# How do I Solve this Equation? Look at the Symmetries! – The Idea behind Galois Theory

**Timo Leuders** 

# Introduction

There are some questions that accompany the development of mathematics through cultures and ages. One of these questions is how to find an unknown quantity x of which one knows some relations such as – in today's algebraic notation:

 $x^2 = x + 5$ 

Finding solutions to such quadratic equations are essentially known since Babylonian times and are core content school mathematics:

$$x^2 - x - 5 = 0 \implies x = \frac{1}{2} + \frac{1}{2}\sqrt{21} \lor x = \frac{1}{2} - \frac{1}{2}\sqrt{21}$$

But how about  $x^5 = x+5$ , which looks only slightly different? Are there also straightforward ways to calculate the solutions? Do the solutions also look symmetric in a similar way?

The quest for solving equations inspired mathematicians to invent (some would rather say: to discover) new concepts such as negative, real or complex numbers. But, solving the polynomial equation in the second example posed severe problems for five hundred years. Why is it so difficult? Let us cheat for a moment and ask a Computer Algebra System (CAS) - which of course uses what is known about solving equations.

Solve[
$$x^4 - 5x^2 + 4 == 0, x$$
]  
L = {-2, -1, 1, 2}

Solve[
$$x^4 - 5x^2 + 3 == 0, x$$
]  

$$L = \left\{ -\sqrt{\frac{1}{2}(5 - \sqrt{13})}, \sqrt{\frac{1}{2}(5 - \sqrt{13})}, -\sqrt{\frac{1}{2}(5 + \sqrt{13})}, \sqrt{\frac{1}{2}(5 + \sqrt{13})} \right\}$$

Solve[
$$x^4 - 5x + 1 == 0, x$$
]  

$$L = \left\{ 1, \frac{1}{3} \left( -1 - 2 \left( \frac{2}{115 + 3\sqrt{1473}} \right)^{1/3} + \left( \frac{1}{2} \left( 115 + 3\sqrt{1473} \right) \right)^{1/3} \right), -\frac{1}{3} + \frac{1}{3} \left( 1 + i\sqrt{3} \right) \left( \frac{2}{115 + 3\sqrt{1473}} \right)^{1/3} - \frac{1}{6} \left( 1 - i\sqrt{3} \right) \left( \frac{1}{2} \left( 115 + 3\sqrt{1473} \right) \right)^{1/3}, -\frac{1}{3} + \frac{1}{3} \left( 1 - i\sqrt{3} \right) \left( \frac{2}{115 + 3\sqrt{1473}} \right)^{1/3} - \frac{1}{6} \left( 1 + i\sqrt{3} \right) \left( \frac{1}{2} \left( 115 + 3\sqrt{1473} \right) \right)^{1/3} \right\}$$

Finally: For Solve $[x^5 + x + 5 == 0, x]$  the CAS gives up and yields *no* solution.

What is going on here? Why does a seemingly small change in the equation lead to such tremendous problems in presenting the solutions? What is the structure of the equation that ultimately decides on the existence or the complexity of a solution? The answer to these questions is: It is all about the symmetry of the equation! But what exactly is the symmetry of an equation?

The attempts in history to find a general solution procedure for polynomial equations finally lead to a transformation of classical algebra (as the art of solving equations) into modern algebra (as the analysis of structure and symmetry). A culmination point in this development was the work of Évariste Galois (1811-1832). This paper tries to give a less technical account of Galois' ideas that changed algebra by showing examples that highlight what it means to "look at structure and symmetry" when trying to solve equations.

#### What is the symmetry of an equation?

When looking at the solutions of a quadratic equation

$$x^{2} + 2x + 3 = 0$$
,  $x_{12} = -1 \pm \sqrt{1 - 3} = -1 \pm i\sqrt{2}$ 

one detects a certain symmetry with respect to the quantity  $i\sqrt{2}$ . Mark that this quantity is not a rational number anymore, although the coefficients of the equation are.  $i\sqrt{2}$  needs to be created in addition to the purely rational numbers for being able to write down a solution. (In modern words this is called a field extension  $\mathbb{Q}(i\sqrt{2})$ ).

