Algebra from Al Khwarizmi to Galois, 830-1830

J.-H. Eschenburg[1]

Abstract
Galois has completed a programme started by Al Khwarizmi 1000 years before.

Keywords Equations · Solvability · Quartic · Galois group

Mathematics Subject Classification 01A30 · 01A40 · 01A55 · 12F10

1 A Day of Misery

On the early morning of May 30, a shot was fired in a park in the south of Paris. A 20-year-old student of mathematics was hit into his stomach; nobody cared for him. Only hours later, some passerby found him and brought him into the nearby Hôpital Cochin. The next day he died there from peritonitis.

This was the miserable end of a young man whose short life was marked by a chain of personal and professional disasters. Yet he had answered a central question of algebra posed 1000 years before: For which equations

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0 \tag{1.1}$$

($a_1, \ldots, a_n$ given numbers) is it possible to compute the unknown x by basic arithmetic operations and extraction of roots (of any order), and for which equations is this impossible? The name of the young student was Évariste Galois; it was the year 1832.[1]

[1] Évariste Galois, 1811 (Bourg-la-Reine)—1832 (Paris). For more details, cf. [3].

✉ J.-H. Eschenburg
eschenburg@math.uni-augsburg.de

[1] Institut für Mathematik, Universität Augsburg, 86135 Augsburg, Germany

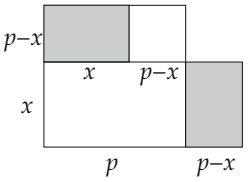
2 The Beginning of Algebra

Galois' work was the completion of a development started 1000 years earlier. Around the year 825, the Khalif Al Mamun, a son and successor of Harun al-Raschid, founded the "House of Wisdom" at Baghdad. He gathered excellent scientists from everywhere in order to translate foreign scientific works from Greek, Persian, Aramaic, Indian and other languages into Arabic. An envoy was sent to Constantinople in order to acquire copies of the important works of ancient Greek science from the Byzantine emperor Theophilos.[2] He might have spoken: "Mighty Emperor: You are owning a huge number of phantastic works from ancient times, papers of Euclid, Archimedes, Diophant, Ptolemy, Aristotle, Galen, and many others. Our Prophet (peace be upon him) has taught us to strive for knowledge and wisdom. Our scientists would like to translate these scriptures into our language to make them understandable for us. Therefore we would like to purchase some copies. Please accept our poor gold for it ..."

But the House of Wisdom became not only a place for translations but also for research. One of the most brilliant minds was the Persian scientist al Khwarizmi.[3] Around 830 he wrote the book "Hisab al-jabr wa-l-muqabala" (Calculation by Completion and Balancing). Both words, completion and balancing, denote certain transformations of equations: al-jabr = completion means removing differences by addition of terms on both sides and muqabala = balancing means substraction of terms on both sides. Later on, the word "al-jabr" was used for the whole mathematical area from which our word "algebra" is derived. The notion of *equation* was new; only Diophant has used a similar concept. It is a kind of a riddle: find a number (the *Unknown*) with certain properties, e.g. the square of the number, increased by 21, is ten times that number, $x^2 + 21 = 10x$. The general form of this equation is $x^2 + q = 2px$ or

$$q = (2p - x)x \tag{2.1}$$

for given numbers p, q. This was only one of several forms of quadratic equations since negative numbers were not used. Formulas were also unknown and everything had to be expressed in words. How did al Khwarizmi solve such equation? [1, p. 169]



He subdivided the square with edge length p into two domains: the small white square with edge length $p - x$ and the L-shaped remainder. By moving the shaded rectangle,

[2] https://upload.wikimedia.org/wikipedia/commons/c/c5/Mamun_sends_an_envoy_to_Theophilos.png.

[3] Muhammad ibn Musa al Khwarizmi (al-Tabari), ca. 780 (Khwarazm, Aral Lake?) - 850 (Baghdad?) His name al Khwarizmi is the origin of the word "algorithm".

we see that the remainder has the area of the lower rectangle with edge lengths x and $2p - x$, which equals q by (2.1). Then, $(p - x)^2 = p^2 - q$, hence

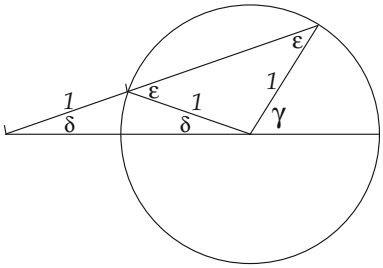
$$x = p + \sqrt{p^2 - q} = 5 + \sqrt{25 - 21} = 7 \tag{2.2}$$

when $p = 5$, $q = 21$. (The second solution $p - \sqrt{p^2 - q}$ is negative.) Thus, the unknown x, the hight of the lower rectangle, can be determined by the figure.

