. All its coefficients are real because every one is symmetrical in all the indices. If the roots are known, $\phi(u)$ can be calculated directly. If they are not, the coefficients of $\phi(u)$ can be found from the coefficients of $P(x)$ using the links between them in terms of the elementary symmetrical polynomials. I quote two cases applied to our $P(x)$. For the weightings $m_1 = 0$, $m_2 = 1$, $m_3 = -1$, $m_4 = 2$ the effect of permutation (12)(34) on V would be $\alpha_1 - \alpha_4 + 2\alpha_3$. Forming the product over all such permutations, $\phi(u)$ is the enormous polynomial

$$\phi(u) \;=\; u^{24} - 48u^{23} + 1024u^{22} - 12672u^{21} + 97392u^{20} - 426368u^{19} + 329984u^{18} + 7907328u^{17} - 38089632u^{16}$$

$$- 103582720u^{15} + 2185411584u^{14} - 14184312832u^{13} + 59457783552u^{12} - 169041045504u^{11} + 176783323136u^{10}$$

$$+ 1315097509888u^9 - 4942034894592u^8 - 36584376766464u^7 + 465967916269568u^6 - 2496268391645184u^5$$

$$+ 10802960426074112u^4 - 38314850302033920u^3 + 104696438279110656u^2$$

$$- 175966655950618624u + 152361615600123904$$

Galois theory would be stuck at this point if it were not for the powerful algorithms which have been developed since 1960 for the rapid computer factorisation of this and larger polynomials. I have given an account of the algebraic and number theory background to the Distinct Degree,

Berlekamp and Cantor-Zassenhaus algorithms in a companion article[14] on *ww.mathstudio.co.uk*. The above factorises into three 8th degree irreducible polynomials:

$$(u^8 - 16u^7 + 160u^6 - 1024u^5 + 5272u^4 - 19648u^3 + 73856u^2 - 171008u + 264848)\times$$

$$(u^8 - 16u^7 + 64u^6 + 128u^5 - 2048u^4 + 8192u^3 + 57344u^2 - 278528u + 475136)\times$$

$$(u^8 - 16u^7 + 32u^6 + 512u^5 - 1064u^4 - 9920u^3 + 4736u^2 + 93184u + 1210768).$$

The degree of these irreducible factors is the degree of the splitting field $\mathbb{S}$ of $P(x)$.

Each of these three has roots which can generate the whole of $\mathbb{S}$. To illustrate this, the third factor can be shown to have roots $2 \pm \sqrt{2}.\sqrt{10 \pm 12i \pm 3\sqrt{13}}$. These are nearly identical, clearly illustrating the point made in §2 about roots being highly similar so that radicals combine or cancel to leave only rational coefficients. All of its 8 roots are equivalent – conjugate – in this regard. A primitive element for the splitting field is $h = \sqrt{10 + 12i + 3\sqrt{13}}$. It is possible to express any element in $\mathbb{S}$ as a linear combination of the powers of this algebraic number, the weighting factors being rationals. Three examples are

$$i = \tfrac{1}{6264}(-4150 + 615h^2 - 20h^4 + h^6), \quad \sqrt{13} = -\tfrac{1}{1566}(1070 + 93h^3 - 30h^4 + h^6),$$

$$i\sqrt{13} = \tfrac{1}{72}(127 - 20h^2 + h^4).$$

With an alternative choice of weightings, $m_1 = 0$, $m_2 = 1$, $m_3 = -1$, $m_4 = 0$, we obtain a simpler resolvent which again factorises and produces a degree 8 irreducible polynomial :

$$\phi(u) = u^{24} - 32u^{22} + 720u^{20} - 1536u^{18} - 136608u^{16} + 4285440u^{14} - 35674368u^{12} + 35880960u^{10}$$

$$+ 6390911232u^8 - 66210504704u^6 + 473107505152u^4 + 41328967680u^2 + 897122304$$

$$= (u^8 + 24u^4 + 3328u^2 + 144)^2\,(u^4 - 16u^2 + 208)^2.$$

This is more manageable. Solving the quadratic in u^2, $u^4 - 16u^2 + 208 = 0$ gives $u = \pm 2\sqrt{2 \pm 3i}$, whilst solving the polynomial in u^8 gives $u = i\hat{A}$ as one root, so the same radicals are reappearing. By this stage we have a good understanding of the roots of $P(x)$, its splitting field $\mathbb{S}$, and three of the subfields into which $P(x)$ factorises.

11.3 Galois group

Since $\mathbb{S}$ in our example has degree 8, there are exactly 8 permutations of the roots α_j, $1 \le j \le 4$ which leave $P(x)$ unchanged. To guide our investigation of what these are, we note that there are only five groups of order 8. There are 4! = 24 permutations of the four roots, but the task now is to identify those eight which leave the field of rational numbers unchanged. In its splitting field $P(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)$, $\alpha_4 = \alpha_1^*$, $\alpha_3 = \alpha_2^*$. Clearly any permutation of the four roots will leave this unchanged. We need to look at how permutations affect polynomials of lower degree than $P(x)$ because these sit in the subfields of $\mathbb{S}$. Some such permutations can be identified readily; complex conjugation is one. This simultaneously maps $\alpha_1 \leftrightarrow \alpha_4$ and $\alpha_2 \leftrightarrow \alpha_3$, so permutation of the indices is (14)(23). Now choose some partially symmetric combinations of roots and see what happens to them under S_4. Three simple choices are

$$\alpha_1 + \alpha_2 = 2 + 2i, \qquad \alpha_3 + \alpha_4 = 2 - 2i \quad \text{so} \quad (\alpha_1 + \alpha_2) = (\alpha_3 + \alpha_4)^*,$$

[14] 'Factorising Polynomials: a background to some algorithms'.

$$\alpha_1\alpha_2 = -2 - i, \qquad \alpha_3\alpha_4 = -2 + i \quad \text{so} \quad (\alpha_1\alpha_2) = (\alpha_3\alpha_4)^*, \tag{14}$$
$$\alpha_1\alpha_2 + \alpha_3\alpha_4 = -4.$$

It is obvious that swapping $\alpha_1 \leftrightarrow \alpha_2$ and $\alpha_3 \leftrightarrow \alpha_4$ together leaves these relations unchanged, so permutation (12)(34) is also within the Galois group. We might call this 'algebraic conjugation' since it swaps A for $-A$, $\hat{A}$ for $-\hat{A}$. (13)(24) is also within $\mathcal{G}$ since

$$(13)(24)(\alpha_1 + \alpha_2) = \alpha_3 + \alpha_4 = (\alpha_1 + \alpha_2)^* = [(13)(24)(\alpha_3 + \alpha_4)]^*$$

showing that the complex conjugate relation is retained. The three permutations (12)(34), (13)(24), (14)(23) together with the identity $I = ()$ form a Klein-V subgroup, $C_2 \times C_2$, of $\mathcal{G}$.

A different combination is $\alpha_1\alpha_3 = (\alpha_2\alpha_4)^*$ and this conjugate relation is preserved by (13) alone, by (24) alone, and by the 4-cycle (1234) and its inverse (1432). In contrast (123) respects none of these relations. The permutations identified so far generate the whole group D_8, the dihedral group which describes the symmetries of a square. We conclude that the Galois group of $x^4-4x^3+4x^2+12x+5$ is D_8. These invariant algebraic relations on partially symmetric combinations of the roots of $P(x)$ are closely related to the intermediate field extensions of $\mathbb{Q}$ in which $P(x)$ will factorise.

Galois groups are all transitive, meaning that every and any group element can be mapped to any other element by multiplication by a third group element. With our choice of $P(x)$ this fact does not help reduce the search since all groups of order 8 are transitive. However for other degrees this is not necessarily the case, and limiting the search only to transitive groups can be a significant saving. There is a beautiful and intriguing 19th century theorem by Richard Dedekind and Georg Frobenius which states that the types of permutation within the Galois group are closely related to how $P(x)$ factorises modulo a prime number. This is illustrated in Appendix 10. Here we just note that it supports the diagnosis as D_8.

11.4 Lattice diagrams

The next stage is to construct the lattice diagrams of the extension field and the Galois group. Since the structure of D_8 is well known, it will point to the structure of the subfields of $\mathbb{S}$ and hence to the intermediate factorisations of $P(x)$. The elements of D_8 can be regarded as permutations as above, or the group can be thought of as being generated by two elements s and t of order 4 and 2 respectively, together with the relation $ts = s^{-1}t$. If the roots actually formed the corners of a square instead of a trapezium in the complex plane, s would correspond to a rotation by one right-angle and $t$to reflection in the real axis. The following matches can be made between the permutations and the operations s and t, in which t is complex conjugation:

()	(1234)	(13)(24)	(1432)	(14)(23)	(24)	(12)(34)	(13)
I	s	s^2	s^3	t	st	s^2t	s^3t

The left panel of Figure 2 is a lattice diagram giving the subgroup structure of D_8 in terms of s and t. The splitting field $\mathbb{S}$ is $\mathbb{Q}(i, A) = \mathbb{Q}(i + A)$. To match the left-hand lattice to the equivalent lattice of subfields we ask "Which subfields remain unchanged when one of these subgroups operates on the roots of $P(x)$?". The easiest case is t which, being complex conjugation, leaves the real parts of the roots unchanged so the invariant subfield corresponding to subgroup $\{I, t\}$ is $\mathbb{Q}(A) \equiv \mathbb{Q}(\hat{A})$ because $1/\hat{A} = 2A/3$. $\mathbb{Q}(A)$ has degree 4 and a basis $\{I, A, \sqrt{13}, \hat{A}\}$.

Dealing with most of the other subgroups requires a more systematic approach. A general element in $\mathbb{S}$ will be some linear combination of the basis vectors at Eq 10a, b. These vectors can be

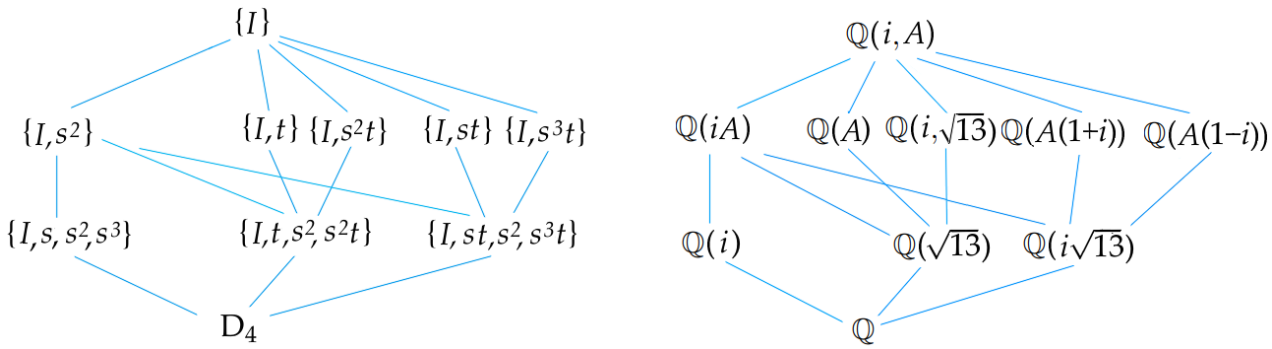

Figure 8: Lattice structure of dihedral group D_8 compared with the subfields of $x^4-4x^3+4x^2+12x+5$.

expressed in terms of the four roots, and that allows the effect of permuting the roots on each base vector to be calculated.

$$i = \tfrac{1}{2}(\alpha_1+\alpha_2)-1 = 1-\tfrac{1}{2}(\alpha_4+\alpha_3) = \tfrac{1}{4}(\alpha_1+\alpha_2-\alpha_3-\alpha_4),$$

$$\sqrt{13} = \tfrac{1}{4}(\alpha_1-\alpha_2)(\alpha_4-\alpha_3),$$

$$i\sqrt{13} = \tfrac{1}{16}(\alpha_1-\alpha_2)(\alpha_4-\alpha_3)(\alpha_1+\alpha_2-\alpha_3-\alpha_4)$$

$$B = \tfrac{1}{2}(\alpha_1-\alpha_2)$$

$$B^* = \tfrac{1}{2}(\alpha_4-\alpha_3)$$

$$iB = \tfrac{1}{8}(\alpha_1+\alpha_2-\alpha_3-\alpha_4)(\alpha_1-\alpha_2)$$

$$iB^* = \tfrac{1}{8}(\alpha_1+\alpha_2-\alpha_3-\alpha_4)(\alpha_4-\alpha_3)$$

$$A = \tfrac{1}{2}(\alpha_1+\alpha_4)-1 = 1-\tfrac{1}{2}(\alpha_2+\alpha_3) = \tfrac{1}{4}(\alpha_1-\alpha_2-\alpha_3+\alpha_4)$$

$$iA = = \tfrac{1}{16}(\alpha_1+\alpha_2-\alpha_3-\alpha_4)(\alpha_1-\alpha_2-\alpha_3+\alpha_4)$$

$$\hat{A} = = -\tfrac{1}{16}(\alpha_1+\alpha_2-\alpha_3-\alpha_4)(\alpha_1-\alpha_2+\alpha_3-\alpha_4)$$

$$i\hat{A} = \tfrac{1}{2}(\alpha_1+\alpha_3)-1 = 1-\tfrac{1}{2}(\alpha_2+\alpha_4) = \tfrac{1}{4}(\alpha_1-\alpha_2+\alpha_3-\alpha_4).$$

We can be guided by the degree of these base vectors. A subgroup of order 2 should fix a subfield of degree $8/2 = 4$, and a subgroup of order 4 should fix a subfield of degree $8/4 = 2$. Therefore the field extensions $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{13})$ and $\mathbb{Q}(i\sqrt{13})$, all of degree 2, must correspond with subgroups of order 4. These are the cyclic group generated by $(1234) = \{I, s, s^2, s^3\}$, and the two Klein-V groups $\{I, t, s^2, s^2t\}$ and $\{I, st, s^2, s^3t\}$. Of the degree-4 field extensions there are $\mathbb{Q}(i, \sqrt{13})$, $\mathbb{Q}(A) \equiv \mathbb{Q}(\hat{A})$ and $\mathbb{Q}(iA) \equiv \mathbb{Q}(i\hat{A})$. However, five are needed to complete the diagram. This suggests that some combination of base vectors may be involved in these other two subfields.

Let us identify s^2. Being the square of (1234), it is (13)(24). Both (13) and (24) swap $A \leftrightarrow -A$ and simultaneously $i \leftrightarrow -i$, so applying them together as (13)(24) leaves iA unchanged. So $s^2 \equiv (13)(24)$ corresponds with $\mathbb{Q}(iA)$. The table gives the consequences of applying each of the

permutations of D_8 to the base vectors listed above:

$I = ()$	(1234)	(1432)	$(13)(24)$	$(14)(23)$	$(12)(34)$	(24)	(13)
i	$-A$	A	$-i$	$-i$	i	A	$-A$
$\sqrt{13}$	λ	λ	$\sqrt{13}$	$\sqrt{13}$	$\sqrt{13}$	λ	λ
$i\sqrt{13}$	μ	$-\mu$	$-i\sqrt{13}$	$-i\sqrt{13}$	$i\sqrt{13}$	$-\mu$	$-\mu$
A	i	$-i$	$-A$	A	$-A$	i	$-i$
iA	$-iA$	$-iA$	iA	$-iA$	$-iA$	iA	iA
$\hat{A}$	$-\frac{3}{2}i$	$\frac{3}{2}i$	$-\hat{A}$	$\hat{A}$	$-\hat{A}$	$-\frac{3}{2}i$	$\frac{3}{2}i$
$i\hat{A}$	$-i\hat{A}$	$-i\hat{A}$	$i\hat{A}$	$-i\hat{A}$	$-i\hat{A}$	$i\hat{A}$	$i\hat{A}$

$\lambda = \frac{1}{2}(\sqrt{13} - 4)$, $\mu = \sqrt{\frac{13\sqrt{13}-46}{8}}$. These show the following invariant vectors:

- (1234) and (1432) are cyclic relabellings of the four roots so leave $P(x)$ unchanged. They are identity permutations.
- $(13)(24)$ fixes $\sqrt{13}$, iA and $i\hat{A}$,
- $(14)(23)$ fixes $\sqrt{13}$, A and $\hat{A}$,
- $(12)(34)$ fixes i and $\sqrt{13}$,
- (24) fixes $(A + i)$, iA, $i\hat{A}$,
- (13) fixes iA, $i\hat{A}$.

The overlap of $(14)(23)$ and $(12)(34)$ at $\sqrt{13}$ strongly suggest that the subgroup $\{I, t, s^2, s^2t\}$ corresponds with $\mathbb{Q}(\sqrt{13})$.

A further device which can be used is to invent a polynomial in the roots which is designed to be invariant only to a particular permutation. For instance $\alpha_1\alpha_3^2 + \alpha_3\alpha_1^2$ is invariant to (13), but would change under (12), (14), (23) and (1234) though not under (24). However $\alpha_1\alpha_3^2 + \alpha_3\alpha_1^2 + \alpha_2 - \alpha_4$ distinguishes even (24).

The form of A is consistent with it being unchanged by permutation $(14)(23)$ which was identified above with t. Similarly $i\hat{A}$ is readily identified with $(13)(24) = s^2$. However, unambiguously identifying most of the other subfields can be tricky. For instance, it would be tempting to identify the fixed field $\mathbb{Q}(i)$ with $(12)(34) = s^2t$, but the degree $[\mathbb{Q} : \mathbb{Q}(i)] = 2$, whereas a permutation of order 2 should fix a field of order $8/2 = 4$. $\sqrt{13}$ would seem to be fixed by $(14)(23) = s^2$, but we have already matched that with $\mathbb{Q}(A)$.

We proceed in this manner to identify other subfields fixed by the various subgroups. The reader may care to check my identification of subfields. Each blue line linking nested subfields implies a degree or order of 2. It becomes clear that the two lattice diagrams are the same apart from being inverted, the larger subgroup fixing the smaller subfield. This is as we would expect since a group with many operations will permute more field elements than one with few.

Part III
Solving general polynomials in radicals

This Part of my article is incomplete. I had intended to write a survey of computational methods for finding the Galois group of any given polynomial and hence finding its roots in radicals where such roots exist. This has proved an involved task and there are several partial reviews already on the internet. I may i n due course pick up this topic again.

All the examples given in Part II above started from a knowledge of the roots of the polynomial in radicals. This is fine for demonstrating the Galois Correspondence, but not much use practically since there is no general way to find the roots of a quintic or higher equation in radicals. This section deal with the mathematical detective work by which is is possible to deduce the Galois group from the coefficients of the given $P(x)$ alone. This is a complicated problem and much ingenuity has been brought to bear on it by mathematicians over many decades. Several approaches have been followed, but some are of little practical use for higher degree polynomials because they require the factorisation of associated polynomials with very high degree. Another approach is to use the numerical values of the roots – quite readily found by Newton's method – to deduce what their algebraic form must be. Appendix 10 explains some theorems by Dedekind and others which help identify Galois groups from their cycle types. Once the Galois group has been determined, there is still the problem of solving $P(x)$ in radicals where this is possible. This requires us to infer the field extensions associated with each subgroup of the Galois group of the splitting field.