The symmetry of the solutions can also be written without explicitly using these extra quantities by just stating the following two rational relations (i.e. equations using only rational numbers and rational operations):

$$x_1 + x_2 = -2$$
,  $x_1 \cdot x_2 = 3$ .

These relations connect the solutions in a symmetric way: Exchanging the two solutions  $x_1$  and  $x_2$  (for which we will use the notation 1 $\leftrightarrow$ 2 or shorter and more common mathematics: (12)) preserves the relations. This reflection symmetry is represented by the following figure:

Considering another equation leads to a different situation:

$$x^{2} + 4x - 5 = 0$$
,  $x_{1,2} = -2 \pm \sqrt{4 - (-5)} = -2 \pm 3$ 

The solutions need no extra quantities and allow for additional rational relations between the solutions, for example

$$5x_1 + x_2 = 0$$
,  $x_1 - 1 = 0$ ,  $x_2 + 5 = 0$ 

These relations lead to a situation of less symmetry between the solutions (one may call this a "partial breakdown of symmetry"): The relations do not hold when exchanging  $x_1$  and  $x_2$ . The following figure suffers from the same breakdown. The two different circles (one single, one double) indicate that the two solutions are not exchangeable anymore.



All this may appear rather trivial and it is still hard to see how this perspective of symmetry can be useful for understanding the solution principles of *any* polynomial equation. This will only become evident when we switch to a more nontrivial case. For this purpose we look at a special type of equations of fourth degree, the so-called bi-quadratics (on the one hand they are simple enough to be solved by means of school mathematics, even without complex numbers, on the other hand they will reveal a complex behaviour with respect to symmetry).

First, consider the general biquadratic equation.

$$x^4 + ax^2 + b = 0$$

By expanding  $(x-x_1)(x-x_2)(x-x_3)(x-x_4) = 0$  one can see, that the four solutions necessarily fulfill the following relations:

$$\begin{aligned} x_1 x_2 x_3 x_4 &= b \\ x_1 x_2 x_3 + x_1 x_2 x_4 + x_1 x_3 x_4 + x_2 x_3 x_4 &= 0 \\ x_1 x_2 + x_1 x_3 + x_1 x_4 + x_2 x_3 + x_2 x_4 + x_3 x_4 &= a \\ x_1 + x_2 + x_3 + x_4 &= 0 \end{aligned}$$

These four equations are symmetric with respect to any permutation of the four solutions. This symmetry is identical with the symmetry group of the tetrahedron, which comprises all rotations and reflections. (For the following analysis it is useful to turn the tetrahedron into the somewhat unusual positition so that one is looking onto an edge).



But the biquadratic equation has additional structure as the solutions are paired in two pairs. For example consider the following concrete equation where  $x_1$  is paired with  $x_2$ , and also  $x_3$  with  $x_4$ .



These relations are preserved under permutations which "respect" the pairs, such as  $1\leftrightarrow 2$  or  $3\leftrightarrow 4$  or  $(1\leftrightarrow 2 \& 3\leftrightarrow 4)$  but also  $(1\leftrightarrow 3 \& 2\leftrightarrow 4)$ ,  $(1\leftrightarrow 4 \& 2\leftrightarrow 3)$ ,  $(1\rightarrow 3\rightarrow 2\rightarrow 4\rightarrow 1)$  or  $(1\rightarrow 4\rightarrow 2\rightarrow 3\rightarrow 1)$ . In mathematical shorthand this can be written as (12),(34), (12)(34),(13)(24),(14)(23),(1324) and (1423). The figure beside the equation represents the same situation: The pairing of opposing vertices reduces the symmetry of the former tetrahedron by allowing only those rotations and reflections which conserve the pairings.