> "The algebra consists in discovering the mathematical methods by which one can determine the Unknown, either arithmetically or geometrically." (Omar Khayyam in: "Treatise on Algebra and Muqabala", 1079)

3 Geometric Solutions of the Cubic

Already Archimedes[4] investigated problems which lead to equations involving the third power of the Unknown, *cubic equations*. One of these problems he solved by means of a compass and a ruler with an adjustable mark on it: the trisection of the angle. In modern language, this problem is equivalent to solving the complex equation $(x + iy)^3 = a + ib$ for given a, b with $a^2 + b^2 = 1$. After substituting $y^2 = 1 - x^2$, the real part of the complex equation is a cubic, $4x^3 - 3x = a$. How did Archimedes solve it?



The triangle within the circle has the angle sum

$$180^\circ = 2\epsilon + (180^\circ - \delta - \gamma),$$

hence $2\epsilon = \gamma + \delta$ $(*)$. The angle sum of the left isosceles triangle amounts to $180^\circ = 2\delta + (180^\circ - \epsilon)$, hence $\epsilon = 2\delta$, and with $(*)$ we obtain $\gamma = 3\delta$.

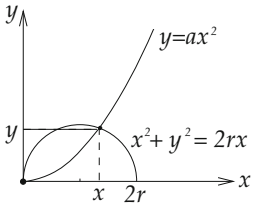
Another problem was the calculation of the height of a spherical segment of given volume.[5] Archimedes had announced a solution of this problem, but it seems that he never worked it out.

The Islamic mathematicians found solutions of cubic equations using the intersection of two conic sections. E.g. the x-value of the intersection point $(x, y) \neq (0, 0)$ between the circle $x^2 + y^2 = 2rx$ and the parabola $y = ax^2$ solves $x^2 + (ax^2)^2 = 2rx$; hence

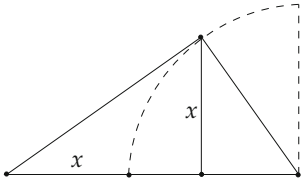
[4] Archimedes of Syracuse, ca. 287–212 B.C.

[5] The volume of the spherical segment of radius r and height h is $V_h = \frac{\pi}{3}(3rh^2 - h^3)$.

(after division by x) the cubic equation $x + a^2x^3 = 2r$. Vice versa, given such cubic equation, one can find the corresponding circle and parabola.



A similar method was carried through for all possible types of cubic equations by Omar Khayyam.[6] His motivation to investigate cubic equations was another geometric problem described in his first treatise "On the division of a quadrant of a circle". It amounts to finding a right triangle such that the hypothenuse equals the sum of one leg plus the altitude over the hypothenuse.



This "Khayyam triangle" seems to be realized in the dome of the Friday (Jameh) Mosque at Isfahan, built in 1088/89, which might indicate that Omar Khayyam contributed to the construction of this magnificent mosque.[7] Concerning cubic equations in general, Omar Khayyam admits in his comprehensive work "Algebra and Muqabala" that he (like his predecessors) has not been able to find an arithmetic solution in the way al Khwarizmi did this for quadratic equations:

> "Perhaps someone else who comes after us may find it out in the case, when there are not only the first three classes of known powers, namely the number, the thing [= the Unknown] and its square."

[6] Omar Khayyam, 1048–1131, was born and died in Naishapur, Persia (Iran). His most fruitful time he was spending at Isfahan (1074–1092) where he wrote "On the division of a quadrant of a circle" and "Algebra and Muqabala" (1077). He contributed to the reform of the Persian calender (1079) and calculated the length of the year as 365.24219858156 days. In 2000, this length was 365.24219052 days which shows the size of loss of rotational energy of the earth. He wrote a large number of quatrains, https://en.wikisource.org/wiki/Quatrains_of_Omar_Khayyam_(tr._Whinfield,_1883), e.g. No. 117:

Alas for that cold heart, which never glows
With love, nor e'er that charming madness knows;
The days misspent with no redeeming love; –
No days are wasted half as much as those!