12 Symbolic computer calculations in Galois theory

The examples given in the body of this article, and indeed in almost all textbooks, explain how the Galois group pf a polynomial can be found once the roots are known explicitly as algebraic numbers. This, of course, is a very contrived situation, useful mostly just for demonstrating the theory. The real test of Galois theory is whether it can be applied to general polynomials whose roots are unknown. It is not difficult to see that this is a very challenging problem since we have almost nothing to go on. All we have is a monic polynomial of degree n with its n coefficients. It may be possible to show that it is irreducible over the rationals using Eisenstein's tests. My reading of the literature on this subject, in so far as I can understand it, leads to the view that many mathematicians have worked for years to find efficient algorithms for determining tha Galois group for polynomials of degree greater than 4. The subject has been reviewed by Alexander Hulpke. The subject was dormant for decades until computers and symbolic manipulation software became available after about 1980. Many algorithms have been studied and the few available implementations seem to use hybrids of these.

The literature states that Galois packages are available on the specialist software platforms PARI (French), KANT (German) and GAP. A challenge in using any of these is setting up the software and learning the coding and syntax. A further challenge is interpreting the output. Hulpke explains that it is impractical to determine the Galois group as a set of its elements, partly because the group can be so large. Moreover, it may not be possible to determine all the elements of the Galois group; instead it is determined as far as its conjugacy classes or some other aggregated characterisation. Some algorithms seem to approach the problem by starting from the fact that the Galois group could be S_n, the symmetric group, and then using various tests and conditions to eliminate sets of elements until only the Galois group is left. With some polynomials the problem may be reduced only to the point of saying that the Galois group could be one of a few possibilities.

12.1 Mathematica

It is disappointing that Mathematica does not have an effective Galois package for polynomials over $\mathbb{Q}$. There was a notebook written by William Paulsen in 1999 for Mathematica 3, but it seems not to have been updated and is not officially supported. Maxima has a Galois package written by the Japanese mathematician Yasuaki Honda using an algorithm set out by Keita Ibuki in an internet blog. For English speaking users the difficulty presents itself that the supporting documentation is in Japanese and quality translations are not available, though on-line translation software tries its best. The ReadMe note gives this information:

> There are two goals achieved in this package:
>
> - To determine if a given polynomial is solvable by radicals or not
> - If it is solvable, then to compute the radical solutions based on the Galois Group and Field theory
>
> **Mathematical background and description**
> Galois theory developed by Evariste Galois says that if a Galois group of a given polynomial is a solvable group, then the polynomial is solvable by radicals. To determine if a given polynomial is solvable or not, we need to do the followings:
>
> - Compute a Galois group of a given polynomial,
> - Compute a series of normal subgroups of the Galois group,
> - Compute quotients of degree of a normal subgroup in the series and its descent subgroup. If all quotients are primes, then the Galois group is solvable.
>
> For a solvable polynomial we perform the following computation according to the computed series of normal subgroups of the Galois group:
>
> 1. Starting from Q as the initial coefficient field of the given polynomial, we compute a radical to add to the coefficient field to obtain the extended field (Galois theory's conclusion on correspondence between subnormal groups reduction and normal extension of fields).
> 2. The above step will be repeated so that the Galois group is reduced to the trivial group, thus we obtain a splitting field of a given polynomial.
> 3. The obtained splitting field is a extensions of Q by radicals.
>
> Along with computing the Galois group, we also compute a minimal polynomial of V where V is a primitive element that extends Q to the splitting field. As the Galois group is reduced and the coefficient field is extended, the minimal polynomial of V is factored into a lower degree polynomial. When the Galois group is reduced to the trivial group thus Q is extended to the splitting field, the minimal polynomial of V becomes a linear so that V is represented in terms of radicals. Finally, we compute solutions of the original polynomial from V based on the formulae obtained in the computing of Galois group.

John Coffey, September 2022

Part IV
Appendices

Appendix 1: Algebraic numbers

In this appendix I jot some musings on algebraic numbers, which seem to me to be elusive quantities.

Any number α which is the root of a polynomial equation $P(x) = 0$ with fractional coefficients is an algebraic number. Strictly we should say that α is 'algebraic over $\mathbb{Q}$'. The term does not usually include the rationals themselves, but rather all numbers involving roots of positive and negative rational numbers, and roots of these roots nested to any depth. In addition there exist more complex functions of the coefficients of the polynomial which we might call 'hyper-radical' algebraic numbers. In fact any number which satisfies a polynomial equation whose coefficients are algebraic numbers is also an algebraic number, as proved in Hardy's book on pure mathematics[15]. The algebraic numbers are countably infinite and dense in the reals (like the rationals themselves), meaning that there is at least one algebraic number within a distance ε of any given real number, no matter how small we specify $\varepsilon > 0$ to be.

As they are the roots of polynomial equations of finite degree, we might wonder whether *all* algebraic numbers must have a form which could in principle be written as some complicated combination of radicals, if only that form were known. It is fair to ask whether Galois theory proves that this form in radicals does exist, not just that an algorithm cannot be discovered. There is certainly an inverse process of first specifying an algebraic number in terms of radicals then finding its minimum polynomial. For example, the real conjugate pair $\alpha_\pm = \sqrt[3]{2} \pm \sqrt{3}$ have minimum polynomial $P = x^6 - 9x^4 - 4x^3 + 27x^2 - 36x - 23$ even though $\alpha_\pm$ cannot be recovered by solving $P = 0$ using any recognised algorithm. In principle, since it does have two radical roots, it should be possible to find its Galois group and hence a chain of normal subgroups which indicate a means of solution. So if P has solutions in radicals, admittedly of simple form, what about the similar irreducible polynomial $Q = x^6 - 10x^4 - 4x^3 + 27x^2 - 36x - 25$? The answer is that the Galois group of the two polynomials are of different kinds, the first soluble, the second not. Where the Galois group is not soluble, no solution in radicals exists – not just that there is not algorithm for finding it. So the only analytic way of expressing its roots is in terms of the horrendously complicated elliptic modular functions or by merely stating that they are the roots of such-and-such a polynomial.

Where maths is applied to physics and engineering, quadratic equations are far more common that cubic and higher order ones. With quadratic calculations it is common and convenient to retain the $\sqrt{\cdot}$ notation. But for practical numerical work the roots are soon converted to decimals correct to a few significant figures. Eq 1 on the first page of this article is the familiar formula guaranteed to give both roots of any quadratic in terms of a square root and possibly $i = \sqrt{-1}$. But what does, say, $\sqrt{5}$ really mean? It is an elementary algebraic number which

- is defined only by the equation which it solves,
- is represented by a point on the real number line whose position we can locate between two close rational numbers, or as a decimal approximation to any required degree of accuracy, $\sqrt{5} = 2 \cdot 23606797.....$

[15] G H Hardy, 'A course in Pre Mathematics', 10th edition, p38, 39, CUP, 1952.

As a continued fraction $\sqrt{5} = \{\{2 : 4, 4, 4, 4, 4, ...\}\}$ with convergents

$$\frac{9}{4}, \quad \frac{38}{17}, \quad \frac{161}{72}, \quad \frac{682}{305} \approx 2 \cdot 236066, \quad .....$$

These alternate around their limiting value and so converge on the algebraic number from above and below. We might say that a square root is alternatively defined by a number whose continued fraction recurs, but there is no direct way to multiply a continued fraction by itself to show that its square equals an integer. Numbers which are not square roots do not recur as continued fractions. As a decimal any algebraic number will almost certainly be non-recurring and of infinite length. Even if we could write down a decimal of infinite length, I see no way of telling whether it is algebraic or, more likely, transcendental. It was a major feat of 19th century mathematics to prove that π is not algebraic.

I have searched mathematical tables looking for expressions other than polynomials which evaluate to an algebraic number. The only two I found are for square roots:

$$\prod_{k=1}^{\infty} \left(1 + \frac{(-1)^{k+1}}{2k-1}\right) = \sqrt{2},$$

$$\lim_{k\to\infty} \frac{2.4.6.8.....2kN}{1.3.5.....(2kN-1)} \cdot \frac{1.3.5....(2k-1)}{2.4.6.8.....2k} = \sqrt{N}.$$

The infinite product is on page 12 of the tables of series and products by Gradshteyn and Ryzhik who attribute it to Euler in his astounding two-volume 'Introductio in Analysin Infinitorum', 1748. The second expression with the limit sign is problem 10 on page 104 of the book on infinite series by T. J. l'A Bromwich, 1907. I have proved these relations and given my working as Q29 in the Problems and Puzzles page of *www.mathstudio.co.uk*.

Though a general cubic equation can be solved in radicals, it would be quite unusual to do so and retain the solution in subsequent calculations. For most practical work a numerical solution is much more useful. This applies even more so to a quartic unless it happens to be a quadratic in x^2. The formula found by the 16th century Italian mathematicians is almost useless. Here, for example, are the three roots of $x^3 + 2x^2 + 5 = 0$, depending on how complex cube roots are taken:

$$\frac{1}{3}\left\{\sqrt[3]{\frac{1}{2}(-151 + 3\sqrt{2505}\,)} + \sqrt[3]{\frac{1}{2}(-151 - 3\sqrt{2505}\,)} - 2\right\}.$$

Algebraically this is totally unwieldy, but its numerical value is readily found by Newton's method and simply stated: about $-2 \cdot 690647$. See Appendix 3 for the derivation of this monstrous formula.

The possibility occurred to several 19th century mathematicians that there might exist functions with higher complexity than nth roots which would solve the general quintic equation, and even the 6th and ones of higher degree. A modern rediscovery of work of Hermite, Gordan, Jordan, Kiepert and others on hyper-radical functions has been summarised in the book 'Beyond the Quartic Equation' by R. Bruce King[16], a professor of inorganic chemistry at the University of Georgia who had deep experience of molecules with the 3D geometry of platonic solids. Hermite had shown that the general quintic can be solved in terms of elliptic functions, the computation of which is eased by using theta functions. Moreover Jordan in 1870 published a paper showing that any algebraic equation can be solved using modular functions. King became so interested in this that he worked

[16] Published by Birkhäuser, 1996.

with a computer scientist to develop a multi-stage algorithm for solving the general quintic in elliptic functions and coded it for computer evaluation.

To me algebraic numbers remain elusive, rather mysterious quantities, and Galois theory seems of more intrinsic and esoteric interest as a branch of algebra than of practical value.

Algebraic closure of a field: This topic is dealt with in some texts on Galois theory, though others do not regard it as essential. Algebraic closure is a generalisation of the concept of a splitting field of a given polynomial with coefficients in K to a much larger field in which *every* polynomial over K splits into linear factors. Thus the algebraic closure of a field K is an extension of K in which every polynomial $f(x) \in K[x]$ has all its roots. The algebraic closure field of K is unique and denoted $\overline{K}$. Clearly $\overline{K}$ could in principle be constructed by adjoining all the roots of all polynomials in $K[x]$. However, its construction can be thought of as a step by step process. Conceptually we list all polynomials in $K[x]$ in order and extend K by adding those roots of $p_1(x)$, $p_2(x)$, $p_3(x)$, ... which are required to form the splitting fields of $p_1(x)$, $p_2(x)$, $p_3(x)$, ... to infinity. Moreover, any polynomial with coefficients in $\overline{K}[x]$ also has its roots in $\overline{K}$, meaning that the algebraic closure of K is itself algebraically closed – a condition we might well have hoped to be true. As an example, by the fundamental theorem of algebra $\mathbb{C}$ is closed and $\overline{\mathbb{R}} = \mathbb{C}$. Similarly the algebraic numbers are the closure of the rationals, $\overline{\mathbb{Q}}$. The purpose of algebraic closure seems to be to give mathematicians comfort that every polynomial over the rationals does indeed have a splitting field. However the Fundamental Theorem of Algebra tells us that *every* equation splits in $\mathbb{Q}$, so the fact that there may be a smaller field of algebraic numbers, $\mathbb{A}$, somewhere between $\mathbb{Q}$ and $\mathbb{C}$, in which all polynomials over $\mathbb{Q}$ split into linear factors seems more of philosophical interest than practical consequence.

Appendix 2: Solution of quadratics by geometrical construction

The ancients would have understood positive and negative integers in the sense of money credit and debt, but to them all lengths were positive. Hence the quadratic equation $ax^2 + bx + c = 0$ could involve only positive roots. If the symbols a and x were understood to be lengths, this equation would be a statement about volumes of solids. b would be an area and c a volume. Dividing by a means setting the thickness of these solids to unity and the resulting equation is then about their sectional areas over the other two dimensions. The reduced equation is $x^2 + px + q = 0$. There are several sets of conditions on the pair p, q which will give either 1 or 2 positive roots and we assume that one of these is satisfied.

An example of the sort of question involving a quadratic which the ancients might have asked is that of finding the Golden Section: the shape of the aesthetically pleasing architectural rectangle which has sides 1 and G, $G > 1$, such that the ratio of length to semi-perimeter equals the ratio of the two sides:

$$G : 1 \text{ as } G + 1 : G \quad \text{from which} \quad G^2 - G - 1 = 0\,.$$

This has one positive and hence meaningful solution: $G = \frac{1}{2}(1 + \sqrt{5})$.

Some elementary constructions

To refresh the reader's memory allow me to illustrate the basic constructions with straight edge and compasses.

A line K perpendicular to a given line L at point P on L is obtained by taking P as centre and marking equidistant arcs on L to either side of P, then in turn using these two marked points as centres of larger and equal circles which intersect at points Q and R which are equidistant above and below P. Connect Q to R and draw the perpendicular K. This is a special case of bisecting an angle, here 180°.

Parallel lines can be constructed by drawing two perpendiculars, one to line L, the next to line K. Alternatively we might allow a triangular set-square to be used, in which case the straight edge is first aligned with the given line L and then slid along the set-square to the required position.

The angle at the circumference of a circle subtended by any diameter is one right angle. This is a useful way of constructing a pair of perpendicular lines in any chosen orientation.

A length l on line L is multiplied by an integer n by marking off the length l n times along L. This is multiplication by repeated addition, and subtraction is similarly made.

A length l on line L between points P and Q is divided by an integer n by first drawing a second line K at a suitable angle to L and passing through the end point P. Along this second line K mark off n equal positions using the compasses. The spacing of these can be chosen as seems most suitable. Let the last such arc be at R. Join QR and add lines parallel to QR passing through each of the arcs where they cut K. The intersection of these parallel lines with L divides L into n equal parts.

The ancients knew of Pythagoras' theorem, that in a right-angled triangle the area of the square constructed on the hypotenuse equals the sum of the areas of the squares on the two shorter sides: $h^2 = a^2 + b^2$ in our notation. The square root of an integer l can be obtained using this quite

amazing fact in several similar ways. We should be careful with the dimensions since if $c^2 = l$, then c is a length and l must be an area. Square roots, therefore, are the lengths of sides of squares of given area. Personally, I cannot see a direct way to obtain the square root of an arbitrary l, but the square roots of many, if not all integers, can be obtained by writing each as the sum or difference of two or more other whole numbers. For instance,

$$2 = 1^2 + 1^2, \qquad 3 = 2^2 - 1, \qquad 5 = 2^2 + 1, \qquad 6 = 2^2 + 2, \qquad 7 = 3^2 - 2\,.$$

Figure 2 shows the construction of $\sqrt{5}$ (left) and $\sqrt{11}$ (right) where these are the lengths of the hypotenuse. The lines at 45° are obtained by bisecting a right angle. Figure 3 shows construction of $\sqrt{3}$ and $\sqrt{7}$ as the lengths of a shorter side. We use the right-angle in a semi-circle theorem in these two cases. For $\sqrt{3}$, 1 is subtracted from 2^2, and for $\sqrt{7}$ we subtract $(\sqrt{2})^2$ from 3^2. The $\sqrt{2}$ length has to be constructed by the auxiliary right-triangle with side 1 seen at the upper right of the figure. In this way a library of square root lengths can be built up and used to construct the roots of larger integers.

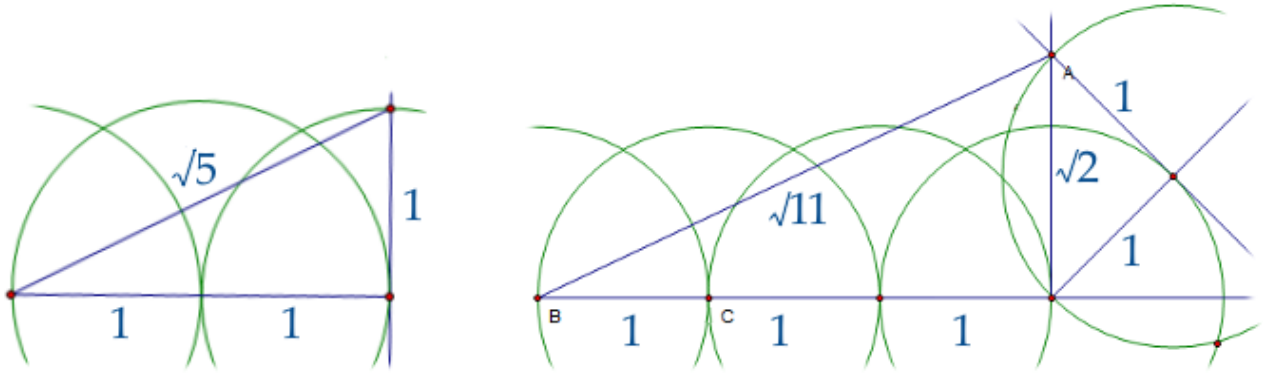

Figure 9: Construction of $\sqrt{5}$ and $\sqrt{11}$ using Pythagoras' theorem.

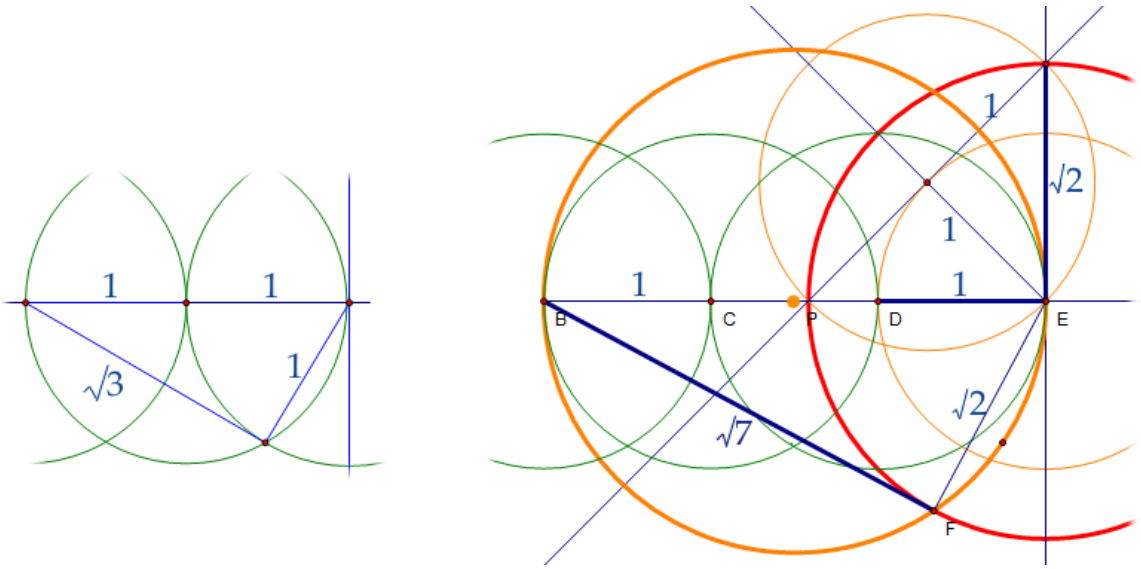

Figure 10: Construction of $\sqrt{3}$ and $\sqrt{7}$ using subtraction in Pythagoras' theorem.