By multiplying solutions

$$x_1 x_3 = \sqrt{3 + \sqrt{7}} \sqrt{3 - \sqrt{7}} = \sqrt{9 - 7} = \sqrt{2}$$
 or  $x_1 x_2 = -\sqrt{3 + \sqrt{7}} \sqrt{3 + \sqrt{7}} = 3 + \sqrt{7}$ 

it is possible to find even further relations:

$$x_1x_3 - x_2x_4 = 0$$
,  $x_1x_4 - x_2x_3 = 0$  or  $x_1x_2 + x_3x_4 - 6 = 0$ 

The group of permutations that preserves *all* possible rational relations between the solutions of an equation is called the *Galois group* of the equation. As to this point we can be sure that the Galois group G of the equation is contained in the dihedral group  $D_4$  (actually, without proof, it is the dihedral group)

 $G \subseteq \{ \, (1), \, (12), \, (34), \, (12)(34), \, (13)(24), \, (14)(23), \, (1324), \, (1423) \, \} = D_4$ 

The symmetry breaking effect of the relations is already depicted in the tetrahedron above, in which the relations are introduced as a symmetry break by tagging two edges. A rotation around an axis through one triangle, such as (123) is not possible anymore.

Let's look at another biquadratic equation. This time the "nested roots" vanish due to the special values of the coefficients:

$$x^{4} - 5x^{2} + 6 = (x^{2} - 2)(x^{2} - 3) = 0$$
,  $x_{1,2,3,4} = \pm \sqrt{\frac{5}{2} \pm \sqrt{\frac{1}{4}}} = \pm \sqrt{\frac{5}{2} \pm \frac{1}{2}}$ 

Some of the rational relations that express the special structure, are:

$$x_{1} + x_{2} = 0, \ x_{3} + x_{4} = 0$$
  
$$x_{1,2}^{2} - 3 = 0 \ x_{3,4}^{2} - 2 = 0$$

This time the symmetry is broken even further: The two pairs cannot be exchanged with each other anymore, since they fulfill mutually exclusive rational relations. Therefore we can be sure that the Galois group G of the equation is contained in the so-called "Klein Four-Group"  $V_4$ 

 $G \subseteq \{ (1), (12), (34), (12)(34) \} = V_4$ 

(Yes, it was actually named after Felix Klein, who first dubbed it "Vierergruppe" in a famous paper cited below). The figure again shows the same symmetry breakdown: the vertex pair connected by the thick line can not be exchanged with the other pair anymore.

Going a step further it is easy to imagine how the symmetry can be broken further:

$$x^{4} - 4x^{2} + 3 = 0 = (x - 1)(x + 1)(x^{2} - 3), x_{1,2,3,4} = \pm\sqrt{2 \pm \sqrt{1}} = \pm\sqrt{2 \pm 1}$$
  
$$x_{1,2}^{2} - 3 = 0 \quad x_{3} + 1 = 0 \quad x_{4} - 1 = 0$$

The symmetry is reduced to  $G \subseteq \{ (1), (12) \} = \mathbb{Z}_2$ . Analogously, in the figure only one pair exchange leaves the figure invariant.

Two less obvious and more interesting situations can occur. The following equation

$$x^4 - 4x^2 + 1 = 0$$
,  $x_{1,2,3,4} = \pm \sqrt{2 \pm \sqrt{3}}$ .

contains some special numbers that allow for some relations not yet encountered:

$$x_1 x_3 = \sqrt{2 + \sqrt{3}} \sqrt{2 - \sqrt{3}} = \sqrt{4 - 3} = 1$$
  
$$x_1 x_3 - 1 = 0, \ x_1 x_4 + 1 = 0, \ x_2 x_3 + 1 = 0, \ x_2 x_4 - 1 = 0$$



These relations break down the dihedral symmetry of a general biquadratic equation to another Galois group isomorphic but not identical to the above

$$G \subseteq \{ (1), (12)(34), (13)(24), (14)(23) \} \cong V_4$$

The figure beside the equation shows the same symmetry. Finally the constellation of parameters in

$$x^4 - 4x^2 + 2 = 0$$
,  $x_{1,2,3,4} = \pm \sqrt{2 \pm \sqrt{2}}$ .

allows for a more intricate construction of rational relation between solutions:

$$x_1^2 - x_1 x_3 = \sqrt{2 + \sqrt{2}} \sqrt{2 + \sqrt{2}} - \sqrt{2 + \sqrt{2}} \sqrt{2 - \sqrt{2}} = (2 + \sqrt{2}) - \sqrt{4 - 2} = 2$$