[7] Alpay Özdural: A Mathematical Sonata for Architecture. Omar Khayyam and the Friday Mosque of Isfahan. Technology and Culture 39 (1998), 699–715, in particular Fig. 6, Seite 710, siehe auch Alpay Özdural: Omar Khayyam and the Friday Mosque of Isfahan, http://www.ensani.ir/storage/Files/20120427103533-5207-449.pdf, in particular Fig. 5, page 147.

In fact, this took more than 400 years to happen! In his treatise "On the division of a quadrant of a circle" he interrupts the mathematical discussion for the following remark which might characterize his way of thinking [4, VK:100]:

> "Self-satisfaction, however, is the privilege of the mediocre people, for their soul can understand only a tiny part of the sciences. And once they have understood this, they believe that this few encompasses and unites all science. That God may save us from such views that lead us astray and prevent us from recognizing the truth and finding our salvation."

4 Algebraic Solution of the Cubic

The cubic equation[8]

$$x^3 + 3ax = 2b \tag{4.1}$$

was solved arithmetically only after 1500 in Italy. It was the time of Italian Renaissance when the ancient scientific works had been rediscovered, many centuries after they were collected and translated at the "House of Wisdom". This was only possible after Europe got in contact with the Islamic culture. A most influential book was "Liber Abaci" by Leonardo of Pisa, named Fibonacci (Pisa 1202 and 1228). He introduced the Arabic numerals and also the number zero and the negative numbers which had been discovered probably by the Indian mathematician Brahmagupta (598—after 665), well known at the "House of Wisdom". Negative numbers were needed in Europe for economic reasons: the credit system was started in Italy in late medieval times.
Three Italian mathematicians, del Ferro, Tartaglia and Cardano[9] found the solution formula for the cubic. Scipione del Ferro was the first, but he kept the formula secret and told it only to one of his students, Antonio Maria del Fiore. The latter challenged one of the leading calculation masters, Nicolo Tartaglia from Venice, by sending him some cubic equations to be solved. Tartaglia did not know the formula, but he sat down and rediscovered it on his own; thus, he won the competition against del Fiore. Girolamo Cardano was a well-known scientist and physician and friend of Tartaglia. He asked Tartaglia to reveal the formula to him which he finally did, in form of a poem.[10] But Cardano had to swear that he would keep the formula secret. His friend and co-worker Ludovico Ferrari (1522–1565) had solved even the fourth degree ("quartic") equation, using the cubic. However, without the solution of the cubic, this was useless, and Tartaglia refused to publish his formula. When Cardano learned that del Ferro had found the formula before Tartaglia, he felt himself no longer committed to his oath and published the solution of the cubic together with a proof in his algebra textbook "Ars Magna" (1545):

---

[8] The general cubic equation $x^3 + ax^2 + bx + c = 0$ can be reduced to (4.1) as follows. Substituting the Unknown x by the expression $\tilde{x} - a/3$, one obtains an equation for $\tilde{x}$ of the form (4.1).

[9] Scipione del Ferro, 1465–1526, Bologna; Nicolo Tartaglia, 1499–1557, Breschia and Venice; Gerolamo Cardano, 1501–1576, Pavia, Milan, Rome.

[10] http://www.math.toronto.edu/alfonso/347/Tartagliaspoem.pdf.

$$x = \sqrt[3]{b + \sqrt{D}} + \sqrt[3]{b - \sqrt{D}}, \quad D = a^3 + b^2. \tag{4.2}$$

Since then it is called "Cardano's formula" though Cardano reported the full story, back to the Islamic mathematicians.

How was this solution found? The contemporary witnesses kept silence about this, we rely on guess work. However, these guesses are not made out of thin air. Then and now, the path to the solution opens up by reflecting about the task.[11] The given Eq. (4.1) seems difficult; we cannot see any solution. But there is another cubic equation whose solution is apparent,

$$(x + u)^3 = v^3 \tag{4.3}$$

with the solution

$$x + u = v, \text{ or } x = v - u. \tag{4.4}$$

Now the idea is to bring the easy Eq. (4.3) into the form of the difficult one, (4.1), by expanding $(x + u)^3$ and using (4.4):

$$v^3 = (x + u)^3 = x^3 + 3xu(x + u) + u^3 \overset{(4.4)}{=} x^3 + 3xuv + u^3.$$

Now, (4.3) has been transformed into (4.1) with

$$a = uv, \quad 2b = v^3 - u^3. \tag{4.5}$$

Vice versa, we can calculate u and v from a, b by means of (4.5):

$$u = \frac{a}{v}, \quad v^3 = 2b + u^3 = 2b + \frac{a^3}{v^3}, \quad \text{hence } (v^3)^2 = 2bv^3 + a^3.$$

The solution of this quadratic equation for v^3 is $v^3 = b \pm \sqrt{D}$ with $D = a^3 + b^2$, and from $2b = v^3 - u^3$ one obtains $-u^3 = 2b - v^3 = b \mp \sqrt{D}$. Thus Cardano's formula (4.2) for $x = v - u$ follows.