Solving the quadratic

I suspect that the ancient mathematicians knew how to solve a quadratic by 'completing the square'—literally. Figure 3 illustrates the case for the golden mean equation $G^2 - G - 1 = 0$. This is a statement about areas: a square of side G, a rectangle with sides G and 1, and a unit square. Since we are dealing with squares, it seems natural to look for a geometrical construction related to this equation which is as close to a square as possible. We don't yet know the precise value of G but it is somewhere between 1 and 2. So in Figure 4 we drawn a square with overall sides representing G. Now cut the $G \times 1$ rectangle in half lengthwise and subtract the two pieces from the G^2 square in a symmetrical way as shown by the bright orange rectangles. Their overlap in the top right corner has also to be subtracted and this is shown by the dark orange square with sides $\frac{1}{2}$. The remaining green area represents $G^2 - G$ and should have area 1. However the green and dark orange blocks together form a square with side $G - \frac{1}{2}$. So $(G - \frac{1}{2})^2 = 1 + \frac{1}{4}$ from which $G = \frac{1}{2} + \frac{1}{2}\sqrt{5}$. G is readily constructed as a length using $\sqrt{5}$ from Figure 1.

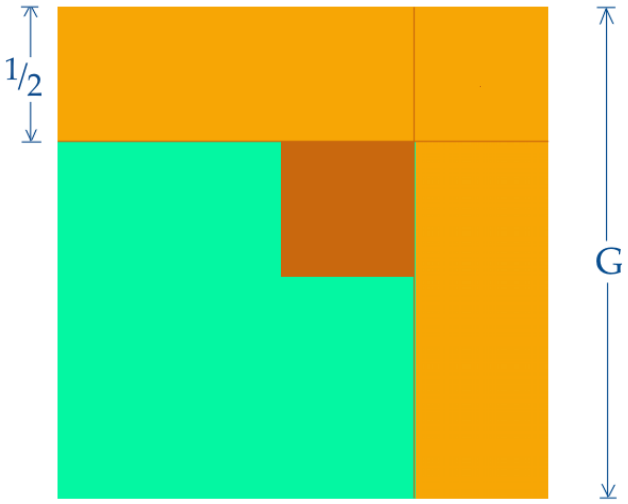

Figure 11: Solving for the golden mean by geometrical construction.

Constructing the pentagon

While we are discussing the golden mean, a number with many engaging properties, let us see how it can be used to construct a regular pentagon. The ancients knew a construction, though I do not know how they discovered it. It arises because the angle at the centre of a pentagon subtended by one of its sides is $\frac{2\pi}{5}$ and $\cos\frac{2\pi}{5} = 1/(2G)$. Moreover the equation $G^2 - G - 1 = 0$ implies that $1/G = G - 1$, so a square of side 1 cut from the end of a rectangle $G \times 1$ leaves a smaller rectangle with exactly the same shape. Figure 5 shows the construction of an angle of 72° once the length G has itself been constructed. The steps in building this are

1. draw the horizontal base line through point A and mark off two equal and touching circles.
2. hence construct the right-triangle with hypotenuse AH equal to $\sqrt{5}$ as in Figure 1 then add 1 at H to extend AH to B.
3. bisect AB to obtain AE with length G. Complete the golden rectangle ACDE.
4. bisect one short side and so divide the golden rectangle lengthwise.

5. bisect a long side CD and construct the semi-circle with CD as diameter.
6. with centre C, intersect this semi-circle at radius $\frac{1}{2}$.
7. complete the triangle CDI. The angle at C is $2\pi/5$ radians.

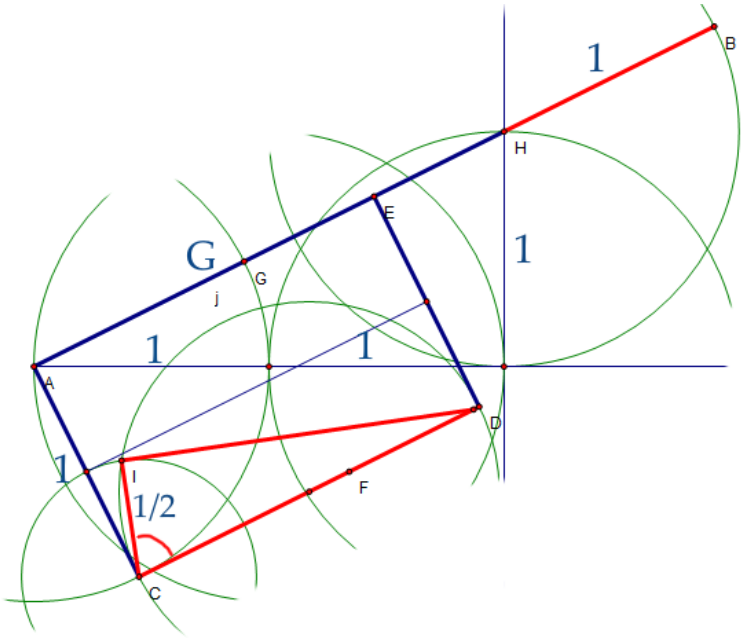

Figure 12: Construction of a golden rectangle and within it an angle of 72°.

Trisecting an angle

Though this is a straight edge and compasses construction, it uses a distance marked by two points on the straight edge and so would not be admissible in Euclid's strict canon. The construction is drawn in Figure 6. Given a base line and an angle of 3θ at A, draw the circle centre A with chosen radius a. Mark the distance a on the straight edge. Use the compass point to constrain the straight edge to pass through point E, where one radius from A meets the circle, and slide the rule until the two marked points are on the circle at C and on the base line at D. The two isosceles triangles ACD, ACE show that the angle at D is θ. Clever!

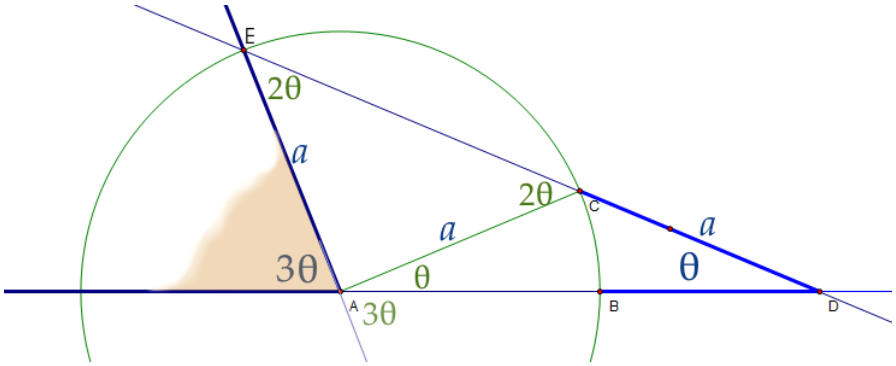

Figure 13: Trisecting an angle using compasses and a marked straight edge.

Appendix 3: Solution of the general cubic

This Appendix recounts the classical solution of the cubic using the formula derived by François Viète in Elizabethan times. First we reduce the general cubic with rational coefficients to a standard form and examine the shapes which the cubic curve can take depending on the coefficients.

The general monic cubic is $C(x) = x^3 + a_2x^2 + a_1x + a_0$. The curve of $C(x)$ is symmetric about its point of inflection at $x = -a_2/3$. So translate the curve by this amount to place the point of inflection on the y-axis. The reduced expression is

$$u^3 + b_1u - b_0, \qquad b_1 = -\frac{a_2^2}{3} + a_1, \quad b_0 = -\frac{2a_2^3}{27} + \frac{a_2\,a_1}{3} - a_0.$$

The shape of the curve depends on the linear factor b_1 as illustrated in Figure 9.

- if $b_1 > 0$, the gradient is everywhere positive so there can be only one real root whatever the value of b_0,
- if $b_1 = 0$, at the point of inflection the curve is horizontal so there will be three equal roots if $b_0 = 0$ and only one otherwise. The real root will be at $u = \sqrt[3]{b_0}$ and have the sign of b_0,
- if $b_1 < 0$, the curve has negative gradient at the origin plus a maximum and a minimum where $u^2 = -b_1/3$. The height of the maximum and depth of minimum from the point of inflection is $\pm\frac{2b_1}{3}\sqrt{\frac{-b_1}{3}}$ so for values of b_0 between these limits there will be three real roots.

Viète's solution uses the clever device of splitting the variable u into two parts to derive two simultaneous equations relating them. Write $u = u_1 + u_2$.

$$u^3 + b_1u - b_0 \;=\; (u_1+u_2)^3 - b_0 + b_1(u_1+u_2) \;=\; u_1^3 + 3u_1^2u_2 + 3u_1u_2^2 + u_2^3 - b_0 + b_1(u_1+u_2)$$

$$=\; u_1^3 + u_2^3 - b_0 \;+ 3u_1u_2(u_1+u_2) + b_1(u_1+u_2).$$

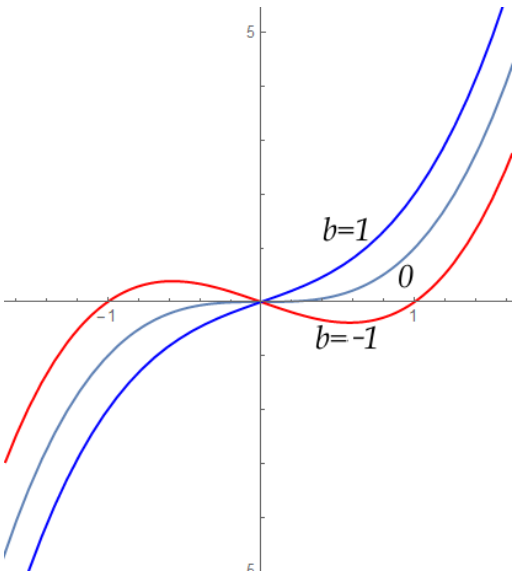

Figure 14: Canonical shapes of the cubic curve $u^3 + b_1u - b_0$ for $b_0 = 0$ and three values of b_1.

This will equal zero if the two parts are respectively zero:

$$u_1^3 + u_2^3 - b_0 = 0 \quad \text{and} \quad (3u_1u_2 + b_1)(u_1 + u_2) = 0.$$

From the second $u_2 = -b_1/(3u_1)$ which we substitute into the first:

$$u_1^3 - \frac{b_1^3}{27u_1^3} - b_0 = 0.$$

At first glance this may look like another cubic, but in fact it is a quadratic in u^3.

$$(u_1^3)^2 - b_0(u_1^3) - \frac{b_1^3}{27} = 0.$$

From here on the solution is clear. The roots of the quadratic are

$$u_1^3 = \frac{1}{2}\left[b_0 \pm \frac{1}{3\sqrt{3}}\sqrt{\Delta}\right], \qquad \Delta = 27b_0^2 + 4b_1^3.$$

$$u_2^3 = \frac{-b_1^3}{27u_1^3} = \frac{2\left[b_0 \mp \frac{1}{3\sqrt{3}}\sqrt{\Delta}\right]}{27b_0^2 - \Delta} = \frac{1}{2}\left[b_0 \mp \frac{1}{3\sqrt{3}}\sqrt{\Delta}\right],$$

the other root of the quadratic. The solution for u_1 has the form of the cube root of a square root, and u_2 has a similar form, making the u_1, u_2 into algebraic conjugates and giving the result the considerable symmetry it needs for all the irrational terms to cancel and the factors to multiply into simple fractions.

Example 1 : In Appendix 1 I quoted the solution of $x^3 + 2x^2 + 5 = 0$ so here work through how this was obtained. The reduced form has $b_1 = -4/3$, $b_0 = -151/27$ and is

$$u^3 - \frac{4}{3}u + \frac{151}{27} = 0.$$

The quadratic in u_1^3 is

$$(u_1^3)^2 + \frac{151}{27}u_1^3 + \frac{64}{729} = 0$$

with solution

$$u_1^3 = \frac{1}{54}\left[-151 \pm 3\sqrt{2505}\right].$$

Using $u_2^3 = -b_1^3/(27u_1^3)$

$$u_2^3 = \frac{64}{729}.\frac{54}{151 \pm 3\sqrt{2505}} = \frac{1}{54}(-151 \mp 3\sqrt{2505}).$$

Taking the upper signs

$$u_1^3 = -0\cdot01574, \qquad u_2^3 = -5\cdot57685.$$

These numerical values present us with the question of how to take the cube roots. The respective real roots are $-0{\cdot}25062$ and $-1{\cdot}77336$ so $u = u_1 + u_2 = -2{\cdot}02398$ corresponding to $x = -2{\cdot}02398 - a_2/3 = -2\cdot69065$. The complex roots are obtained by rotating the real values of each of u_1 and u_2 by $\pm120°$ in the complex plane by multiplying each by $\exp(\pm2\pi i/3)$ before adding them. These cube roots are $0\cdot12531 \pm 0\cdot21705i$ and $0\cdot88668 - 1\cdot53577i$ placing the complex roots at $u = 1\cdot01199 \pm 1\cdot31873i$.

Example 2 : This is a case of three real roots: $x^3 - 3x = 1$. With $b_1 = -3$ and $b_0 = 1$ the quadratic for $u_{1,2}^3$ has complex conjugate roots $(1 \pm i\sqrt{3})/2 = 0.5 \pm 0 \cdot 86603i$. The cube roots of u_1^3 are

$$0 \cdot 93969 + 0 \cdot 34202i, \qquad -0 \cdot 76604 + 0 \cdot 64279i, \qquad -0 \cdot 173648 - 0 \cdot 98481i$$

where each is $\exp(2\pi/3)$ times the previous, in cyclic order. The cube roots of u_2^3 are

$$0 \cdot 93969 - 0 \cdot 34202i, \qquad -0 \cdot 173648 + 0 \cdot 984808i, \qquad -0 \cdot 76604 - 0 \cdot 64279i$$

also in anticlockwise cyclic order. It is clear from the green and purple points in the Argand diagram of Figure 10 how the two sets of roots, each root rotated by 120° from the next in its set, are added in conjugate pairs to give the three real roots $u = u_1 + u_2$. Since $|u_1^3| = 1$, all the points lie on the unit circle. The roots are at twice the distance for the origin of the three reds spots. It is an elegant construction which shows the symmetry behind the apparently unrelated values of the three roots.

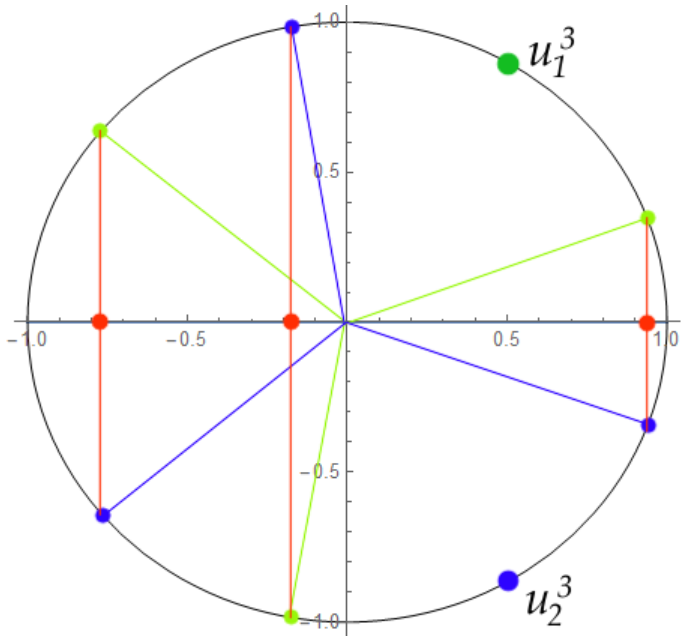

Figure 15: Formation of the three real roots x of $x^3 - 3x - 1$ from two sets of cube roots (yellow-green and blue-purple). Red spots mark $\alpha/2$ values in roots $x = \alpha$.

Appendix 4: Division in field $\mathbb{Q}(\sqrt[3]{N})$

It is easy to see that adjoining the square root $\sqrt{N}$ of a prime number N to the base field $\mathbb{Q}$ gives an extended field with general element $a + b\sqrt{N}$. The algebraic conjugate $a - b\sqrt{N}$ and the relation $(a + b\sqrt{N})(a - b\sqrt{N}) = a^2 - b^2N$ readily produce a rational number. Note that $a - b\sqrt{N} \neq 0$ for N prime so this shows that division of elements produces numbers which also have the form $c + d\sqrt{N}$, $c,\ d \in \mathbb{Q}$. The position with a cube root extension $\mathbb{Q}(\sqrt[3]{N})$ is less obvious. Here I show that $1/g$ has the same form as $g = a + bN^{1/3} + cN^{2/3}$.

Take two algebraic numbers with the form of g and multiply them:

$$g = a + bN^{1/3} + cN^{2/3}, \qquad h = p + qN^{1/3} + rN^{2/3},$$

$$gh = (ap + brN + cqN) + (aq + bp + crN)N^{1/3} + (ar + bq + cp)N^{2/3}.$$

This confirms that the product of two numbers in this extended field is also in the extended field. In order to divide we need the equivalent of an algebraic conjugate to g; call this $\hat{g}$. The product $g\hat{g}$ will be a purely rational number if the coefficients of $N^{1/3}$ and $N^{2/3}$ are both zero. Solving simultaneously for q and r yields

$$q = \frac{p(-ab + c^2N)}{a^2 - bcN}, \qquad r = \frac{p(b^2 - ac)}{a^2 - bcN}.$$

The factor p appears in both of these and hence in h. It allows us to set $p = a^2 - bcN$ and cancel the denominator from $h = \hat{g}$ provided $a^2 \neq bcN$[17]. We therefore obtain

$$\hat{g} = (a^2 - bcN) + (-ab + c^2N)N^{1/3} + (b^2 - ac)N^{2/3}$$

which will make $g\hat{g}$ rational – specifically $g\hat{g} = a^3 + b^3n - 3abcn + c^3n^2$. From this $1/g = \hat{g}/(g\hat{g})$ which has the form $A + BN^{1/3} + CN^{2/3}$, $A,\ B,\ C \in \mathbb{Q}$. Thus the field $\mathbb{Q}(\sqrt[3]{N})$ is closed under division.