The two roots that annihilate each other in the last step stem from different nesting levels. The ensuing relations

$$x_1^2 + x_1x_3 - 2 = 0$$
,  $x_3^2 - x_3x_2 - 2 = 0$ ,  $x_2^2 - x_2x_4 - 2 = 0$  or  $x_4^2 - x_4x_1 - 2 = 0$ 

have a cyclic structure and reduce the symmetry to a cyclic group:

 $G \subseteq \{\,(1),\,(12)(34),\,(1324),\,(1423)\,\} = \,\mathbb{Z}_4$ 

To create an analogous symmetry in the tetrahedron one can reduce the symmetry by drawing arrows and thus allowing only for cyclic rotations among the vertices.

# What does symmetry tell about the solution of an equation?

You may have wondered how the analysis of the structure and symmetry of the solutions could contribute to the original problem, the solution of the equation. The situation is similar to the famous "principle of insight" from gestalt psychology: When finding the right way of restructuring a problem (finding a good gestalt), one often has already found the main step to its solution. This is also true here, although there are still some more details to be understood.

#### Large Symmetry $\leftrightarrow$ Few Relations $\leftrightarrow$ Complex Solutions

The examples have shown the following qualitative behaviour: When the equation has no "special features", there is perfect symmetry between the solutions. Only total symmetric relations such as  $x_1 + x_2 + x_3 + x_4 = 0$  or  $x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 = 0$  hold for the solutions, meaning that the Galois group would contain *all* permutations. The general equation of degree 4

 $(x^4 + ax^3 + bx^2 + cx + d = 0)$  bears maximal symmetry which shows up in the Galois group being the complete symmetric group  $S_4$  of all permutations. Whenever there are features in an equation that lead to unusual relations between the solutions (such as  $x_1 + x_2 = 0$  in the biquadratic equation) certain symmetries are broken (such as (13) in the example). They disappear from the Galois group which reduces to a subgroup of  $S_4$  (such as  $D_4$  in the example). Furthermore: A solution formula for an equation (provided there is one) is less complex with respect to the use of nested roots, the smaller the symmetry is. This indicates that the size of the symmetry group somehow measures the complexity of a potential solution formula.

#### Solving an equation $\leftrightarrow$ Adding radicals $\leftrightarrow$ Reducing the Galois group

Fortunately this qualitative behaviour works in a mathematically very definite manner, giving rise to a complete understanding of the process of solving an equation. Giving a solution of an equation can be seen as a stepwise construction of the solutions by building more and more complex expressions with roots ("radicals"). This process is called "adjoining" and amounts to extending the rational numbers  $\mathbb{Q}$  with roots of rational numbers, and then roots of roots and so on. This is clearly illustrated by "solving" the equation  $x^4 - 6x^2 + 2 = 0$  from above and stepwise build the solutions  $x_{1,2,3,4} = \pm \sqrt{3 \pm \sqrt{7}}$ 

Numbers known in	Some relations between	Symmetry group (=all permutations
this step	the roots	that preserve all relations)
${\mathbb Q}$ - only rational	$x_1 + x_2 = 0, \ x_3 + x_4 = 0$	D <sub>4</sub> = { (1), (12), (34), (12)(34), (13)(24),
numbers	$x_1 x_3 - x_2 x_4 = 0$	(14)(23), (1324), (1423) } - this is the
	$x_1 x_2 + x_3 x_4 - 6 = 0$	Galois group of the equation
	and many more	

In the next step we adjoin as a first new number  $\sqrt{7}$  and also allow rational combinations. This extends the field  $\mathbb{Q}$  to  $\mathbb{Q}(\sqrt{7}) = \{a + b\sqrt{7} \mid a, b \in \mathbb{Q}\}$ . Regarding this number field as "known numbers", new relations between the solutions appear. These relations on the other hand break symmetries and thus reduce the symmetry group.