5 The Discovery of Complex Numbers

Let us consider two examples of cubic equations $x^3 + 3ax = 2b$:

Example 5.1 $x^3 - 6x = 9$. Then

$$a = -2, \quad b = 9/2, \quad D = a^3 + b^2 = -8 + \frac{81}{4} = \frac{81 - 32}{4} = \frac{49}{4}.$$

[11] I owe the following consideration to Urs Kirchgraber.

Hence $\sqrt{D} = \frac{7}{2}$ and $b + \sqrt{D} = \frac{9+7}{2} = 8$ and $b - \sqrt{D} = \frac{9-7}{2} = 1$, thus $x = \sqrt[3]{8} + \sqrt[3]{1} = 2 + 1 = 3$. Check: $3^3 - 6 \cdot 3 = 27 - 18 = 9$.

Example 5.2 $x^3 - 6x = 4$. Then

$$a = -2, \quad b = 2, \quad D = -8 + 4 = -4.$$

Now, we have got a problem: since D is negative, the square root $\sqrt{D}$ does not exist! The solution method seems to fail. All what Cardano could do was to give this case the name "Casus Irreduciblis", the unreducible case. But actually this was a scandal: The equation $x^3 - 6x = 4$ has apparently the solution $x = -2$, since $(-2)^3 - 6(-2) = -8 + 12 = 4$. However, nobody knew its relation to Cardano's formula.

But only a generation later, around 1570, the "unreducible case" was solved, not by a mathematician, but by a water engineer from Bologna, Raffael Bombelli.[12] Of course, he would say, square roots of negative numbers cannot exist, since squares are positive. But let us pretend for a moment that such numbers still existed (later they would be called *imaginary*), and let us calculate with such "numbers" as usual. Actually, we only would need one such number, later called i (for "imaginary"), which squares to -1, then, e.g. $2i$ would square to -4, etc. Cardano's "solution" now would look as follows:

$$x = \sqrt[3]{2 + 2i} + \sqrt[3]{2 - 2i}. \tag{5.1}$$

But what should we do with such a result? How can we draw the cubic root of $2 + 2i$? Bombelli could not answer this question, but instead he could compute the third power of such "numbers", e.g.:

$$\begin{aligned}(-1 + i)^3 &= -1 + 3i - 3i^2 + i^3 \\ &= -1 + 3i + 3 - i \\ &= 2 + 2i\end{aligned}$$

and similarly $(-1-i)^3 = 2-2i$. Luckily enough, the third powers of $-1+i$ and $-1-i$ are precisely the "numbers" whose third root we want to calculate. Hence, these are *cubic numbers*, third powers of known numbers, like 1 and 8 in the first example. Thus, $\sqrt[3]{2 \pm 2i} = -1 \pm i$, and from (5.1) we obtain the solution $x = (-1+i)+(-1-i) = -2$ which we already know. The "imaginary" square roots of negative numbers have been magically disappeared!

This was a true magic moment in the history of mathematics. Bombelli dared to surpass the limits of traditional conception: "there are no square roots of negative numbers", and he reached correct results on this path. The third time in mathematics history (after the discovery of irrational numbers by scholars of Pythagoras and the zero and the negative numbers by Indian mathematicians) the number concept became drastically

[12] Rafael Bombelli, 1526–1572, Bologna.

extended. It should take more than two centuries until the "imaginary numbers" had lost their mysticism and were fully accepted. Sums of real and imaginary numbers as in the previous computations were called *complex* numbers. One had to re-think the geometric idea of numbers: they would no longer form a scale or a line, but a plane, using real and imaginary parts as planar coordinates (Wessel 1797, Argand 1806).[13] Eventually, the twentieth century's quantum physics should prove the fundamental importance of the complex numbers for the physical reality of our world.