I have looked also at $\mathbb{Q}(\sqrt[5]{N})$ in which we expect the general element to be $g = a+bk+ck^2+dk^3+ek^4$, $k = \sqrt[5]{N}$. It is easy to show that the product $gh = (a+bk+ck^2+dk^3+ek^4)(p+qk+rk^2+sk^3+tk^4) = \alpha + \beta k + \gamma k^2 + \delta k^3 + \epsilon k^4$, $\alpha, \beta, \gamma, \delta, \epsilon \in \mathbb{Q}$. I find that, though the algebraic expressions are more complicated, it is possible to solve the four simultaneous equations $\beta = \gamma = \delta = \epsilon = 0$ and obtain $q = pU/D$, $r = pV/D$, $s = pW/D$, $t = pX/D$ where $D,\ U,\ V,\ W,\ X$ involve only sums and products of a, b, c, d, e. By setting $p = D$, assuming $D \neq 0$, we obtain $gh = \alpha$, a purely rational number. So setting $\hat{g} = h$ an algebraic conjugate is formed as for the cubic above, allowing reciprocals and quotients to be calculated, all with the same structure as g.

Perhaps there is a ready proof that this behaviour occurs with the general field extension $\mathbb{Q}(\sqrt[n]{N})$.

[17] There must be more going on here than I have investigated because some numerical tests show that the result holds even when $a^2 - bcN = 0$

Appendix 5: Finite fields as quotient rings of polynomials

Review of some algebraic structures

This appendix is a refresher on the relations between a field and a ring. Though our interest is in the ring of polynomials $P[x]$ on one variable x with coefficients in some field K, the main points are more obviously illustrated in the ring of integers $\mathbb{Z}$. Recall that there is a hierarchy of algebraic structures of increasing specialisation: set → group → ring → integral domain → field. Briefly

- a group is a set with one operation between any pair of elements such that it is closed under that operation, there is an identity element, each element has a unique inverse, and concatenation of the operation is associative.

- a ring is an abelian group under addition which also has a second operation, multiplication. Regarding multiplication, not all rings are commutative (e.g matrices), not all have a unit element, some have zero-divisors (pairs of element, neither being zero, which multiply to give zero). Therefore not all elements have an inverse. Multiplication is associative and distributive over addition.

- a field is a ring with a single unit element in which all elements except zero under multiplication have a unique inverse. In a field multiplication is commutative.

- in a group G a normal sub-group H is one whose left and right cosets are the same (as sets): $gH = Hg$ for all elements $g \in G$. This can also be expressed by saying that the set of conjugates gHg^{-1} of H is the set H: that is, a normal subgroup is invariant under conjugation. If the elements in H are regarded as defined an equivalence class, H and its cosets partition G into other equivalence classes where the order $|H|$ divides the order $|G|$ (Lagrange's theorem). The set of $n = |G|/|H|$ equivalence classes themselves form a group called the quotient group G/H. For instance, in a regular n-gon the set of rotations forms a normal subgroup C_n and the cosets are these rotations combined with a reflection.

- in a ring, the structure which corresponds to a normal subgroup in an ideal, I. This is a proper sub-ring closed under addition and, under multiplication, has the property that if i is in the ideal and a lies outside it, then both ai and ia (which are the same in a commutative ring) lie within I. The ideal may not have a unit – for example, the even numbers in $\mathbb{Z}$. The cosets of I are the partitioned equivalence classes which have the same remainder (residue) under multiplication with any element of I. A quotient ring can be formed by taking I and its cosets each to be a single equivalence class and member of the quotient ring. In this quotient ring the ideal I is the zero element.

- If R is a commutative ring with unity and the dividing ideal is prime, the quotient ring is an integral domain. Prime here means that if the product ab of ring elements is in I, then either a or $b \in I$ (or both are).

- If R is a commutative ring with unity and the dividing ideal is maximal, the quotient ring is a field. An ideal is maximal if it does not sit inside a larger sub-ring. For example, in the integers $2\mathbb{Z}$ = ... −2, 0, 2, 4, 6, ... is maximal, but $6\mathbb{Z}$ = ... −6, 0, 6, 12 ... is not because it lies inside $2\mathbb{Z}$. Maximal ideals are always prime, but the converse is not true. An example of a field as a quotient ring is $\mathbb{Z}/3\mathbb{Z}$ which is the set of three elements: those with remainder 0 and those with remainders 1 and 2. These equivalence classes, also called the congruence classes, are sometimes written $\bar{0}$, $\bar{1}$, $\bar{2}$ and they form the quotient group $\mathbb{Z}_3 \equiv C_3$, the cyclic group of three elements.

- The formation of quotient polynomial rings by maximal polynomial ideals is a critical tool in Galois theory because it gives a way to define a field extension.

Example of field as residues of an irreducible polynomial

An example is perhaps the easiest way to explain how to create the elements of a finite field from a polynomial. Consider the system $P[p\mathbb{Z},x]/M_n[x]$ where $P[p\mathbb{Z},x]$ is the set of all polynomials in x with coefficients in the field $p\mathbb{Z}$ where p is a prime integer. $M_n[x]$ is a polynomial in x of degree n, also with coefficients in $p\mathbb{Z}$, which is irreducible in $p\mathbb{Z}$. As a concrete example take $p = 2$ and $n = 4$. Create the set of all polynomials of degree 4 which are irreducible in $2\mathbb{Z}$: that is, ones that are not zero for $x = 0$ or $x = 1$. The only ones are

$$M_4[x] \;=\; 1+x^3+x^4, \qquad 1+x^2+x^4, \qquad 1+x+x^4, \qquad 1+x+x^2+x^3+x^4.$$

Bear in mind that here $-1 = +1$. When a general polynomial of arbitrarily large degree is divided by any of these, the remainder must be a polynomial of degree at most 3. Its form will be ax^3+bx^2+cx+d where the four coefficients a, b, c, d are either 0 or 1. Since each coefficient can take on 2 values and there are 4 independent coefficients, there are only $2^4 = 16$ possible distinct remainders. A few are

$$0,\;\; 1,\;\; x,\;\; 1+x,\;\; x^2,\;\; 1+x^2,\;\; x+x^2,\;\; 1+x+x^2,\;\; x^3,\;\; 1+x^3,\;\; x+x^3,\; \textit{etc.}$$

These are the 16 elements of the required field. They are the residue classes of any of the four irreducible polynomials $M_4[x]$ above. Since the x^k are essentially only place holders, these field elements could equally be written 0000, 1000, 0100, 1100, 0010, 1010, etc. Here I have adopted the order used by Mathematica by which the powers of x increase to the right.

The created set is clearly closed under addition. To illustrate that it is also closed under multiplication and that elements have inverses, take the examples in Table 1. Here two polynomials, $a = 1+x+x^3 \equiv 1101$ and b, are multiplied. The product is reduced according to the $M_4[x]$ chosen to define the field. In the penultimate column ab is reduced by $11001 \equiv 1+x+x^4$ and in the last column by $10011 \equiv 1+x^3+x^4$. In Table 1 note that every element occurs only once, and in particular that the inverse of 1101 is unique in each case.

As an example of how this calculation is done, first take $M_4[x] = 1+x+x^4$. This defines an ideal and any element in it has zero remainder. So $1+x+x^4 \equiv 0$ making $x^4 \equiv -1-x \equiv 1+x$ in $2\mathbb{Z}$.

$$(1+x+x^3)(1+x^2) \;=\; (1+x+x^2+2x^3+x^5) \;\equiv\; 2x^3+2x^2+2x+1 \;\equiv\; 1 \mod 2$$

so the inverse of 1101 is 1010 when reduced by 11001. However

$$(1+x+x^3)(1+x^2) \;=\; (1+x+x^2+2x^3+x^5) \;\equiv\; 3x^3+x^2+2x+2 \;\equiv\; x^3+x^2 \mod 2$$

so the product (1101)(1010) is 0011 when reduced by $M_4[x] = 10011$. The choice of dividing polynomial, therefore, does affect the created field by determining how the elements multiply.

The construction $P[p\mathbb{Z},x]/M_n[x]$ will generate the unique field of p^n elements. The only finite fields that exists have these orders: 2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17, 19, 23, 25, 27, 29, 31, 32, 37, etc. All others putative fields would have zero divisors such as $2 \times 2 = 4 \equiv 0$ in $4\mathbb{Z}$.

The 16 elements form an abelian group under addition, generated by 1000, 0100, 0010, 0001. The 15 non-zero elements also form a group under multiplication. Table 2 lists the order of each element subject to the two irreducible divisors and shows the same orders for every element. There

$M_4[x]$			1 1 0 0 1	1 0 0 1 1
	a	b	ab	ab
1	1 1 0 1	0 0 0 0	0 0 0 0	0 0 0 0
2		1 0 0 0	1 1 0 1	1 1 0 1
3		0 1 0 0	1 0 1 0	1 1 1 1
4		1 1 0 0	0 1 1 1	0 0 1 0
5		0 0 1 0	0 1 0 1	1 1 1 0
6		1 0 1 0	**1 0 0 0**	0 0 1 1
7		0 1 1 0	1 1 1 1	0 0 0 1
8		1 1 1 0	0 0 1 0	1 1 0 0
9		0 0 0 1	1 1 1 0	0 1 1 1
10		1 0 0 1	0 0 1 1	1 0 1 0
11		0 1 0 1	0 1 0 0	**1 0 0 0**
12		1 1 0 1	1 0 0 1	0 1 0 1
13		0 0 1 1	1 0 1 1	1 0 0 1
14		1 0 1 1	0 1 1 0	0 1 0 0
15		0 1 1 1	0 0 0 1	0 1 1 0
16		1 1 1 1	1 1 0 0	1 0 1 1

Table 1: Products of element 1101 with all 16 elements in the field, reduced according to two irreducible polynomial divisors, a) 11001 and b) 10011.

are 8 elements of order 15, two of order 3 and four of order 5. This implies a cyclic group generated by any of the order-15 elements, with two subgroups of orders 3 and 5, suggesting that the whole group is the direct product $C_{15} = C_3 \times C_5$. It is true in general that a cyclic group C_n has $\phi(n)$ generators where $\phi(n)$ is the Euler totient function which counts the number of integers less than n and coprime to n (including 1). For $n = 5$ this is 4, namely $\{1, 2, 3, 4\}$, and for $n = 15$ is 8, namely $\{1, 2, 4, 7, 8, 11, 13, 14\}$. The C_3 subgroup is {1000, 0110, 1110}. The C_5 subgroup is generated by any of 0001, 0101, 0011 or 1111. Having a different dividing polynomial $M_4[x]$ changes the order in which elements are generated in each subgroup, but as sets the same elements are generated. For example $0001^2 = 0011$ with $M_4[x] = 11001$, but $0001^2 = 1111$ with $M_4[x] = 10011$. The product of any element from the C_3 subgroup with any one from the C_5 has order 15 and is one of the 8 generators of the whole C_{15} group.

The discussion above has been for fields with coefficients in $p\mathbb{Z}$, but the logic still applies when they are in $\mathbb{Q}$. For example, consider the meaning of $\mathbb{Q}[x]/(x^2+1)$. The polynomial remainders on division by $(x^2 + 1)$ can have degree 0 or 1 so the only possible forms are ax, $ax + b$ or b where $a, b \in \mathbb{Q}$. These are the residue classes of the ideal generated by $x^2 + 1$. $x^2 + 1$ leaves remainder 0 so $x^2 + 1 \equiv 0$. Hence $x = \pm\sqrt{-1} = \pm i$ and $\mathbb{Q}[x]/(x^2 + 1)$ means all algebraic numbers of the form $a \pm ib$. These are the complex numbers and their conjugates.

$M_4[x]$		11001	10011
1	0 0 0 0		-
2	1 0 0 0	1	1
3	0 1 0 0	15	15
4	1 1 0 0	15	15
5	0 0 1 0	15	15
6	1 0 1 0	15	15
7	0 1 1 0	3	3
8	1 1 1 0	3	3
9	0 0 0 1	5	5
10	1 0 0 1	15	15
11	0 1 0 1	5	5
12	1 1 0 1	15	15
13	0 0 1 1	5	5
14	1 0 1 1	15	15
15	0 1 1 1	15	15
16	1 1 1 1	5	5

Table 2: The order k of each element f under multiplication such that $f^k = 1$. Values for two dividing polynomials $M_4[x]$.

Appendix 6: Splitting field extensions of a polynomial

This Appendix gives a couple of examples of determining the tower of extensions which build to the splitting field of a given polynomial. It illustrates some misunderstandings and pit falls. Here I investigate three given irrationals.

Polynomial $x^3 - 5$

In $\mathbb{C}$ $x^3 - 5 = 0$ has the roots $\sigma = \sqrt[3]{5} \approx 1 \cdot 71$, the real cube root of 5, plus the complex conjugate roots $\sigma\omega$, $\sigma\omega^2$, $\omega = \exp(2\pi i/3) = \frac{1}{2}(-1 + i\sqrt{3})$. The lowest power of σ which is a rational number is $\sigma^3 = 5$, so the degree of extension of $[\mathbb{Q}(\sigma) : \mathbb{Q}] = 3$. Similarly the lowest power of ω which is rational is $\omega^3 = 1$. However it would be a mistake to think that the combined degree of these two extensions of $\mathbb{Q}$ is $3 \times 3 = 9$. The reason why this is incorrect is that both degrees have been measured from $\mathbb{Q}$ as the base. The correct view is to have one extension build on the previous one, not on the base field.

In $\mathbb{Q}(\sigma)$ the given cubic factors as $x^3 - 5 = (x - \sigma)(x^2 + \sigma x + \frac{5}{\sigma})$. Using the quadratic formula Eq 3 the quadratic factor has roots

$$x = \frac{1}{2}\left(-\sigma \pm \sqrt{\sigma^2 - \frac{20}{\sigma}}\right).$$

But $20/\sigma = 4\sigma^3/\sigma$ so $x = \frac{1}{2}(-\sigma \pm i\sigma\sqrt{3})$. This presentation shows clearly that over the field $\mathbb{Q}(\sigma)$ the quadratic factor has degree 2 and the tower of extensions is

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{5}) \subset \mathbb{Q}(\sqrt[3]{5},\ i\sqrt{3})$$

and the overall degree is $3 \times 2 = 6$. The base vectors of the splitting field are 1, σ, σ^2, $i\sqrt{3}$, $i\sigma\sqrt{3}$, $i\sigma^2\sqrt{3}$. Alternatively they are 1, σ, σ^2, $\sigma\omega$, $\sigma^2\omega$. Note that ω^2 lies in this field as $1/\omega$.

Polynomial $x^5 - 3$

If $\beta = \sqrt[5]{3} \approx 1 \cdot 2475$, the real 5th root of 3, then $x^5 - 3$ factors as

$$x^5 - 3 = (x - \beta)\left(x^4 + \beta x^3 + \beta^2 x^2 + \beta^3 x + \frac{3}{\beta}\right) = (x - \beta)\prod_{k=0}^{4} x^k \beta^{4-k}.$$

The product is a form of cyclotomic polynomial. The more familiar version is

$$x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + x^{n-3} + ... + x + 1).$$

The roots are the $n - 1$ complex numbers $x = \sqrt[n]{1} = \exp(2\pi i/n)$. With the β coefficients present the roots of $(x - \beta)\prod_{k=0}^{4} x^k \beta^{4-k} = 0$ are the four complex numbers $x = \beta\sqrt[5]{1} = \beta\exp(2\pi i/5)$. Now

$$\exp(2\pi i/5) = \cos(2\pi/5) + i\sin(2\pi/5) = \frac{1}{4}(\sqrt{5} - 1) + i\frac{1}{2\sqrt{2}}\sqrt{5 + \sqrt{5}}.$$

The field extension over $\mathbb{Q}(\beta)$ can be generated by $\eta = i\left(\sqrt{\frac{5}{2} + \frac{\sqrt{5}}{2}}\right) = 2i\sin(72°)$ which has degree 4. It has minimal polynomial $y^4 + 5y^2 + 5$, a quadratic in y^2, equivalent to $16\sin^4(2\pi/5) - 20\sin^2(2\pi/5) + 5$,

and has degree 4. The base vectors of the extension can be expressed in various ways in terms of η and its powers. For instance $\sqrt{5} = (\eta^4/5 - \eta^2) + 4$. The tower of extensions is

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt[5]{3}) \subset \mathbb{Q}\left(\sqrt[5]{3},\ i\sqrt{\frac{1}{2}(5+\sqrt{5})} \right) \equiv \mathbb{Q}(\sqrt[5]{3},\ i\sin(2\pi/5))$$

with degree $5 \times 4 = 20$.

It is shown in Appendix 7 that the automorphism group of D_5, the dihedral group of symmetries of a regular pentagon, is isomorphic to the semi-direct product $C_5 \rtimes C_4$ and has order 20. This is no coincidence, but an example of the main theorem on Galois theory, that the degree of the extension from $\mathbb{Q}$ to the splitting field of a polynomial is equal to the order of the group of automorphisms of the roots.

Polynomial $x^6 - 5$

For this final example we again factorise but observe that $x^6 - 5$ is a cubic in x^2. Therefore it is $(x-\delta)(x+\delta)(x^4+\delta^2x^2+\delta^4)$ where $\delta = \sqrt[6]{5} \approx 1\cdot3077$, the real sixth root of 5. The extension $\mathbb{Q}(\delta) : \mathbb{Q}$ therefore has degree 6. Using Eq 3 the 4th order polynomial factor, a quadratic in x^2, has the four roots

$$\pm\frac{\delta}{\sqrt{2}}\sqrt{-1 \pm i\sqrt{3}}.$$

These look as if the lowest power of each which is a rational number is the 4th. However

$$\frac{1}{\sqrt{2}}\sqrt{-1 \pm i\sqrt{3}} = \frac{1}{2}(1 \pm i\sqrt{3})$$

so adjoining $i\sqrt{3}$ to $\mathbb{Q}(\delta)$ is enough to create the splitting field. The tower of extensions is

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt[6]{5}) \subset \mathbb{Q}(\sqrt[6]{5},\ i\sqrt{3})$$

with degree $6 \times 2 = 12$. This is consistent with the automorphism group D_{12}, the symmetry group of a regular hexagon, also being D_{12} with 12 elements.

Appendix 7: Finding the minimal polynomial

The term 'minimal polynomial' refers to the irreducible polynomial of smallest degree which has a given algebraic number or set of algebraic numbers as its root(s). In Galois theory we are interested in the minimal polynomial of three types of algebraic number:

1. the minimal polynomial of α where α is a root of a give polynomial $P(x)$,
2. the minimal polynomial of the primitive element γ of a simple field extension $\mathbb{Q}(\gamma)$, such as might be formed by combining two or more adjoined algebraic numbers: $\mathbb{Q}(\gamma) = \mathbb{Q}(\alpha, \beta)$,
3. the minimal polynomial of the Galois group of $P(x)$, formed as the product of linear factors $\prod(x - s_j(\beta))$ where β is a root of $P(x)$ and s_j are all the automorphisms of the splitting field of $P(x)$.

Finding the minimal polynomial associated with a given irrational number can be a challenge if the number is at all complicated. Here I investigate three given irrationals. The investigation leads to the 'primitive element theorem' which states that any finite field extension F of $\mathbb{Q}$ has a single element θ such $F = \mathbb{Q}(\theta)$. This means that any finite field extension can be cast as a simple extension of the rationals.