$\mathbb{Q}(\sqrt{7})$	$x_1 x_2 - 3 - \sqrt{7} = 0$	$V_4 = \{ (1), (12), (34), (12)(34) \}$ - this is a
$= \{a + b\sqrt{7} \mid a, b \in \mathbb{Q}\}$	as an additional relation	subgroup of the Galois group

This process can be continued. When adjoining  $\sqrt{3+\sqrt{7}}$  one solution is already explicitly reached. The symmetry with respect to this solution is completely broken.

$\mathbb{Q}(\sqrt{7})(\sqrt{3+\sqrt{7}})$	$x_1 - \sqrt{3 + \sqrt{7}} = 0$	$\mathbb{Z}_2^{}$ = { (1), (34), } - this is a further
	as an additional relation	subgroup

In a final step, by adjoining  $\sqrt{3-\sqrt{7}}$  the symmetry is completely broken, a total reduction is reached and every solution is expressed by radical expressions.

$\mathbb{Q}(\sqrt{7})(\sqrt{3}+\sqrt{7})(\sqrt{3}-\sqrt{7})$	$x_3 - \sqrt{3 - \sqrt{7}} = 0$	E = { (1) } - total reduction is reached
	as an additional relation	

This example gives a clue about the connection between the central concepts linked with the structure of an equation. Actually all these four processes are more or less the same:

- 1) "constructing solutions of an equation":  $\sqrt{7} \rightarrow \sqrt{3+\sqrt{7}} \rightarrow \sqrt{3-\sqrt{7}}$
- 2) "extending the field of numbers":  $\mathbb{Q} \to \mathbb{Q}(\sqrt{7}) \to \mathbb{Q}(\sqrt{7})(\sqrt{3+\sqrt{7}}) \to \mathbb{Q}(\sqrt{7})(\sqrt{3+\sqrt{7}})(\sqrt{3-\sqrt{7}})$
- 3) "reducing the symmetry between the solutions by finding new relations"
- 4) "finding subgroups of the Galois group":  $D_4 \triangleright V_4 \triangleright \mathbb{Z}_2 \triangleright E$

Mark the parallelism between extending number fields and reducing the Galois groups:

$$D_4 \triangleright V_4 \triangleright \mathbb{Z}_2 \triangleright E$$

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{7}) \subset \mathbb{Q}(\sqrt{7})(\sqrt{3+\sqrt{7}}) \subset \mathbb{Q}(\sqrt{7})(\sqrt{3+\sqrt{7}})(\sqrt{3-\sqrt{7}})$$

This can be taken a step further and leads to a one-to-one relation between *all* subfields (in this example of  $\mathbb{Q}(\sqrt{7})(\sqrt{3}+\sqrt{7})(\sqrt{3}-\sqrt{7})$ ) and *all* subgroups of the Galois Group (in this example  $D_4$ ) – the famous "fundamental theorem of Galois theory".

## Can Galois theory provide formulas for the solutions?

This question should best be answered by Galois himself (although his answer rather sounds like the famous answers in Radio Eriwan jokes: "principally yes, but..."): "*If you now give me an algebraic equation chosen at will and you want to know whether it is solvable by radicals or not, I would only show the means to answer the question, not wanting to charge myself or anyone else to do this. In one word: the calculations are impractical" (Galois, 1832, p.39). You may understand this if you consider that Galois' concrete procedure would require an equation of fifth degree to construct and factorize a polynomial of degree 120. This puzzled many of Galois' contemporaries who had hoped for a feasible algorithm. They simply did not follow Galois on his radically new perspective: Galois stopped looking for a solution algorithm for all equations of fifth or higher degree. Instead he rephrased the question: What is the essential structure of an equation that indicates its solution? He understood that it is not the coefficients but the symmetry of solutions in terms of rational relations. Of course he used many ideas from Lagrange and Ruffini, but essentially it was him who took the giant leap from classical algebra ("how do I solve* 

an equation") to modern algebra ("what is the structure of the equation in terms of symmetry").

Once Galois had established the abstract theory of equation structures he could use it for a higher purpose: His theory could answer the question why the solution by radicals was difficult in one case and easy in another one. And it could even explain why it was sometimes even more than difficult – it was impossible!