Mathematically, the complex numbers turned out to be true miracles. Not only quadratic and cubic equations but *every* equation of type (1.1) could be solved by complex numbers ("fundamental theorem of algebra"). This was known since mid of eighteenth century, but for a complete proof one had to wait for the Ph.D. thesis of C.F. Gauß (1799).[14] As a consequence, the Eq. (1.1) of degree n has not just one, but n solutions (counted with multiplicities): if $x = a$ is one solution, one obtains from (1.1) another equation of degree $n - 1$ by dividing the left hand side through $x - a$. This new equation again has a solution, etc.

6 Galois: the Limits of Algebraic Calculations

By the "fundamental theorem of algebra" it was known that Eq. (1.1) has always a (possibly complex) solution x. But was it possible to calculate x by means of basic arithmetic operations and roots of arbitrary order? Paolo Ruffini (1799) and Niels Henrik Abel (1824)[15] had recently shown that this was impossible for the general *quintic* equation, the one starting with the 5th power of the Unknown. What was the precise condition? Could one determine for every equation whether or not it is possible to calculate a solution?

On the evening before the fatal duel, Galois wrote a letter to his friend Auguste Chevalier in which he summarized his essential mathematical findings. The algebraic papers had been written 2 years ago (1830) but had not been published. His comment on the equation problem amounts to the following statement: "If each of these groups has a prime number of permutations then the equation will be solvable by radicals; otherwise, not." ("Sinon, non").[16] Galois had defined a group of permutations (renumberings) of the solutions $x_1, \ldots, x_n$, today called *Galois group*. More precisely (cf [5, Appendix

[13] Caspar Wessel, 1745 (Vestby, Norway)–1818 (Copenhagen), Jean-Robert Argand, 1768 (Geneva)–1822 (Paris). Argand who (like Wessel) was not a professional mathematician is also known for his elementary proof of the "fundamental theorem of algebra".

[14] Carl Friedrich Gauß, 1777 (Braunschweig)–1855 (Göttingen). Gauß' proof used that the polynomial expression $p(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ is close to x^n when $|x|$ is large. To apply this, one had to compute the n-th power x^n for every complex number x. This was done by Leonhard Euler, 1707 (Basel)–1783 (St. Petersburg) who introduced the exponential expression $e^{it} = \cos t + i \sin t$: we have $x = re^{it}$ for real numbers r, t and therefore $x^n = r^n e^{\text{int}}$. A modern version of Gauß' proof would use the *winding number* which counts the number of turns around the origin for a closed curve. The winding number w of the closed curve $p(re^{it})$, $t \in [0, 2\pi]$, equals n when r is large (since $p(re^{it}) \approx r^n e^{int}$) and zero when r is very small (unless $a_n = 0$, but then $p(0) = 0$). Thus, w must change its value at some r_o which (by continuity) means that the curve $p(r_o e^{it})$ meets the origin 0.

[15] Paolo Ruffini, 1765 (Valentano)–1822 (Modena), Niels Henrik Abel, 1802 (Finnøy, Norway)–1829 (Froland, Norway).

[16] https://www.ias.ac.in/article/fulltext/reso/004/10/0093-0100, http://langevin.univ-tln.fr/notes/Galois/.

D], [2]), the Galois group contains those permutations which preserve the algebraic relations between the solutions.[17] When this group is "solvable", that is decomposable (by a normal series) into factors of prime order,[18] then Galois indicates an algorithm by which the equation can be solved, and else he shows that there are no solutions by *radicals* (expressions in the coefficients $a_1, \ldots, a_n$ which involve only basic arithmetic operations and roots of any order). The complicated Eq. (1.1) had been replaced by a much easier object, a finite group whose structure carries essential information about the equation and, in particular, it decides whether or not the equation is solvable by radicals.

I would like to explain the ideas of Galois using the example of the general *quartic* equation ($n = 4$),

$$x^4 - ax^3 + bx^2 - cx + d = 0. \tag{6.1}$$

As mentioned before, this equation was already solved in sixteenth century by Cardano's friend Ludovico Ferrari. He represented the left hand side of (6.1) as the product of two quadratic expressions in the Unknown, and the coefficients of these expressions could be determined by solving a cubic equation. Of course one tried the same method also for the quintic equation ($n = 5$), by representing its left hand side as a product of a quadratic and a cubic expression in the Unknown. Again one had to calculate the coefficients of these expressions, but this time the computation led to an equation of 10th degree which remained unsolvable. Why does this idea work for the quartic but does not for the quintic? This remained a secret for centuries; the calculation did not give a clue.