Polynomial 1 with root $\alpha = \sqrt[3]{2} + \sqrt{5}$

The required polynomial must, by definition, be a linear combination of α and its powers. The challenge is to find coefficients which will make the polynomial zero. It is necessary to work out the first few powers of α then look for weighting coefficients to make their sum zero. We find

$$\alpha = 2^{1/3} + \sqrt{5}, \qquad \alpha^2 = 5 + 2^{2/3} + 2.2^{1/3}\sqrt{5}, \qquad \alpha^3 = 2 + 15.2^{1/3} + 5\sqrt{5} + 3.2^{2/3}\sqrt{5}\,.$$

We pause here to notice that some irrational elements are reappearing. Let

$$a = 2^{1/3}, \qquad b = \sqrt{5}, \qquad c = 2^{2/3}, \qquad d = 2^{1/3}\sqrt{5}, \qquad e = 2^{2/3}\sqrt{5}\,.$$

These are base vectors of the field $\mathbb{Q}(\sqrt[3]{2}, \sqrt{5})$. The powers of α can be written in terms of these as base vectors:

$$\alpha = a + b, \qquad \alpha^2 = 5 + c + 2d \qquad \alpha^3 = 2 + 15a + 5b + 3e.$$

How far do we have to go in finding powers in α? For the polynomial to equal 0 the sum, weighted by the coefficients, of each of the a, b, c, etc. must be zero. To achieve this we will need at least two of each a, b, etc. for there to be any chance of them cancelling. So far we only have one e so we continue:

$$\alpha^4 = 25 + 2a + 8b + 30c + 20d, \quad \alpha^5 = 100 + 125a + 25b + 2c + 10d + 50e,$$

A trial shows that there is not a polynomial $a_0 + a_1\alpha ... + a_5\alpha^5$ which gives zero. Pressing on

$$\alpha^6 = 129 + 150a + 375c + 200b + 150d + 12e.$$

We form

$$P(\alpha) = a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4\alpha^4 + a_5\alpha^5 + a_6\alpha^6$$

$$= a_1(a + b) + a_2(5 + c + 2d) + a_3(2 + 15a + 5b + 3e) + a_4(25 + 2a + 8b + 30c + 20d)$$

$$+ a_5(100 + 125a + 25b + 2c + 10d + 50e) + a_6(129 + 150a + 200b + 375c + 150d + 12e).$$

The coefficients of a, b are

$$a \;:\; a_1 + 15a_3 + 2a_4 + 125a_5 + 150a_6\,, \qquad\qquad b \;:\; a_1 + 5a_3 + 8a_4 + 25a_5 + 200a_6\,,$$

etc., but the equations to solve for a_1, a_2, ... a_6 are more clearly seen in matrix form:

$$\begin{pmatrix} 1 & 0 & 15 & 2 & 125 & 150 \\ 1 & 0 & 5 & 8 & 25 & 200 \\ 0 & 1 & 0 & 30 & 2 & 375 \\ 0 & 2 & 0 & 20 & 10 & 150 \\ 0 & 0 & 3 & 0 & 50 & 12 \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

This can be reduced using elementary row operations. There is one arbitrary coefficient, a_6, in terms of which

$$a_1 = -60a_6, \quad a_2 = 75a_6, \quad a_3 = -4a_6, \quad a_4 = -15a_6, \quad a_5 = 0\,.$$

To obtain a monic polynomial set a_6 to 1 and evaluate

$$-60(a+b) + 75(5+c+2d) - 4(2+15a+5b+3e) - 15(25+2a+8b+30c+20d) \\ + (129 + 150a + 200b + 375c + 150d + 12e) = 121.$$

It is a relief to see that this is a rational number. The required polynomial containing $2^{1/3} + \sqrt{5}$ as one of its roots is

$$P(x) = x^6 - 15x^4 - 4x^3 + 75x^2 - 60x - 121.$$

As a numerical check, $\sqrt[3]{2} + \sqrt{5} = 3\cdot 495989$ and this does indeed satisfy $P(3\cdot 495989) = 0$. Since the coefficients are all real, the roots must be in conjugate pairs so we expect $\sqrt[3]{2} - \sqrt{5} = -0\cdot 976147$ also to be a root, and indeed it is.

Is $P(x)$ the minimal polynomial of the given irrational? Given the way it has been constructed, the answer is probably Yes, but it would be good to prove that it is irreducible over $\mathbb{Q}$. To apply Eisenstein's criterion we look for a prime number p which divides all the coefficients except the leading one, but p^2 does not divide the constant a_0. No such p exists for $P(x)$ as written and I have failed to find a substitution $x \to u + k$ for $-10 \le k \le +10$ which meets the criterion either. There are other sophisticated tests for irreducibility, but I have not explored them. Mathematica thinks it is irreducible.

The significance of the quantities $a = \sqrt[3]{2}$, $b = \sqrt{5}$, etc. can now be seen. They are base vectors which together with 1 span the vector space of the root field. A general algebraic number in this field is a linear combination of 1, a, b, c, d and e. The field extension from $\mathbb{Q}$ has degree 6 which is 2×3, the indices of the roots. Though the field extension $\mathbb{Q}(\sqrt[3]{2} + \sqrt{5})$ is simple, it can be broken into the short tower $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[3]{2}, \sqrt{5})$ or $\mathbb{Q} \subset \mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\sqrt[3]{2}, \sqrt{5})$.

Polynomial 2

I found this hairy problem in a book on 'Rings, Fields and Groups' by R.B.J.T. Allenby of Leeds University, page 279. (How many initials does a man need!?)

> **Q:** Find a polynomial $f(x)$ in $\mathbb{Q}$ having $\sqrt{3} + \sqrt[4]{1 + \sqrt[3]{\frac{5}{2}}}$ as a zero. Exhibit a radical tower over $\mathbb{Q}$ which contains the splitting field of $f(x)$.

Allenby does not give the answer in the back of his book. It seems likely that the degree of the minimal polynomial will be the multiple of 2, 4 and 3, which is 24. There would then be 23 irrational base vectors in the root field. The method used above for the easier root could be applied with care. Mathematica gives

$$1038361 - 7354368x^2 + 17716992x^4 - 24529248x^6 + 17630256x^8 - 8842104x^{10} + 3158252x^{12} - 836352x^{14} + 164544x^{16} - 23616x^{18} + 2352x^{20} - 144x^{22} + 4x^{24}.$$

This is hardly a problem for a student textbook. It would be interesting to know of algorithms which are more efficient that the one I have used here.

Polynomial 3 with root $\sqrt{1+\sqrt[3]{5}}$

Applying the above algorithm to this irrational which has nested roots, it soon becomes clear that the base vectors of the root field are

$$1, \quad a = 5^{1/3}, \quad b = 5^{2/3}, \quad c = \sqrt{1+5^{1/3}}, \quad d = 5^{1/3}\sqrt{1+5^{1/3}}, \quad d = 5^{2/3}\sqrt{1+5^{1/3}}.$$

In terms of these the powers of the given α are

$$\alpha = c, \quad \alpha^2 = 1+a, \quad \alpha^3 = c+d, \quad \alpha^4 = 1+2a+b,$$
$$\alpha^5 = c+2d+e, \quad \alpha^6 = 6+3a+3b, \quad \alpha^7 = 6c+3d+3e.$$

I have taken this to the 7th power because we need at least two of each basis vector for them to cancel. Our first attempt at finding a polynomial is

$$a_0 + a_1c + a_2(1+a) + a_3(c+d) + a_4(1+2a+b) + a_5(c+2d+e) + a_6(6+3a+3b) + a_7(6c+3d+3e)$$

though higher powers will need to be added if no solution for these coefficients a_j can be found. The matrix equation is

$$\begin{pmatrix} 0 & 1 & 0 & 2 & 0 & 3 & 0 \\ 0 & 0 & 0 & 1 & 0 & 3 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 3 \\ 0 & 0 & 1 & 0 & 2 & 0 & 3 \\ 0 & 0 & 0 & 0 & 1 & 0 & 3 \end{pmatrix} \begin{pmatrix} a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

This is easily row reduced. There are two arbitrary values. This hints that the polynomial may be reducible, as does having to include α^7 for a vector space of degree 6. We find $a_1 = -6a_7$, $a_2 = 3a_6$, $a_3 = 3a_7$, $a_4 = -3a_6$, $a_5 = -3a_7$. The constant term evaluates to $-6a_6$. Setting $a_6 = a_7 = 1$, the polynomial is

$$x^7 + x^6 - 3x^5 - 3x^4 + 3x^3 + 3x^3 - 6x - 6.$$

Suspecting that this is reducible, try some small values of x. -1 is a zero, so divide by $x+1$ to obtain

$$x^6 - 3x^4 + 3x^2 - 6$$

which is irreducible over $\mathbb{Q}$. This minimal polynomial is a cubic in x^2 so $-\sqrt{1+\sqrt[3]{5}}$ is also a root.

You might ask whether a different irreducible polynomial would result from a different choice of a_6 and a_7, so test this with $a_6 = 2$, $a_7 = -5$, say. The polynomial is

$$12 - 30x - 6x^2 + 15x^3 + 6x^4 - 15x^5 - 2x^6 + 5x^7 = (-2+5x)(-6+3x^2-3x^4+x^6)$$

and the minimal polynomial found is as before. For all irrationals, the minimal polynomial is unique.

The Primitive Element theorem

I will approach this by showing that $\mathbb{Q}(\alpha,\beta)$ can be written as $\mathbb{Q}(\alpha+\beta)$. Here α is an algebraic number which satisfies a minimal polynomial of degree A while β satisfies one of degree B. This means that

$$\alpha^A = c_{A-1}\alpha^{A-1} + c_{A-2}\alpha^{A-2} + ... + c_1\alpha + c_0, \qquad \beta^B = d_{B-1}\beta^{B-1} + d_{B-2}\alpha^{B-2} + ... + d_1\alpha + d_0. \quad (A7.1)$$

The degree of $\mathbb{Q}(\alpha,\beta)$ is AB. It is spanned by the base vectors $1,\alpha,\alpha^2,....,\alpha^{A-1}$ plus all products of this set with $\beta,\beta^2,....,\beta^{B-1}$, and they total to $A+A(B-1)$ elements. The element with the highest degree is $\alpha^{A-1}\beta^{B-1}$ whose combined degree is $A+B-2$.

Let $\gamma=\alpha+\beta$. We want to show that α and β can be written in terms of γ and its powers, because then all products $\alpha^j\beta^k$ can also be written in terms of γ alone, so showing that $\mathbb{Q}(\alpha,\beta)$ can be written as $\mathbb{Q}(\alpha+\beta)$. The binomial theorem gives us all powers of γ. Each γ^j can be reduced modulo A and B using the relations in Eq A7.1. The product $\alpha^{A-1}\beta^{B-1}$ does not appear until γ^{A+B-2}. To solve for all AB field base vectors we need an AB square matrix, so the binomial expansions must be continued to γ^{AB} and each reduced modulo α^A, β^B. At this stage we have a set of simultaneous linear equations with a unique solution which relates all field elements in $\mathbb{Q}(\alpha,\beta)$ to powers of γ.

The examples given above in this Appendix can be seen as cases of this procedure, but I will work though one more example. Suppose, therefore, that α is a root of x^3-x^2-3 and β of x^2+2x+5, both of which are irreducible over $\mathbb{Q}$. Note that neither α nor β is specified explicitly but only as $\alpha^3=\alpha^2+3$, $\beta^2=-2\beta-5$. Then $\alpha^4=\alpha^2+3\alpha+3$, $\beta^3=-\beta+10$, $\beta^4=12\beta+5$, *etc.* Letting $\gamma=\alpha+\beta$ we develop the matrix equation

$$\begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 \\ -5 & 0 & 1 & -2 & 2 & 0 \\ 13 & -15 & 1 & -1 & -6 & 3 \\ 8 & 43 & -29 & 24 & -4 & -8 \\ -207 & 28 & 54 & -64 & 75 & -25 \\ 482 & -582 & 207 & -154 & -186 & 154 \end{pmatrix} \begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \\ \beta \\ \alpha\beta \\ \alpha^2\beta \end{pmatrix} = \begin{pmatrix} \gamma \\ \gamma^2 \\ \gamma^3 \\ \gamma^4 \\ \gamma^5 \\ \gamma^6 \end{pmatrix}.$$

Matrix inversion gives all the field basis vectors in terms of γ. Thus, with $N=685933=4369\times157$,

$$\begin{aligned}
157 &= -146\gamma-69\gamma^2-30\gamma^3-18\gamma^4-4\gamma^5-\gamma^6 \\
N\alpha &= 171922\gamma+118748\gamma^2-81288\gamma^3+56323\gamma^4+7562\gamma^5+5737\gamma^6 \\
N\alpha^2 &= 359930\gamma-272492\gamma^2-61436\gamma^3-940\gamma^4+8618\gamma^5+2547\gamma^6 \\
N\beta &= 514011\gamma-118748\gamma^2+81288\gamma^3-56323\gamma^4-7562\gamma^5-5737\gamma^6 \\
N\alpha\beta &= -1260639\gamma-393188\gamma^2-215669\gamma^3-252458\gamma^4-55561\gamma^5-17933\gamma^6 \\
N\alpha^2\beta &= 1153813\gamma+1164943\gamma^2+6411\gamma^3+99020\gamma^4-2976\gamma^5+8990\gamma^6
\end{aligned}$$

The veracity of this can be tested numerically. On solving the parent equations, $\alpha=1.863706528..$ and $\beta=-1+2i$, and I find that all the above solutions agree. The top row gives the minimal polynomial for γ as $x^6+4x^5+18x^4+30x^3+69x^2+146x+157$. Two of its roots are γ and its complex conjugate. The six roots (three conjugate pairs) must span $\mathbb{Q}(\alpha,\beta)$.

Since two independent extensions, each made by adjoining one algebraic number, can be fused into one simple extension, the process can be extended so that any number of simple extensions fuse into one large simple extension: $\mathbb{Q}(\alpha, \beta, \gamma, \delta) = \mathbb{Q}(\alpha + \beta, \gamma, \delta) = \mathbb{Q}(\alpha + \beta + \gamma, \delta) = \mathbb{Q}(\alpha + \beta + \gamma + \delta)$.

Appendix 8: Automorphisms

Textbooks and the literature talk in terms of automorphisms of the field extensions, and how the automorphisms of an extension which leave the base field unchanged form a group. This appendix explains this in algebraic terms, though the reader may already accept that automorphisms are just permutations of the field elements, and permutations form a group.

In §1 we planted the idea that the similarities, indeed symmetries, of the roots of a polynomial are what allow cancellation of the square, cube and higher radicals when the roots are added and multiplied, as at Eq 5. This section looks at the permutations of the roots which display this symmetry, and explains the concept of a field automorphism. The section also alludes to the Galois Correspondence between field extensions and the Galois group of automorphisms/permutations, though a fuller explanation of this central theorem is delayed until §5 and §6.

The reader may know the concepts of homomorphism and isomorphism of algebraic structures. We have two sets, A and B, of elements $a_j \in A$, $b_k \in B$ where the indices j, k run over several or even many values. A joining, multiplication or concatenation operation $\circ$ applies between elements of A and a similar operation $*$ applies within B. A homomorphism θ maps elements of A to elements of B in such a way that the relations between elements carry over from A to B. This means that the result of composing two elements and mapping them from A to B is the same whether the joining operation is applied first in the space of A or later in that of B. Symbolically

$$\text{if } \theta(a_1) = b_1 \text{ and } \theta(a_2) = b_2, \quad \text{then } \theta(a_1 \circ a_2) = \theta(a_1) * \theta(a_2) = b_1 * b_2.$$

In addition $\theta(I) = e$ where I is the identity element in A and e the identity in B.

In a general homomorphism several elements of A could be sent to the identity e. We then say that the homomorphism is 'not faithful' because a distortion has occurred and information in A has been lost in the transfer to B. The section of A which is lost by being mapped to e (*i.e.* obliterated) is called the 'kernel' of the homomorphism. An isomorphism is a homomorphism which is faithful: it is a bijection, meaning every element of A maps to a separate distinct element of B and none is left over. Only I maps to e. With an isomorphism there is a reverse operation θ^{-1} which uniquely maps each element $b \in B$ back to its corresponding $a \in A$.

An automorphism is an isomorphism where the sets A and B, and hence the operations $\circ$ and *, are the same. An automorphism θ maps an algebraic structure to itself. It permutes the elements by mapping a_j to a_k in such a way that $\theta(a_j \circ a_k) = \theta(a_j) \circ \theta(a_k)$. Clearly the identity I must map to itself and this implies that inverses of elements map to the corresponding inverses, since

$$\text{if } \theta(a) = b, \text{ then } \theta(I) = \theta(a.a^{-1}) = \theta(a)\theta(a^{-1}) = b.b^{-1} = I.$$

Also an element of general order m can map only to another element of order m. An automorphism is essentially a relabelling of the elements of an algebraic structure.

Suppose we have a field K extended to L by adjoining an algebraic number: $K \subset L = K(\alpha)$. Rather than studying automorphisms of the whole field L, Galois theory deals with those automorphisms of the field *extensions* $L : K$ in which K is left undisturbed by the permutations; only the extension part is permuted. This was alluded to in the examples of §1 where $P(x) = x^2 - 2$ could have its two algebraic roots interchanged without disturbing the rational coefficients of the polynomial. The term 'K–automorphism of L' is used to mean that K is unchanged while those

other elements in $L = K(\alpha)$ which involve only α may be shuffled. For example, the complex numbers $\mathbb{C}$ are an extension of the reals: $\mathbb{C} = \mathbb{R}(i)$, $i^2 = -1$. The only $\mathbb{R}$-automorphism of $\mathbb{C}$ is complex conjugation, $i \to -i$, $-i \to i$, denoted by *. This mirrors the complex plane in the real axis, an operation which does not move either the additive identity 0 or multiplicative identity 1. Under it $(z_1 + z_2)^* = z_1^* + z_2^*$ and $(z_1 z_2)^* = z_1^* z_2^*$, so preserving the algebraic relations. All of $\mathbb{R}$ is left unchanged. This is field automorphism of the extension $\mathbb{C} : \mathbb{R}$ and $[\mathbb{C} : \mathbb{R}] = 2$.

What is the effect of a $\mathbb{Q}$-automorphism on $P(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_1 x + a_0$? Since x takes numerical values within the splitting field of $P(x)$, the homomorphism property means that $\theta(x * x) = \theta(x)\theta(x)$ or more generally that $\theta(x^n) = (\theta(x))^n$. Then

$$\theta(x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_1 x + a_0) = \theta(x^n) + \theta(a_{n-1}x^{n-1}) + \theta(a_{n-2}x^{n-2}) + ... + \theta(a_1 x) + \theta(a_0)$$

$$= (\theta(x))^n + a_{n-1}(\theta(x))^{n-1} + a_{n-2}(\theta(x))^{n-2} + ... + a_1\theta(x) + a_0$$

since the rational coefficients are invariant. This states that x and $\theta(x)$ both satisfy $P(x)$ and means that an automorphism maps one root of $P(x)$ to another root of $P(x)$. These roots are said to be 'conjugate'. So if one root α_j is known and a field automorphism θ is known, at least one other root $\theta(\alpha_j)$ can be found. This is a crucial point: automorphisms of a field (and any of its subfields) can only carry the roots of a particular irreducible polynomial into other of its roots. I give an illustration of this below, but first consider a simple example of a $\mathbb{Q}$-automorphism.