This is what we will finally undertake: We will look at the solution process from the point of view of symmetry (i.e. from the reduction of the Galois group). In the example above the stepwise reduction from the Galois group to the trivial group  $D_4 \triangleright V_4 \triangleright \mathbb{Z}_2 \triangleright E$  every step has a "remarkable property" (as Galois himself called it): Every smaller group is a special kind of subgroup of the larger group (a "normal subgroup") and the quotient of the group sizes is always a prime number (in this case 8:4:2:1, so always p=2). Galois realized that this property is necessary and sufficient for the equation to be solved by radicals. For all equations of degree 4 or lower any group can be reduced by obeying the "remarkable property". Among the equations of degree 5 (or higher) most of the examples have no special feature and therefore possess a large Galois group (a large symmetry, a high complexity, few relations between the solutions). The equation  $x^5 - 4x + 2 = 0$  for example has the Galois group S<sub>5</sub> (i.e. all permutations of 5 elements) – no relation between solutions reduces the symmetry - and so one should hope for a reduction like this

 $S_5 \triangleright ... \triangleright ... \triangleright D_5 \triangleright \mathbb{Z}_5 \triangleright E$ 

which, with respect to the group sizes, would amount to 120 : ... : ... : 10 : 5 : 1. But one can show by inspecting the subgroups of  $S_5$  that there is no such sequence as would be necessary. Therefore there can be no general solution by radicals for all equations which have a certain complexity, and in particular a general formula for equations of degree 5 or higher does not exist. This was already known and proven some years before Galois (by Ruffini and Abel), but within an analysis like the one from Galois the answer on solvability is a mere corollary.

## **Further reading**

The explanations of the core ideas behind Galois theory presented here, give a glimpse on the meaning and the beauty of a key theory for modern mathematics.

Many details and many close connections to other aspects (construction with compass and ruler, cyclotomic numbers, invention of complex numbers, minimal polynomials and so on) have been omitted. Fortunately there are many textbooks that not only deliver modern Galois theory in an abstract way (and thereby barring the reader from understanding the key idea) but which try to facilitate an acquaintance with the many aspects of Galois theory. Depending on the intention of the reader different books are recommended:

- The original: Galois, É. (1846). Écrits et Memoires Mathematiques d'Évariste Galois,
  R. Bourgne and J.MP. Azra, Editors, Gauthier-Villars, Paris, 1962. Also:
  Oeuvres Mathematiques d'Évariste Galois, Gauthier-Villars, Paris, 1897, and J.
  Math. Pureset Appl. (1) 11, 381-444.
- An extensive analysis of the original in a classical approach and with a complete English translation: Edwards, H. M. (1984). Galois theory. New York: Springer-Verlag. See also: Edwards, H. M. (2011). Galois's Version of Galois Theory - Talk Presented at the Galois Bicentennial. Institut Henri Poincaré, Paris, October 24, 2011.
- A popular description, accessible without formal mathematics: Stewart, I. (2007). Why beauty is truth: a history of symmetry. New York: Basic Books.
- An elementary approach with an emphasis also on the historical predecessors: Bewersdorff, J. (2006). Galois theory for beginners: a historical perspective. Providence: American Mathematical Society.
- A historical geometric approach not elementary: Klein, F. (1956). Lectures on the Icosahedron and the Solution of Equations of the Fifth Degree. New York: Dover. Republished with commentaries by P. Slodowy, Basel: Birkhäuser, 1993. See also: Nash, O. (2014). On Klein's icosahedral solution of the quintic. Expositiones Mathematicae, 32(2), 99-120. See also: http://arxiv.org/abs/1308.0955
- A textbook on algebra with close connections to school mathematics unfortunately only in German (yet): Leuders, T. (2016). Erlebnis Algebra – zum aktiven Entdecken und selbstständigen Erarbeiten. Heidelberg: Springer.
- A discussion why and how future teachers might approach Galois theory during university: Leuders, T. (2016). Subject Matter Analysis with a Perspective on Teacher Education – The Case of Galois Theory as a Theory of Symmetry. Journal für Mathematikdidaktik