However, in Galois' approach, the distinction between the cases $n = 4$ and $n \geq 5$ became quite apparent. For the general equation of degree n, the Galois group is the full permutation group (symmetric group) S_n. The group S_4 has a special property: the three pairwise transpositions, (12)(34), (13)(24), (14)(23) form together with the identity permutation (which does not change anything) a *normal subgroup* H: the composition of two elements of H is again in H, and for all $\sigma \in H$ and every permutation τ we have $\tau\sigma\tau^{-1} \in H$ (if σ is a pairwise transposition, the same is true for $\tau\sigma\tau^{-1}$). Therefore, S_4 can be decomposed (in the sense of a normal series) into the factors H and $S_4/H \cong S_3$. Decomposing H and S_3 further, the group S_4 is decomposed into four factors with order (number of elements) 2, 2, 3, 2. But for S_n with $n \geq 5$, the pairwise transpositions form no longer a subgroup; in fact there is no proper normal subgroup other than A_n, the set of even permutations, where $|S_n/A_n| = 2$, and A_n itself has no proper normal subgroups at all. Note that $|A_n| = n!/2$ is never a prime number except for $n = 3$ (the case of a cubic).

---

[17] E.g. the solutions of the equation $x^n = a$ ("pure equation") are $x_j = \sqrt[n]{a} \cdot \zeta^j$ for $j = 1, \ldots, n$, where $\zeta = e^{2\pi i/n}$, thus $x_k = \zeta^{k-j} x_j$. Therefore, a permutation σ in the Galois group of this equation must preserve this relation: $x_{\sigma(k)} = \zeta^{k-j} \cdot x_{\sigma(j)}$. Thus, $\sigma(k) - \sigma(j) \equiv k - j \mod n$, and since there are no other relations, the Galois group is the cyclic group of order n, generated by the cyclic permutation $(12\cdots n)$.

[18] More precisely: if there is a descending series $G = G_0 \supset G_1 \supset \cdots \supset G_k = \{e\}$ with the property that G_{j+1} is a normal subgroup of G_j and that $p_j = |G_j/G_{j+1}|$ is a prime number for $j = 1, \ldots, k-1$.

The decomposition of the Galois group leads to an algorithm for calculating the solutions. The numbers a, b, c, d are given, the four solutions x_1, x_2, x_3, x_4 are wanted. The inverse process (computing a, b, c, d from x_1, x_2, x_3, x_4) would be much easier: when (6.1) has the solutions x_1, x_2, x_3, x_4, the polynomial

$$p(x) = x^4 - ax^3 + bx^2 - cx + d, \tag{6.2}$$

on the left hand side of (6.1) can be represented as

$$p(x) = (x - x_1)(x - x_2)(x - x_3)(x - x_4) \tag{6.3}$$

since there is just one quartic equation with these solutions. Expanding the right hand side of (6.3) and comparing coefficients with (6.2) we see that a, b, c, d are the *elementary symmetric polynomials* in the variable $\mathbf{x} := (x_1, x_2, x_3, x_4)$,[19]

$$\begin{aligned} a &= x_1 + x_2 + x_3 + x_4 = \sigma_1(\mathbf{x}), \\ b &= x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 = \sigma_2(\mathbf{x}), \\ c &= x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 = \sigma_3(\mathbf{x}), \\ d &= x_1x_2x_3x_4 = \sigma_4(\mathbf{x}). \end{aligned} \tag{6.4}$$

This is the generalization of Vieta's theorem for the coefficients of quadratic equations.[20] By the fundamental theorem on symmetric polynomials,[21] any symmetric polynomial in $\mathbf{x}$ can be written as a polynomial expression in the elementary symmetric polynomials which are the coefficients a, b, c, d.
Now one looks for "resolvents". These are polynomials in $\mathbf{x}$ which are not invariant under the full permutation group, but only under the normal subgroup H. The simplest such expressions (lowest degree) are

$$\begin{aligned} y_1 &= (x_1 + x_2)(x_3 + x_4) = x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 \\ y_2 &= (x_1 + x_3)(x_2 + x_4) = x_1x_2 + x_1x_4 + x_3x_2 + x_3x_4 \\ y_3 &= (x_1 + x_4)(x_2 + x_3) = x_1x_2 + x_1x_3 + x_4x_2 + x_4x_3 \end{aligned} \tag{6.5}$$

[19] We are considering simultaneously all quartic equations. Any of them is uniquely determined by its four solutions x_1, x_2, x_3, x_4 which now will be considered as variables and, thus, the coefficients a, b, c, d can be considered as functions in these variables.