Look again at $\mathbb{Q}(\sqrt{2})$, the splitting field of both $x^2 - 2 = 0$ and $x^2 - 2ax + a^2 - 2b^2 = 0$. It consists of an infinity of algebraic numbers all of the form $u + v\sqrt{2}$, $u, v \in \mathbb{Q}$. For $x^2 - 2ax + a^2 - 2b^2$ the two roots are $a + b\sqrt{2}$ and $a - b\sqrt{2}$. A $\mathbb{Q}$-automorphism of the splitting field by definition leaves a and b unchanged so the only possible permutation is of the adjoined $\sqrt{2}$ part; it is to swap $\sqrt{2}$ and $-\sqrt{2}$. To check that this is an automorphism observe that for all numbers in the field

1. adding, $\theta((u + v\sqrt{2}) + (c + d\sqrt{2})) = u + c - (v + d)\sqrt{2} = \theta(u + v\sqrt{2}) + \theta(c + d\sqrt{2})$,
2. the multiplicative identity is $1 + 0\sqrt{2}$,
3. $\theta((u+v\sqrt{2})(c+d\sqrt{2})) = \theta(uc+2vd+(ud+vc)\sqrt{2}) = uc+2vd-(ud+vc)\sqrt{2} = (u-v\sqrt{2})(c-d\sqrt{2}) = \theta(u + v\sqrt{2})\,\theta(c + d\sqrt{2})$.

Moreover the polynomial expressed in linear factors is $[x - (a + b\sqrt{2})][x - (a - b\sqrt{2})]$ which expands to $x^2 - 2ax + a^2 - 2b^2$. The symmetry between $\sqrt{2}$ and $-\sqrt{2}$ is the reason the $\pm b\sqrt{2}$ terms cancel to leave only rational coefficients.

This next example illustrates that a field automorphism can only permute the roots of the same polynomial. Take the extension $\mathbb{Q}(\alpha, \omega)$ where α is the real cube root of 2: $\alpha \approx 1{\cdot}26$, $\alpha^3 = 2$, and ω is the complex cube root of unity $= (-1 + i\sqrt{3})/2$. α satisfies the minimal irreducible polynomial $x^3 - 2$ whose other two roots are $\omega\alpha$ and $\omega^2\alpha$. Now $x^3 - 1 = (x - 1)(x^2 + x + 1)$ is reducible. The irreducible quadratic factor has roots ω, $\omega^2 = -1 - \omega$. Since ω^2 is linearly dependent on ω, a basis for the extended field is

$$\{1,\ \alpha,\ \alpha^2,\ \omega,\ \omega\alpha,\ \omega\alpha^2\}.$$

Now we test three permutations of these base vectors to see which are automorphisms. Two general algebraic numbers are

$$N_1 = c_0 + c_1\alpha + c_2\alpha^2 + c_3\omega + c_4\omega\alpha + c_5\omega^2\alpha, \qquad N_2 = d_0 + d_1\alpha + d_2\alpha^2 + d_3\omega + d_4\omega\alpha + d_5\omega^2\alpha.$$

The product of these has 36 terms so I have evaluated their products using algebraic software and report the outcomes.

Permutation 1 : $\theta_1 : \alpha \to \omega\alpha$. Then $\theta(N_1N_2) - \theta(N_1)\theta(N_2) = 0$. This is an automorphism because α and $\omega\alpha$ are both roots of $x^3 - 2 = 0$.
Permutation 2 : $\theta_1 : \alpha \to \omega^2\alpha$. Again $\theta(N_1N_2) - \theta(N_1)\theta(N_2) = 0$. This is also an automorphism for the same reason.
Permutation 3 : $\theta_1 : \alpha \to \alpha^2$. This time $\theta(N_1N_2) - \theta(N_1)\theta(N_2) \neq 0$. This is not an automorphism because α satisfies $x^3 - 2 = 0$ while α^2 satisfies $x^3 - 4 = 0$, both irreducible polynomials.
So while α and α^2 lie in the same field with basis $\{1, \alpha, \alpha^2, \omega, \omega\alpha, \omega\alpha^2\}$, they are not conjugates. Indeed they also lie in the same subfield $\mathbb{Q}(\alpha) \equiv \mathbb{Q}(\alpha^2)$. Denote the roots of $x^2 - 2$ by $\alpha, \omega\alpha, \omega^2\alpha$ and the roots of $x^2 - 4$ by $\beta, \omega\beta, \omega^2\beta$. The fields they generate are isomorphic with $\alpha \leftrightarrow \beta^2$ and $\alpha^2 \leftrightarrow \beta$. In fact $\alpha^2 = \beta$ and $\beta^2 = 2\alpha$.

The subset of automorphisms of a field extension $L : K$ which leave all numbers in the smaller base field K unchanged form a subgroup of all possible automorphisms of L, and is called the Galois group, denoted $\mathcal{G}$.

Automorphisms also exist in groups. In these a group acts in effect on a copy of its own set of elements, permuting them yet preserving the identity, sending elements only to others with the same order, and preserving conjugacy classes. Several examples of group automorphisms are given in Appendix 7. One of the challenges in this subject is to keep a clear distinction between a group (or field) and its group of automorphisms. We are dealing with structures which have some symmetries amongst their elements, and the automorphisms are about how the elements of these structures can be swapped around without effectively doing more than relabel the elements.

This Appendix is about calculating the automorphism group Aut(G) of a group G. It is relevant to the automorphisms of the splitting field extension of a polynomial where the roots of the polynomial have the same symmetries as the elements of the group G.

An automorphism is an isomorphism of the group into itself, that is a mapping of the elements of G which permutes some elements of G in such a way as to maintain the algebraic relations amongst the group's elements. The isomorphism means that if ϕ is a mapping of group elements g_k into other group elements, then $\phi(g_1g_2) = \phi(g_1)\phi(g_2)$. This means that the actions of multiplying elements and of applying the mapping commute – the order of application does not affect the result.

To be clear, some groups describe the symmetries of regular objects such as a rectangle, square or hexagon. The disposition of these physical objects can be described by the positions of their vertices provided these are labelled. The vertices are just a set, not a group; it is their symmetry operations – rotations, reflections, etc. – which form a group, G. Pair-wise combinations of G's symmetry elements, $g_ig_j = g_k$, can be set out in a multiplication or composition table. An automorphism is a swapping of these group elements which does not change the relations in the composition table – it is just a relabelling of the symmetry operations. Clearly symmetry elements can be interchanged only if they have the same order, and one generator of the group can be exchanged only with another. The automorphisms themselves have their own symmetries and so form a group, Aut(G). Any group G will have its automorphism group, whether G can be represented as the symmetries of a regular physical object or is a purely abstract group.

Automorphisms of $C_2 \times C_2$: This is the Viergroupe, the symmetries of a playing card, a non-square rectangle. If its four corners are labelled 1, 2, 3, 4, two reflections in the long and short sides are permutations $a = (12)(34)$ and $b = (14)(23)$, and when concatenated as $ab = (13)(24) = ba$ they describe a 180° rotation about the centre. The group is $\{I, a, b, ab\}$. a, b and ab all have order 2. Its multiplication table is:

I	a	b	ab
a	I	ab	b
b	ab	I	a
ab	b	ab	I

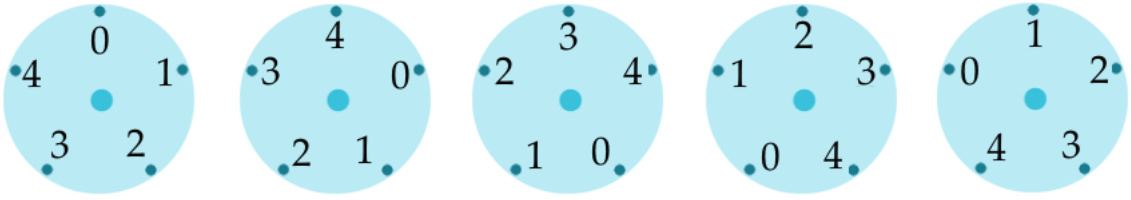

Figure 16: Symmetries of a 5-hour clock.

It is clear that this structure is not changed if a and b are interchanged provided that $ba = ab$ as is the case. Indeed all permutations of the three elements a, b and ab leave the structure of the table unchanged. There are $3! = 6$ such permutations. We conclude that $\mathrm{Aut}(C_2 \times C_2) = S_3$, the symmetric group on 3 elements. The automorphisms are the identity plus the permutations $(a\ b)$, $(a\ ab)$, $(b\ ab)$, $(a\ b\ ab)$, $(a\ ab\ b)$. $\mathrm{Aut}(C_2 \times C_2)$ can be presented as $< s^3, t^2, ts = s^2t >$ where $s = (a\ b\ ab)$ and $t = (a\ b)$. The elements are I, s, $s^2 = (a\ ab\ b)$, t, $st = (a\ ab)$ and $s^2t = (b\ ab)$.

We have here two groups: $C_2 \times C_2$ describing the symmetries of a rectangle, and $\mathrm{Aut}(C_2 \times C_2) = S_3$ acting to permute the symmetry elements in $C_2 \times C_2$ without disturbing its structure.

Automorphisms of C_5: C_5 is the cyclic group of five members, $\{I = a^5,\ a,\ a^2,\ a^3,\ a^4\}$ and can be generated by any of a, a^2, a^3, a^4. Since an automorphism can only send one generator to another, there are only four automorphisms of C_5:

$$s_1 : a \to a, \qquad s_2 : a \to a^2, \qquad s_3 : a \to a^3, \qquad s_4 : a \to a^4.$$

To explore this more deeply I will discuss the automorphisms of C_5 in two further ways. First take 0, 1, 2, 3, 4 to be equally spaced positions around a 5-hour clock. The symmetries of this object, which form the cyclic group of operations C_5, are rotations in increments of one 'hour', two, three and four 'hours'. Figure 15 shows the five distinct orientations resulting from the actions of C_5's members, and the permutation notation for each action. These permutations suggest four ways in which the composition table for the elements 0 to 4 can itself be permuted. The tables for addition of hours under these permutations are as follows:

0	1	2	3	4
1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3

0	2	4	1	3
2	4	1	3	0
4	1	3	0	2
1	3	0	2	4
3	0	2	4	1

0	3	1	4	2
3	1	4	2	0
1	4	2	0	3
4	2	0	3	1
2	0	3	1	4

0	4	3	2	1
4	3	2	1	0
3	2	1	0	4
2	1	0	4	3
1	0	4	3	2 .

These four tables have the same form, with diagonals of the same numbers running SW to NE. Each table is just a relabelling of another. They display the four automorphisms of C_5. Since all '0's stay in the same places in each of these tables, the automorphisms can be regarded as permutations of only the four labels '1', '2', '3', '4'. If s denotes (1243), then s^2 =(14)(23), s^3 =(1342) and $\mathrm{Aut}(C_5) = C_4$ with members $\{I, s, s^2, s^3\}$.

The second way of looking at the automorphisms emphasises that they preserve structural relations amongst the elements. Take the cyclic group to have elements $\{I = a^5, a, a^2, a^3, a^4\}$. As above, the alternative notation is to denote a^k by its index k and replace multiplication of elements by addition of their indices: $\{0 \equiv 5, 1, 2, 3, 4\}$. This represents C_5 as the finite field $\mathbb{Z}/\mathbb{Z}_5$ under addition. To see why in any homomorphism the identity I cannot be swapped with another element, suppose that I is mapped to a^k and element $a^m \to a^n$. Then

$$\phi(I.a^m) = \phi(a^m) \to a^n \quad \text{but} \quad \phi(I)\phi(a^m) \to a^k.a^n = a^{k+n} \neq a^n \quad \text{unless } k = 0.$$

That means that the automorphisms can involve only permutations of the other four elements, as we saw above. All 4! = 24 permutations are listed in the table below. The starting position is at the top left in red. A mapping of this sequence to itself constitutes the identity permutation. In the identity permutation (in red) the sum of indices in the first two columns equals that in the third column: $1 + 2 = 3 \mod 5$. I have picked out in blue the only other permutations for which this is also true. Now apply to these eight the condition that the sum of indices in the first and third columns equals that in the last: $1 + 3 = 4 \mod 5$. Four more permutations are eliminated by this leaving
We now observe that columns two and four add to column one modulus 5, and in fact this also holds for all four sequences. They correspond to the permutations (in cycle notation)

$$(1)(2)(3)(4), \qquad (1243), \qquad (1342), \qquad (14)(23)$$

respectively, just the ones found by in the first approach. They have orders 1, 4, 4, and 2 respectively.

This example of $\mathrm{Aut}(C_5) = C_4$ illustrates the general case that $\mathrm{Aut}(C_p) = C_{p-1}$ for p a prime. If the group has a non-prime number n of elements, its automorphism group has $\phi(n)$ elements where $\phi(n)$ is the Euler totient function which counts the numbers of integers relatively prime to n. The reason is that in C_n there are not $n-1$ generators if n is composite. For example, $C_6 = \{I, a, a^2, a^3, a^4, a^5\}$, but only a and a^5 will generate the whole group by repeated multiplication. a^2 only generates the subgroup $\{I, a^2, a^4\}$ and a^3 only generates $\{I, a^3\}$. $\phi(6) = 2$.

Automorphisms of C_{15} : This is a cyclic group isomorphic to the direct product $C_3 \times C_5$. An automorphism must respect both conjugacy classes and map one generator to another. Consequently there can be no cross-over between the generators of C_3 and those of C_5. Therefore $\mathrm{Aut}(C_3 \times C_5)$ must be the direct product $\mathrm{Aut}(C_3) \times \mathrm{Aut}(C_5)$.

If $C_3 = \{I, a, a^2\}$, then both a and a^2 are generators and there is only one non-identity automorphism θ such that $\theta(a) = a^2$, $\theta(a^2) = a^4 \equiv a \mod 3$. To see that this retains the structure of the group observe that

$$(\theta(a))^2 = (a^2)^2 = a^4 = a = \theta(a^2),$$
$$\theta(a^2).\theta(a^2) = (a)^2 = a^2 = \theta(a) = \theta(a^4) = \theta(a^2.a^2),$$
$$\theta(a).\theta(a^2) = a^2.a = I.$$

1	**2**	**3**	**4**	**2**	**1**	**3**	**4**	3	1	2	4	4	1	2	3
1	2	4	3	2	1	4	3	**3**	**1**	**4**	**2**	4	1	3	2
1	3	2	4	2	3	1	4	3	2	1	4	4	2	3	1
1	**3**	**4**	**2**	2	3	4	1	3	2	4	1	**4**	**2**	**1**	**3**
1	4	2	3	**2**	**4**	**1**	**3**	3	4	1	2	4	3	1	2
1	4	3	2	2	4	3	1	**3**	**4**	**2**	**1**	**4**	**3**	**2**	**1**

1 2 3 4 2 4 1 3 3 1 4 2 4 3 2 1

There are therefore only two automorphisms of C_3, the other being the trivial one, so its automorphism group is C_2: $\mathrm{Aut}(C_3) = C_2$. We have seen above that $\mathrm{Aut}(C_5) = C_4$. Hence $\mathrm{Aut}(C_{15}) = C_2 \times C_4$.

Automorphisms of D_{10}: This is the dihedral group of symmetries of a regular pentagon. It is created by two generators, a and b, with orders 5 and 2 respectively, plus the relation $ba = a^{-1}b = a^4b$, written $G =< a, b \mid a^5, b^2, ba = a^{-1}b >$. Its 10 elements are $\{I, a, a^2, a^3, a^4, b, ab, a^2b, a^3b, a^4b\}$. It has one C_5 subgroup of $\{I, a, a^2, a^3, a^4\}$, and five C_2 subgroups, each I plus one of b, ab, a^2b, a^3b, a^4b. Physically, if a pentagon is drawn around the unit circle, a describes anticlockwise rotation by 72° and b is reflection in the x axis. The relation $ba = a^{-1}b$ means that a 72° anticlockwise rotation then a $y \to -y$ reflection is identical to a reflection then a 72° clockwise rotation. Written in terms of permutations of the pentagon's vertices labelled 1, 2, 3, 4, 5, the rotations are a=(12345), a^2=(13524), a^3=(14253), a^4=(15432) and the reflections, with mirror line passing through vertices 1 to 5 in turn, are b=(24)(34), ba=(13)(45), ba^2=(15)(24), ba^3=(12)(35) and ba^4=(14)(23).

D_{10} is generated by a, $a^5 = I$ and b, $b^2 = I$, but it can equally well be generated by any of a, a^2, a^3, a^4 paired with any of b, ab, a^2b, a^3b, a^4b. There are therefore 20 ways of relabelling the elements – in other words, there are 20 automorphisms. As seen above, there are 4 automorphisms of the C_5 subgroup where a^k is sent to $a^{jk \mod 5}$, $1 \le j \le 4$. Each of these can be combined with one of the reflections, making $5 \times 4 = 20$ automorphisms in total. To make this plain, the table lists the five automorphisms which involve $a \to a^3$.

a series		b series					
$1 \to$	3	$b \to$	b	$1b$	$2b$	$3b$	$4b$
$2 \to$	1	$1b \to$	$3b$	$4b$	b	$1b$	$2b$
$3 \to$	4	$2b \to$	$1b$	$2b$	$3b$	$4b$	b
$4 \to$	2	$3b \to$	$4b$	b	$1b$	$2b$	$3b$
		$4b \to$	2b	$3b$	$4b$	b	$1b$

The notation is that a^k is represented by its index k, so in the a-series panel $1 \to 3$ denotes $a \to a^3$. The reflections are in the b-series panel where b can be sent to any of b, $ab = 1b$, $a^2b = 2b$, $a^3b = 3b$ or $a^4b = 4b$, making the five automorphisms in the blue-text columns. The elements in red are unchanged. There are three similar panels for $a \to a$, $a \to a^2$ and $a \to a^4$. The five rotations, being the elements containing b, form one conjugacy class. a and a^4 are inverses and form another conjugacy class, as do a^2 and a^3. Automorphisms which involve permutations within conjugacy classes are called 'inner automorphisms'. Therefore $a \to a^2$, $a \to a^3$ are outer automorphisms.