[20] François Viète (lat. Vieta), 1540–1603 (Paris).

[21] In a symmetric polynomial, for any term $x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$ there exists another term with the same powers $k_1, \ldots, k_n$, but in decreasing order, $k_1 \geq k_2 \geq \cdots \geq k_n$. We put $\left(x_1^{k_1}\cdots x_n^{k_n}\right)$ the symmetric polynomial which arises from $x_1^{k_1}\cdots x_n^{k_n}$ by adding all permutations of this term. These polynomials are lexicographically ordered by the weakly decreasing sequences $(k_1, \ldots, k_n)$, e.g. $(3, 3, 1) > (3, 2, 2)$. The symmetric polynomial $\sigma_1^{k_1-k_2}\sigma_2^{k_2-k_3}\cdots\sigma_n^{k_n}$ has the same highest term as $\left(x_1^{k_1}\cdots x_n^{k_n}\right)$. Hence, the difference of both expressions has a highest term of lower order in our lexicographical ordering. Continuing this procedure, we finally end with the zero polynomial and, thus, we have written our given symmetric polynomial as a polynomial expression in the variables $\sigma_1, \ldots, \sigma_n$.

By construction, y_1 is invariant under (12)(34), which transposes the pairs x_1, x_2 and x_3, x_4, but y_1 is also invariant under (13)(24) (and thus under (14)(23)) since

$$(x_3 + x_4)(x_1 + x_2) = (x_1 + x_2)(x_3 + x_4) = (x_4 + x_3)(x_2 + x_1).$$

The same holds for y_2, y_3.[22] These new expressions y_1, y_2, y_3 are the solutions of the cubic equation

$$0 = (y - y_1)(y - y_2)(y - y_3) = y^3 - uy^2 + vy - w, \tag{6.6}$$

u, v, w being the elementary symmetric polynomials in $\mathbf{y} = (y_1, y_2, y_3)$:

$$\begin{aligned} u &= y_1 + y_2 + y_3 = \sigma_1(\mathbf{y}) \\ v &= y_1y_2 + y_1y_3 + y_2y_3 = \sigma_2(\mathbf{y}) \\ w &= y_1y_2y_3 = \sigma_3(\mathbf{y}) \end{aligned} \tag{6.7}$$

After inserting (6.5), these expressions become symmetric polynomials[23] in the variables $\mathbf{x} = (x_1, x_2, x_3, x_4)$. E.g. the first coefficient is

$$\begin{aligned} u &= y_1 + y_2 + y_3 \\ &= x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 \\ &\quad + x_1x_2 + x_1x_4 + x_3x_2 + x_3x_4 \\ &\quad + x_1x_2 + x_1x_3 + x_4x_2 + x_4x_3 \\ &= 2b \end{aligned} \tag{6.8}$$

and similarly (but with more computations)

$$v = b^2 + ac - 4d \tag{6.9}$$

$$w = abc - a^2d - c^2 \tag{6.10}$$

Now, we know the coefficients of (6.6), hence we can solve this cubic equation. From the solutions y_1, y_2, y_3 and (6.5) we obtain x_1, x_2, x_3, x_4.[24]

Example 6.1 $x^4 - 2x^3 - 13x^2 + 14x + 24 = 0$. Then, $u = 2b = -26$, $v = b^2 + ac - 4d = 169 - 28 - 96 = 45$, $w = 28 \cdot 13 - 96 - 14 \cdot 4 = 14 \cdot (26 - 14) - 96 = 72$. Thus, the cubic equation is $y^3 + 26y^2 + 45y - 72 = 0$ with the solutions $y_1 = 1$,

[22] In fact, $\{y_1, y_2, y_3\}$ is the orbit of y_1 under the permutation group $G = S_4$ which acts on the space of polynomials in $\mathbf{x} = (x_1, x_2, x_3, x_4)$ by permutation of the four variables.

[23] Since G permutes the orbit $\{y_1, y_2, y_3\}$, a symmetric polynomial τ in $\mathbf{y} = (y_1, y_2, y_3)$ is also a symmetric polynomial $\tilde{\tau}$ in $\mathbf{x}$, namely $\tilde{\tau}(\mathbf{x}) = \tau(\mathbf{y}(\mathbf{x}))$. For this argument, we do not need that H is a normal subgroup. By the fundamental theorem for symmetric polynomials (cf. footnote 21), it can be expressed by the coefficients $\sigma_i(\mathbf{x})$. To find this expression explicitly, one has to apply the algorithm given in footnote 21.

[24] The cubic equation corresponds to a field extension (passing from u, v, w to y_1, y_2, y_3) with Galois group $G/H \cong S_3$, and the last step, solving quadratic equations for z_i, corresponds to the field extension passing from y_j to x_i with Galois group $H = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.

$y_2 = -24$, $y_3 = -3$. Then, $z = z_i := x_1 - x_i$ $(i = 2, 3, 4)$ solves the equation $z^2 - 2z = -y$ with $y \in \{1, -24, -3\}$ and, hence, $(z-1)^2 = -y + 1 \in \{0, 25, 4\}$ and $z \in \{1, 1 \pm 5, 1 \pm 2\}$. Which sign is right has to be checked, here we find $z_2 = 1$, $z_3 = 1 - 5 = -4$, $z_4 = 1 + 2 = 3$. The sum of the three terms z_i, $i = 2, 3, 4$ is $2x_1 + a = 2x_1 + 2$, on the other hand, it is $1 - 4 + 3 = 0$, hence $x_1 = -1$ from which we get $x_i = z_i - x_1 = z_i + 1$; thus, $x_2 = 2$, $x_3 = -3$, $x_4 = 4$ which are the correct solutions of the above equation.
In general, one has to consider the "pure equations" $x^n = a$ corresponding to n-th roots. In footnote 17, we saw that the corresponding Galois group is the cyclic group generated by the cycle $\sigma = (12 \cdots n)$. Vice versa, if an arbitrary Eq. (1.1) of order n has this Galois group, it can be reduced to a pure equation, using an old argument of Lagrange.[25] However, applying this argument needs proving that expressions in the solutions $x_1, \ldots, x_n$ which are invariant under the Galois group are "known quantities": they can be computed from the coefficients by means of basic arithmetic operations. This is a cornerstone of Galois theory, however, see footnote 21 for the case when the Galois group is the full permutation group.

When the Galois group can be decomposed into cyclic groups (which holds in particular if the orders of all factors are prime numbers), the problem of finding solutions is decomposed into partial problems of finding solution of pure equations corresponding to the factors, which amounts to drawing roots. Otherwise, the equations corresponding to the (minimal) factors are not pure and thus cannot be solved by roots.
Since geometric methods can be expressed arithmetically, Galois has fulfilled the programme of algebra as stated by Omar Khayyam:

> "discovering the mathematical methods by which one can determine the Unknown, either arithmetically or geometrically."

References

1. Alten, H.-W., et al.: 4000 Jahre Algebra. Geschichte, Kulturen, Menschen, Springer (2003)
2. Başaru, D.: Galoisgruppe - alt und neu, Bachelor's thesis, Augsburg 2015. http://myweb.rz.uni-augsburg.de/~eschenbu/BA_DilanB.pdf
3. Eschenburg, J.-H.: Sternstunden der Mathematik. Springer, Berlin (2017)
4. Linden, S.: *Die Algebra des Omar Chayyam*, Edition Avicenna (2012)
5. Rotman, J.: Galois Theory, 2nd edn. Springer, Berlin (1998)

[25] Joseph-Louis Lagrange, 1736 (Turin)–1813 (Paris): Réflexions sur la résolution algébrique des équations (1771/1772), http://gallica.bnf.fr/ark:/12148/bpt6k229222d/f206. Let $x_1, \ldots, x_n$ be the solutions of our equation and $\Omega = \{\omega \in \mathbb{C} : \omega^n = 1\}$ be the set of unit roots. For each $\omega \in \Omega$ we put

$$y_\omega(\mathbf{x}) = \sum_j \omega^j x_j .$$

We can easily compute $\mathbf{x}$ from the set $\{y_\omega : \omega \in \Omega\}$, just by inverting a unitary matrix. Applying σ to y_ω shifts the index of each x_j by one, thus $\omega \cdot \sigma\, y_\omega = y_\omega$. In particular, $b_\omega := y_\omega^n$ is invariant under the Galois group, hence "known". Now, we obtain y_ω from b_ω by drawing the n-th root.