Some example calculations will show the homomorphism property. Take $\theta : a \to a^3, b \to ab$ and calculate products both before and after mapping under θ.

$$\theta(ba.a^2) = \theta(a^4b.a^2) = \theta(a^4.a^4b.a) = \theta(a^3.a^4b) = \theta(a^2b) = \theta(2b) = 2b = a^2b$$

$$\text{and} \quad \theta(4b)\theta(2) = 3b.1 = a^3ba = a^3.a^4b = a^2b = 2b$$

so this agrees. Also, using $ba = a^4b$, the following agrees

$$\theta(a^2.a^3b) = \theta(b) = 1b = ab \quad \text{and} \quad \theta(a^2).\theta(a^3b) = a.b \quad \text{and} \quad \theta(a).\theta(a^4b) = a^3.a^3b = ab.$$

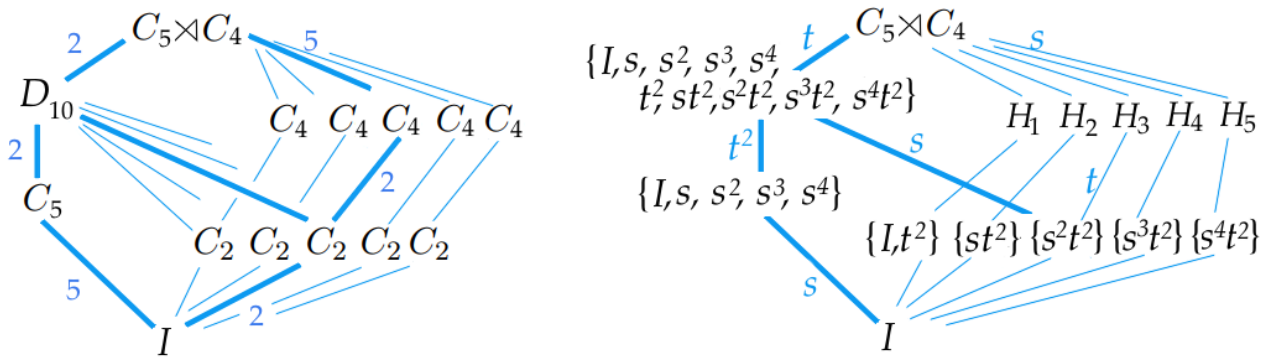

Figure 17: Structure of the group $H_{20} = C_5 \rtimes C_4$ of automorphisms of a pentagon. Group presented as $< s^5 = t^4 = I, ts = s^2t >$. $H_1 = \{I, t, t^2, t^3\}$, $H_2 = \{I, s^2t, st^2, s^4t^3\}$, $H_3 = \{I, s^3t^3, s^2t^2, s^4t\}$, $H_4 = \{I, st, s^3t^2, s^2t^3\}$, $H_5 = \{I, st^3, s^4t^2, s^3t\}$.

as does

$\theta(a^2b.a^3) = \theta(a^4b) = a^3b$ and $\theta(a^2)\theta(ba^3) = \theta(a^2)\theta(a^2b) = a.a^2b = a^3b$ and $\theta(a^2b)\theta(a^3) = a^2b.a^4 = a^3b$.

Group H_{20} of 20 elements, the automorphism group of D_{10}, is quite a complicated object. Its structure is shown in Figure 16, which is equivalent to Figure 7 in the main text. It has the presentation[18] $< s^5 = t^4 = I,\ ts = s^2t >$ and can be studied using the WordGroups or PermGroups computer programs available at *www.mathstudio.co.uk* in the Group Theory section. In the diagram on the right the numbers on the blue connecting lines give the factor by which the order of subgroup increases. In the right panel the elements added to form the next level of subgroups are written on the blue lines. The braces {..} denote elements within the subgroups. The C_5 cyclic subgroup has elements $\{I, s, s^2, s^3, s^4\}$ and the five elements of order 2 are t^2 and its products with the powers of s. These 10 elements together form the D_{10} dihedral group of symmetries of a regular pentagon. There are five subgroups of order 4 constructed from the powers of t with the powers of s such as $\{I, st, s^3t^2, s^2t^3\}$. It is an example of a Frobenius group and the holomorph of the cyclic group C_5, the holomorph being the semi-direct product of C_5 and its automorphism group C_4: $H_{20} = \text{Hol}(C_5) = C_5 \rtimes C_4$. I leave further exploration of these qualities to the interested reader.

[18] I am using s and t for generators of the automorphism group to avoid confusion with the a and b which generated the parent group D_{10}.

Appendix 9: Symmetric polynomials and primitive elements

If $P(x)$ is written as at Eq 2 as a product of factors $x - \alpha_j$ over all the roots α_j and expanded, the coefficients of x^k are seen to be sums of products of the α_j. This is shown at Eq 4 for the case of $n = 5$. The important property of these sums of products is that they are symmetrical in the roots α_j. Any permutation of the indices j leaves the coefficients unchanged in value. For example, for $n = 5$ the coefficient of x is

$$\alpha_1\alpha_2\alpha_3\alpha_4 + \alpha_1\alpha_2\alpha_3\alpha_5 + \alpha_1\alpha_2\alpha_4\alpha_5 + \alpha_1\alpha_3\alpha_4\alpha_5 + \alpha_2\alpha_3\alpha_4\alpha_5.$$

The permutation (134) converts this to

$$\alpha_3\alpha_2\alpha_4\alpha_1 + \alpha_3\alpha_2\alpha_4\alpha_5 + \alpha_3\alpha_2\alpha_1\alpha_5 + \alpha_3\alpha_4\alpha_1\alpha_5 + \alpha_2\alpha_4\alpha_1\alpha_5$$

which is numerically identical; the five terms have just been rearranged from the order [a b c d e] to [a e b d c].

This property has many powerful consequences. Any polynomial $R(\alpha_1, \alpha_2, ...\alpha_n)$ which is symmetric in the roots α can be written in terms of a polynomial $C(c_1, c_2, ...c_n)$ in the coefficients of $P(x)$. (Here I am writing $P(x) = x^n + c_{n-1}x^{n-1} + ... + c_1x + c_0$ so that they appear distinct from the roots α.) C is not generally symmetric in the c_k. Because of this property it is possible to determine the splitting field of $P(x)$ without knowing its roots, using just the dual relations between roots and coefficients. From this the Galois group of $P(x)$ can be found. This in turn may reveal a composition series in the subfields which presents a path to solving $P(x) = 0$ in radicals, assuming it is soluble.

There are many examples in the literature of the duality of $R(\alpha_1, \alpha_2, ...\alpha_n)$ and $C(c_1, c_2, ...c_n)$, but a couple more here will not be amiss.
Example : Take $P(x)$ to be the irreducible cubic $x^3 - 2x^2 + 3x - 5$ so $c_2 = -2$, $c_1 = 3$, $c_0 = -5$. Find

$$W = \alpha_1^3\alpha_2 + \alpha_2^3\alpha_3 + \alpha_3^3\alpha_1 + \alpha_1^3\alpha_3 + \alpha_2^3\alpha_1 + \alpha_3^3\alpha_2$$

in terms of the c_k. The numerical values of the roots are $\alpha_1 = 1{\cdot}8437$, $\alpha_2 = 0{\cdot}0781 + 1{\cdot}6449i$, $\alpha_3 = \alpha_2^*$. Direct calculation shows that $W = -16$. It is the fact that W is symmetrical in the roots that ensures that it lies in $\mathbb{Q}$. If W were not symmetric, its transformed version would involve not just the c_k but also one or more of the roots α_j. We will now derive that $W = -2c_1^2 - c_0c_2 + c_1c_2^2$. One could try by-hand algebraic manipulation, but there is a systematic way to achieve the result.

An algorithm

I will illustrate this using the above example of a cubic.
Stage 1 : For each x^j subtract the symmetric polynomial in the roots from the corresponding coefficient. These differences are all zero.

$$d_2 = c_2 + (\alpha_1 + \alpha_2 + \alpha_3) = 0, \qquad d_1 = c_1 - (\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1) = 0, \qquad d_0 = c_0 + \alpha_1\alpha_2\alpha_3 = 0\,.$$

Stage 2 : Eliminate α_3 from d_1 by writing $d_1 = g_1(\alpha_3)d_2 + r_1$. Even though d_2 is zero this can be done by polynomial division $d_1/d_2 = g_1$ remainder r_1 in which d_1, d_2 are regarded as polynomials in the variable α_3. Since d_1 is also zero, r_1 must also be zero. The division can be done in Mathematica with the `PolynomialRemainder[..]` function and in Maxima with `divide`. The result is

$$\frac{d_1(\alpha_3)}{d_2(\alpha_3)} = \frac{c_1 - \alpha_1\alpha_2 - \alpha_2\alpha_3 - \alpha_3\alpha_1}{c_2 + \alpha_1 + \alpha_2 + \alpha_3} \;=\; -\alpha_1 - \alpha_2 \text{ remainder } r_1 = c_1 + (\alpha_2 + \alpha_1)c_2 + \alpha_2^2 + \alpha_1\alpha_2 + \alpha_1^2.$$

The same is done with d_0:

$$\frac{d_0(\alpha_3)}{d_2(\alpha_3)} \;=\; \alpha_1\alpha_2 \text{ remainder } r_0 = c_0 - c_2\alpha_1\alpha_2 - \alpha_1\alpha_2^2 - \alpha_1^2\alpha_2.$$

Finally eliminate α_2 from d_0 by dividing by r_0 by r_1. (Since this is zero in a computer implementation it is convenient to relabel r_1 as a new d_1 and r_0 as a new d_0.)

$$\frac{r_0(\alpha_2)}{r_1(\alpha_2)} = \frac{c_0 - \alpha_1\alpha_2c_2 - \alpha_1\alpha_2^2 - \alpha_1^2\alpha_2}{c_1 + (\alpha_2+\alpha_1)c_2 + \alpha_2^2 + \alpha_1\alpha_2 + \alpha_1^2} \;=\; -a_1 \text{ remainder } c_0 + c_1\alpha_1 + c_2\alpha_1^2 + \alpha_1^3.$$

This last remainder is clearly zero because it is the original cubic with the root α_1 in place of x. We now have three expressions, all zero, which relate the coefficients to the roots, but arranged so that the new d_0 (previous r_0) contains only α_1, the new d_1 contains only α_1 and α_2, and d_2 still contains all three. For an nth order polynomial there will be n quantities d_j in such a hierarchy. For the cubic they are

$$d_2 = c_2 + \alpha_1 + \alpha_2 + \alpha_3, \qquad d_1 = c_1 + c_2(\alpha_1+\alpha_2) + \alpha_1^2 + \alpha_1\alpha_2 + \alpha_2^2, \qquad d_0 = c_0 + c_1\alpha_1 + c_2\alpha_1^2 + \alpha_1^3.$$

Stage 3 : We are given an arbitrary expression W which is symmetric in the roots and use division by the three final d_j values obtained in Stage 2 to eliminate one α_k at a time until W has been converted to an expression solely in the coefficients c_k. The three stages eliminate α_3, α_2, then α_1 in turn. Regarded as polynomials in α_3 the division $\frac{W(\alpha_3)}{d_2(\alpha_3)}$ leaves remainder R_2 =

$$-c_2^3\alpha_1 - 3c_2^2\alpha_1^2 - 4c_2\alpha_1^3 - 2\alpha_1^4 - c_2^3\alpha_2 - 6c_2^2\alpha_1\alpha_2 - 9c_2\alpha_1^2\alpha_2 - 4\alpha_1^3\alpha_2 - 3c_2^2\alpha_2^2 - 9c_2\alpha_1\alpha_2^2 - 6\alpha_1^2\alpha_2^2 - 4c_2\alpha_2^3 - 4\alpha_1\alpha_2^3 - 2\alpha_2^4$$

$$\frac{R_2(\alpha_2)}{d_1(\alpha_2)} \text{ leaves remainder } R_1 = -2c_1^2 + c_1c_2^2 + c_1c_2\alpha_1 + c_2^2\alpha_1^2 + c_2\alpha_1^3$$

$$\frac{R_1(\alpha_1)}{d_0(\alpha_1)} \text{ leaves remainder } R_0 = -2c_1^2 - c_0c_2 + c_1c_2^2$$

which is the result quoted for the Example above; it W in terms of the coefficients.

A theorem of Lagrange

This clever theorem involving symmetric polynomials was published by Lagrange in 1770. He was Italian but a naturalised French citizen, and a contemporary of the composer Joseph Haydn. It concerns arbitrary (non symmetric) polynomials Q and R formed from the roots α_j of an nth degree polynomial $P(x)$. If now the roots are permuted by all $n!$ permutations of the S_n symmetry group, $n!$ distinct versions of Q and R will be formed: label these Q_j, R_j, $1 \le j \le n!$. It is important that they are all different. The theorem states that two further polynomials $H(u)$ and $K(u)$ can be derived such that, for every permutation σ_k

$$Q_k.K(R_k) = H(R_k).$$

The same $H(u)$ and $K(u)$ apply for all permutations. Moreover, the symmetries of the roots means that the coefficients of both $H(u)$ and $K(u)$ can be expressed solely in terms of the coefficients of $P(x)$.

The expressions become too long and unwieldy for demonstration purposes if $P(x)$ has even cubic degree, so we will just take $P(x) = x^2 + c_1x + c_0$. Suppose that under the two permutations of S_2 Q and R take the values :

$$Q_1 = 2\alpha_1 - \alpha_2^2, \qquad R_1 = \alpha_1^2 - 3\alpha_2,$$

$$Q_2 = 2\alpha_2 - \alpha_1^2, \qquad R_2 = \alpha_2^2 - 3\alpha_1.$$

To be clear, the roots need not be known – they are unknown algebraic numbers. Form the product

$$\phi(u) \;=\; (u - R_1)(u - R_2) \;=\; u^2 + [3(\alpha_1 + \alpha_2) - \alpha_1^2 - \alpha_2^2]u + [9\alpha_1\alpha_2 + \alpha_1^2\alpha_2^2 - 3(\alpha_1^3 + \alpha_2^3)].$$

Take $K(u)$ to be the derivative of $\phi(u)$:

$$K(u) = \frac{d\phi(u)}{dv} \;=\; 2u + [3(\alpha_1 + \alpha_2) - \alpha_1^2 - \alpha_2^2].$$

Its degree is 1 less than that of $\phi(u)$, so is $n-1$. H is formed by deleting from $\phi(u)$ each linear factor $(u - R_j)$ in turn and replacing it with Q_j, then summing all such products. In this quadratic case

$$H(u) = Q_1(u-R_2)+(u-R_1)Q_2 \;=\; [2(\alpha_1+\alpha_2)-(\alpha_1^2+\alpha_1^2)]u+[6(\alpha_1^2+\alpha_2^2)-5(\alpha_1^2\alpha_2+\alpha_1\alpha_2^2)+\alpha_1^4+\alpha_2^4].$$

Since Q does not contain v, the degree of $H(u)$ is also $n-1$. From these

$$K(R_1) \;=\; 3(\alpha_1 - \alpha_2) + \alpha_1^2 - \alpha_2^2, \qquad K(R_2) = 3(\alpha_2 - \alpha_1) + \alpha_2^2 - \alpha_1^2,$$

$$Q_1K(R_1) \;=\; -6\alpha_1\alpha_2 - 5\alpha_1\alpha_2^2 - \alpha_1^2\alpha_2^2 + 2\alpha_1^3 + 3\alpha_2^3 + \alpha_2^4 \;=\; H(R_2)$$

and $Q_2K(R_2)$ is the same with the indices 1 and 2 interchanged. Of course, $H(R_j)$, $K(R_j)$ are not symmetric because the chosen Q, R were not, but the coefficients of both $H(u)$ and $K(u)$ are symmetric and therefore can be expressed in terms of the coefficients of $P(x)$.

$$H(u) = (2c_0 - 2c_1 - c_1^2)u \;+\; 2c_0^2 + c_0(-12 + 5c_1 - 4c_1^2) + c_1^2(6 + c_1^2)$$

$$K(u) \;=\; 2u + 2c_0 - 3c_1 - c_1^2.$$

To put in some numbers, suppose $P(x) = x^2 - 2x - 5$ so that $\alpha_1 = 1 + \sqrt{6}$, $\alpha_2 = 1 - \sqrt{6}$. Then $H(u) = 10(28 - u)$, $K = 2u - 8$,

$$Q_1 = -5 + 4\sqrt{6}, \quad Q_2 = -5 - 4\sqrt{6}, \quad R_1 = 4 + 5\sqrt{6}, \quad Q_2 = 4 - 5\sqrt{6},$$

$$K(R_1) = 10\sqrt{6}, \quad Q_1K(R_1) = 10(24 - 5\sqrt{6}) = H(R_1)$$

and similarly for R_2. Also $2c_0 - 3c_1 - c_1^2 = -8$, the constant term of $K(u)$, $2c_0 - 2c_1 - c_1^2 = -10$, the coefficient of u in $H(u)$, and finally the constant term is $2c_0^2 + c_0(-12 + 5c_1 - 4c_1^2) + c_1^2(6 + c_1^2) = 280$.

The theorem becomes empty of content if any two or more of the Q_j or R_j are the same. For example, R_1 will equal R_2 above if both are symmetrical in α_1, α_2. Then R_1 is a rational number and $H(R_1) = H(R_2) = K(R_1) = K(R_2) = 0$.

Appendix 10: Cycle type & theorems by Dedekind, Frobenius and Chebotaryov

First I explain what is meant by the 'cycle type' of a permutation. A cycle is a permutation such as (12), (354), (14573) in which the the stated elements move one place to the right and the rightmost element reappears at the leftmost position; the elements move one place around a loop. These examples are respectively a 2-cycle, a 3-cycle and a 5-cycle. Any permutation can be written as a unique product of disjoint cycles – ones which have no elements in common. Thus (12)(46), (124)(6375) are disjoint cycles of types $[2,2]$ and $[3,4]$ respectively, where the type is labelled by the number of elements in each constituent cycle, in ascending order. The cycle (1)(2)(5)(7) does not change any elements so any cycle of type $[1,1,1,...,1]$ represents the identity permutation.

Dedekind discovered the following remarkable and beautiful result. Let $P(x)$ be an irreducible polynomial over $\mathbb{Q}$ and let G be its Galois group. Factorise $P(x)$ modulo any prime p and note the degree of each polynomial factor. If the degrees of these factors are d_1, d_2, ..., d_k, then G contains a subgroup whose permutation cycle type is $[d_1, d_2, ..., d_k]$. Amazing! Below are some examples.

The method for finding the Galois group based on this and related theorems by Frobenius and Chebotaryovrelies on algorithms to calculate the discriminate of $P(x)$ and to factorise it modulo any prime. At the end of this Appendix I have added some notes on these essential supporting algorithms.

Example 1 : Take the polynomial $x^4 - 4x^3 + 4x^2 + 12x + 5$ which was used in §5. It factors mod p as follows:

$$\text{mod } 5 \ : \ x(x+2)(x^2+4x+1) \ \Rightarrow \ \text{cycle type } [1,1,2],$$

$$\text{mod } 17 \ : \ (x^2+6x+2)(x^2+7x+11) \ \Rightarrow \ \text{cycle type } [2,2],$$

$$\text{mod } 29 \ : \ (x+13)(x+19)(x+24)(x+27) \ \Rightarrow \ \text{cycle type } [1,1,1,1],$$

$$\text{mod } 31 \ : \ x^4 - 4x^3 + 4x^2 + 12x + 5 \Rightarrow \ \text{cycle type } [4].$$

This tells us that the Galois group has subgroups with types (ab), $(ab)(cd)$, I = () and $(abcd)$ respectively. A search of other primes yields no other types. So already we know a lot about this Galois group.

If $P(x)$ is factored over quite a lot of primes – 50 or more – you can observe the frequency with the various sets of degrees d_1, d_2, ... d_k occur. d_1, d_2, ... d_k add to n, the degree of $P(x)$, and so $[d_1, d_2, ..., d_k]$ is a partition of n. For example, over the primes up 239 $x^4 - 4x^3 + 4x^2 + 12x + 5$ factors into 4 of the identity type, 12 of type $[1,1,2]$, 18 of type $[2,2]$ and 15 of type $[4]$. There are 52 primes up to 239, but the wisdom is not to include those which divide the discriminant of $P(x)$. Here this is $29952 = 2^8.3^2.13$, so 2, 3 and 13 are deleted from the list, leaving 49 primes. (Ways of calculating the discriminant and of factorising polynomials are mentioned in the next subsection.) Are these random statistics? Frobenius showed that the probability of factorisation mod p implying a particular cycle type T, tends asymptotically to the ratio

$$\frac{\#T}{\#p} \ = \ \frac{\#C}{|G|}$$

as $p \to \infty$. Here $\#p$ is the number of primes less than a limit p_{max}, $\#T$ is the number of cycles of type T within that range, $|G|$ is the order of the Galois group, and $\#C$ is the number of elements

in G with cycle type T. $\#C$ can also be regarded as the size of the conjugacy class with that cycle stricture.

Applying this to the numbers above, $4:49$ for I is about 1:12, and $12:49$ for $[1,1,2]$ is 1:4. The ratio $\#T:\#p$ is called the 'density' of the cycle type, and it can only be approximated by taking p_{max} be to large. I recalculated the frequencies for $p_{max} = 1993$, which is 297 primes excluding 2, 3 and 13. The respective estimates of densities are

type, T	$\#T$	$\#p/\#T$
$[1,1,1,1]$	35	$8\cdot5$
$[1,1,2]$	76	$3\cdot9$
$[2,2]$	111	$2\cdot7$
$[4]$	75	$4\cdot0$

So the conjugacy class $I \equiv [1,1,1,1] \equiv ()$ occurs at the rate of $35/297 = 1/8\cdot5$ of the order of the G. But in any group the identity occurs only once, so $|G|$ must be about 1×8.5, consistent with D_8 having 8 elements. The number of elements of type $[4] \equiv (abcd)$ occurs $75/297 \approx 1/4$ the order of G, which is $8/4 = 2$. Similarly the conjugacy class with permutation type (ab) also occurs twice. Type $(ab)(cd)$, with cycle type $[2,2]$, occurs about $8/2\cdot7 \approx 111/35 \approx 3$ times. If you look back at §5, you will see that there are two 4-cycles, (1234), (1432), two 2-cycles, (13), (24), and three 2-2-cycles, (12)(34), (13)(24), (14)(23). This agrees with the cycle density predictions.

Example 2 : Now apply this to x^5-3 which was studied in §7. The discriminant is $253125 = 3^4.5^5$ so 3 and 5 have been deleted as they do not give valid information. Factorisation modulo the first 400 primes results in only four partitions of $n = 5$ as cycle types $[1,1,1,1,1]$, $[1,2,2,]$, $1,4]$ and $[5]$. There is no type $[1,1,1,2]$ nor $[2,3]$. Their frequncies are

type, T	$\#T$	$\#p/\#T$
$[1,1,1,1,1]$	20	$19\cdot8$
$[1,2,2]$	96	$4\cdot1$
$[1,4]$	204	$1\cdot9$
$[5]$	76	$5\cdot2$

From these we expect $|G| = 20$, $20/4\cdot1 \approx 5$ instances of the permutation type $(ab)(cd)$, $20/1\cdot9 \approx 10$ instances of the permutation type $(abcd)$, and $20/5\cdot2 \approx 4$ instances of the 5-cycle $(abcde)$. There are five groups of order 20, of which the Frobenius group $\mathrm{Hol}(C_5)$ has 5 elements of order 2, 10 of order 4, and 4 of order 5, again in remarkable agreement.

This theory has been developed into a computer-based algorithm for determining Galois groups, named after the Ukranian Nikolai Chebotaryov who developed his density theorem in 1922. This is an extension of Frobenius' theorem. The method clearly depends on the speed with which a computer can factorise $P(x)$ over finite fields, and on how large p_{max} must be to obtain a sufficiently robust estimate of the limiting cycle type densities. The method has been coded in Mathematica and evaluated against Stauduhar's method in the thesis by Tessa Wildsmith of Portsmouth University. She judges that it is applicable only to polynomials of low degree – say up to 6 or 7. It is essential that enough identity cycles $[1,1,...,1]$ be obtained for $|G|$ to be estimated, and if $|G|$ is large such identities will occur very infrequently. She uses $p_{max} = 10,000$.

Example 3 : I checked this myself by examining about twenty degree-7 polynomials of the form x^7-ax^2+bx+c but failed to find one which had the identity factorisation within the first 500 primes.

7! = 5040 so over 5000 primes would have to be examined if the Galois group were S_7. Nevertheless I have obtained, out of interest, the frequencies of the various cycles types for one polynomial, $x^7 - 5x^2 - x + 1$, on the grounds that there might be helpful integer relations between them. The table below lists, for all cycles types obtained, the number observed, $\#C$, and the ratio of this to $\#p = 598$.

type	7	1,6	3,4	2,5	1,1,5	111,4	1,2,4	1,2,2,2	2,2,3	1,1,2,3	111,2,2	1111,3
$\#C$	100	97	58	61	64	26	66	15	52	42	12	5
$\#p/\#C$	6.0	6.2	10.3	9.8	9.4	23.0	9.1	39.9	11.5	14.3	49.9	119.8

Table 3: Observed number of cycle types in $x^7 - 5x^2 - x + 1 \mod p$ in over 598 primes up to 4441 excluding 2 and 163.

It would require much mathematical detective work to identify the Galois group from this. We do know that G is either S_7, order 5040, or one of its subgroups. The discriminant has the value $1124702608 = 2^4.163.431251$ and is not a perfect square, so G cannot be either the alternating group A_7 or one of its subgroups. The failure to observe the identity permutation over 600 primes suggests that $|G| > 360$. The list above shows that G contains cycles of lengths 7, 6, 5, 4, and 3, and the number of 3 cycles is 120/6 = 20 times more than the number of 6 or 7 cycles. There are a few other suggestive ratios.

Fortunately for group S_7 the size of each conjugacy class can be calculated in terms of factorials and these are tabulated on the internet at *groupprops.subwiki.org/wiki/Symmetric_group:S7*. For example there are 720 7-cycles, 840 6-cycles, 504 5-cycles, 210 4-cycles and only 70 3-cycles. I tabulated the ratio of occurrence for every pair of cycle types in the data above for x^7-5x^2-x+1, and did the same with the published values for S_7. The difference in these experimental and theoretical ratios are given in Table 4, as percentages. Where the observed numbers of the two cycle types in each ratio are large, the agreement is quite close, but is wildly different when one of the observed frequencies is small. That is why most of the values highlighted in blue are towards the bottom of the table. So is the Galois group S_7? Probably. It is almost certain that x^7-5x^2-x+1 is not soluble in radicals.

	7	1 6	3,4	2,5	1 1 5	1,1,1,4	1,2,4	1,2,2,2,	2,2,3	1123	11122
1 6	17										
3,4	1	-33									
2,5	21	-8	12								
1 1 5	13	-15	7	-5							
1,1,1,4	42	-27	23	-5	6						
1,2,4	37	14	21	12	17	6					
1,2,2,2,	-19	**-153**	-13	**-73**	**-53**	-27	**-160**				
2,2,3	**-151**	**-213**	**-88**	**-123**	**-117**	**-50**	**-173**	-21			
1123	**67**	31	38	25	32	12	7	11	**74**		
11122	**148**	8	**83**	28	**53**	17	**-50**	25	**233**	**-50**	
11113	**971**	**740**	**560**	**500**	**560**	**220**	**420**	**150**	**740**	**240**	**90**

Table 4: The difference between the relative frequencies of cycles types in numerical data and the theoretical values of S_7. Values are percentage difference in ratio. Values over 50% are emphasised in blue.

Example 4 : In his paper Richard Stauduhar uses his own method to find the Galois group of $P(x) = x^6 - 32x^4 + 160x^3 - 320x^2 + 384x - 256$. The discriminant is $2^{42}.3^2.101^2$, a perfect square, and so G is either the alternating group A_6 or one its subgroups. I factorised $P(x)$ modulo all 599 primes up to 4441 and found only the identity and three other conjugacy classes. The frequencies are in the table: Since the identity [1111] occurs with frequency about 1/28 in G, and there is only

type	[3,3],	[2,4]	[1122]	[1111]
number, $\#C$	209	158	211	21
$\#C/\#p$	$0 \cdot 35$	$0 \cdot 26$	$0 \cdot 35$	$0 \cdot 035$
$\#p/\#C$	$2 \cdot 9$	$3 \cdot 8$	$2 \cdot 8$	$28 \cdot 5$

one identity, the order of G must be 28, within the statistical spread of the sample of primes used. Since 28 does not divide 6!, $|G|$ is probably either 30 or 24. The table on Figure 18 at the very end of this document states that S_6 dos not have a subgroup of order 30, but that the group labelled S_4 (a) with 24 elements has only three other conjugacy classes of types [3,3], [2,4], [2,2], exactly those found. Note that all these are even permutations; this is because they are conjugacy classes within A_6. Taking G to be 24, the above statistics predicts the number of elements with [3,3] cycle structure to be $8 \cdot 4$, those with [2,4] to number $6 \cot 3$, and the [1122]=[2,2] type to number $8 \cdot 4$. Figure 18 gives the theoretical values of S_4 to be 8,6 and 9 respectively.

Since S_4 is a soluble group, there is a chance that this sixth degree polynomial can be solved in radicals. The following normal sequence has abelian quotient groups:

$$I \subset C_2 \subset V_4 \subset A_4 \subset S_4$$

where $V_4 = C_2 \times C_2$ is the Klein V-group. The degrees of each of the corresponding field extensions will be 2, 2, 3 and 2, suggesting that the solution will look something like $\sqrt{(}b_4 + \sqrt[3]{(}b_3 + \sqrt{(}b_2 + \sqrt{b_1})))$. Stauduhar, however, does not quote a solution in radicals and I have not looked hard for it.

Calculating the discriminant Δ

The discriminant of a monic polynomial $P(x)$ with roots $\alpha_1, ...\alpha_n$ is

$$\Delta(P) = (-1)^{n(n-1)/2} \prod_{i,j,i\neq j}^{i=n,j=n} (\alpha_i - \alpha_j) = \prod_{i,j<i}^{i=n,j=n-1} (\alpha_i - \alpha_j)^2 .$$

It carries information about the roots: i) if $\Delta(P) = 0$, there are repeated roots, ii) if $\Delta > 0$, all roots are real, iii) if $\Delta < 0$, there is at least one pair of complex conjugate roots. There is a related quantity often defined which I will call $\delta(P)$ and which is the signed square root of Δ:

$$\delta(P) = \prod_{i,j<i}^{i=n,j=n-1} (\alpha_i - \alpha_j), \qquad \Delta = \delta^2.$$

Since $\delta^2 = \Delta$ and $\Delta \in \mathbb{Q}$, $\delta(P)$ will be either a purely real number or a purely imaginary number.

Since the roots are not usually known, it is essential that Δ can be computed from the coefficients only. We are assured that Δ can be expressed in terms of the coefficients of $P(x)$ because it is clearly a symmetric function of the roots. For all but equations of degree 2 and 3, however, this is not an efficient method. This is largely because the number of terms in Δ increases

rapidly with degree n, from 2 terms for a quadratic, 5 for a cubic, 16 for a quartic, 59 for a quintic and 246 for a 6th degree polynomial. A faster method has been found using the so-called Sylvester matrix.

In its general form the Sylvester matrix is associated with the so-called 'resultant' or 'eliminant' of two polynomials, P and Q. The resultant $Res(P,Q)$ is the determinant of a matrix in the coefficients of both P and Q such that if P and Q share a roots in common, the $Res(P,Q) = 0$. If

$$P = p_n x^n + p_{n-1}x^{n-1} + ... + p_1 x + p_0, \qquad Q = q_m x^m + p_{m-1}x^{m-1} + ... + q_1 x + q_0,$$

then $Res(P,Q)$ is the determinant of the $n+m$ square matrix constructed from successively shifted rows of the two sets of coefficients:

$$\begin{pmatrix}
p_n & p_{n-1} & p_{n-2} & .... & .... & 0 & 0 & 0 \\
0 & p_n & p_{n-1} & p_{n-2}.... & & .... & 0 & 0 \\
0 & 0 & p_n & p_{n-1} & p_{n-2}.... & & .... & 0 \\
... & ... & ... & ... & ..... & & ... & ... \\
0 & 0 & .... & ... & .... & p_2 & p_1 & p_0 \\
q_m & q_{m-1} & q_{m-2} & .... & .... & 0 & 0 & 0 \\
0 & q_m & q_{m-1} & q_{m-2}.... & & .... & 0 & 0 \\
0 & 0 & q_m & q_{m-1} & q_{m-2}.... & & .... & 0 \\
... & ... & ... & ... & ..... & & ... & ... \\
0 & 0 & .... & ... & .... & q_2 & q_1 & q_0
\end{pmatrix}$$

There are m rows from P and n from Q. The discriminant of $P(x)$ is the resultant of $P(x)$ and its derivative, $P'(x)$. The reason is that if $P(x)$ has a double factor $(x-\alpha_k)^2$, its derivative will share the factor $x-\alpha_k$. Thus to calculate Δ for the polynomial $x^4 - 4x^3 + 4x^2 + 12x + 5$ studied in §5 we have $n = 4$ and $m = 3$ so the 7×7 Sylvester matrix is

$$\begin{pmatrix}
1 & -4 & 4 & 12 & 5 & 0 & 0 \\
0 & 1 & -4 & 4 & 12 & 5 & 0 \\
0 & 0 & 1 & -4 & 4 & 12 & 5 \\
4 & -12 & 8 & 12 & 0 & 0 & 0 \\
0 & 4 & -12 & 8 & 12 & 0 & 0 \\
0 & 0 & 4 & -12 & 8 & 12 & 0 \\
0 & 0 & 0 & 4 & -12 & 8 & 12
\end{pmatrix}.$$

Its determinant is fairly readily evaluated with computer software and has the value 29952.

Some explanation is needed as to why Δ is a positive perfect square if the Galois group is an alternating group A_n or one of its subgroups. This requires that $\delta(P)$, defined above, be a rational number. If it is rational, in the base field $\mathbb{Q}$, all permutations within the Galois group must by definition leave $\delta(P)$ unchanged. Now if θ is a permutation within G, its effect on $\delta(P)$ is either to leave it unchanged or to multiply it by -1, depending on whether θ is an even permutation like (123) or an odd one like (1325). So δ will remain unchanged if G consists only of even permutations, which is the definition of the alternating group A_n and its subgroups. Therefore $\delta(P)$ can be rational only if G is A_n and then $\Delta = \delta^2$ is a perfect square.

The column (!) is marked with a (*) if the group is not solvable, and is marked with (□) if it is a subgroup of A_n.

- For degree 3, there are 2 transitive subgroups of S_3, with generators and cycle types as follows:

#	Order	!	Name	Generators	1	2	3
3T1	3	□	A_3	(123)	1		2
3T2	6		S_3	(123), (12)	1	3	2

- For degree 4, there are 5 transitive subgroups of S_4, with generators and cycle types as follows:

#	Order	!	Name	Generators	1	2	2,2	3	4
4T1	4		C_4	(1234)	1		1		2
4T2	4	□	V_4	(12)(34), (13)(24)	1		3		
4T3	8		$D_{2\cdot 4}$	(1234), (13)	1	2	3		2
4T4	12	□	A_4	(123), (234)	1		3	8	
4T5	24		S_4	(123), (12)	1	6	3	8	6

- For degree 5, there are 5 transitive subgroups of S_5, with generators and cycle types as follows:

#	Order	!	Name	Generators	1	2	2,2	3	2,3	4	5
5T1	5	□	C_5	(12345)	1						4
5T2	10	□	$D_{2\cdot 5}$	(12345), (15)(24)	1		5				4
5T3	20		F_{20}	(12345), (1243)	1		5			10	4
5T4	60	□*	A_5	(123), (345)	1		15	20			24
5T5	120	*	S_5	(12345), (12)	1	10	15	20	20	30	24

- For degree 6, there are 16 transitive subgroups of S_6, with generators and cycle types as follows:

#	Order	!	Name	Generators	1	2	2,2	2,3	2,4	2,2,2	3	3,3	4	5	6
6T1	6		C_6	(123456)	1					1		2			2
6T2	6		S_3	(135)(246), (14)(23)(56)	1					3		2			
6T3	12		$S_3 \times C_2$	(123456), (14)(23)(56)	1		3			4		2			2
6T4	12	□	A_4	(14)(25), (135)(246)	1		3					8			
6T5	18		F_{18}	(246), (14)(25)(36)	1					3	4	4			6
6T6	24		$A_4 \times C_2$	(36), (135)(246)	1	3	3			1		8			8
6T7	24	□	S_4 (a)	(14)(25), (135)(246), (15)(24)	1		9		6			8			
6T8	24		S_4 (b)	(14)(25), (135)(246), (15)(24)(36)	1		3			6		8	6		
6T9	36		$S_3 \times S_3$	(246), (15)(24), (14)(25)(36)	1		9			6	4	4			12
6T10	36	□	F_{36}	(246), (15)(24), (1452)(36)	1		9		18		4	4			
6T11	48		$S_4 \times C_2$	(36), (135)(246), (15)(24)	1	3	9		6	7		8	6		8
6T12	60	□*	A_5	(12346), (14)(56)	1		15					20		24	
6T13	72		$F_{36} \rtimes C_2$	(246), (24), (14)(25)(36)	1	6	9	12	18	6	4	4			12
6T14	120	*	S_5	(12346), (12)(34)(56)	1		15			10		20	30	24	20
6T15	360	□*	A_6	(12)(3456), (123)	1		45		90		40	40		144	
6T16	720	*	S_6	(123456), (12)	1	15	45	120	90	15	40	40	90	144	120

- For degree 7, there are 7 transitive subgroups of S_7, with generators and some cycle types as follows (for any cycle type not listed, S_7 is the only transitive subgroup containing it):

#	Order	!	Name	Generators	1	2,2	2,4	2,2,2	2,2,3	3	3,3	5	6	7
7T1	7	□	C_7	(1234567)	1									6
7T2	14		$D_{2\cdot 7}$	(1234567), (27)(36)(45)	1			6						6
7T3	21	□	F_{21}	(1234567), (124)(365)	1						14			6
7T4	42		F_{42}	(1234567), (132645)	1			7			14		14	6
7T5	168	□*	$PSL_2(\mathbb{F}_7)$	(1234567), (12)(36)	1	21	42				56			48
7T6	2520	□*	A_7	(34567), (123)	1	105	630		210	70	280	504		720
7T7	5040	*	S_7	(1234567), (12)	1	105	630	105	210	70	280	504	840	720

Figure 18: Tables of transitive subgroups of S_n for n = 3 to 7.// From *web.northeastern.edu/dummit /teaching_fa20_5111 /5111_transitive_subgroup_tables.pdf*, with thanks.