Évariste Galois and the Solvability of Equations

Ross Dempsey

Department of Physics and Astronomy
Johns Hopkins University

JHU Splash, 2018

Outline

Math on a Clock

- Modular arithmetic is arithmetic with an upper bound
- Example, modulo 5:

$$1+2 \equiv 3 \pmod 5, \qquad 2+3 \equiv 0 \pmod 5, \qquad 3+4 \equiv 2 \pmod 5$$

Math on a Clock

- Modular arithmetic is arithmetic with an upper bound
- Example, modulo 5:

$$1+2 \equiv 3 \pmod 5, \qquad 2+3 \equiv 0 \pmod 5, \qquad 3+4 \equiv 2 \pmod 5$$

- Basically: a set ($\{0, 1, 2, 3, 4\}$), and an operation ($+$)

Rubik's Cube

- There are a set of operations you can perform on a Rubik's cube
- Performing two in sequence is equivalent to another operation

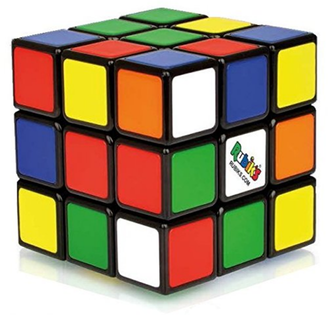


Figure: A Rubik's cube has 43,252,003,274,489,856,000 possible moves.

Rubik's Cube

- There are a set of operations you can perform on a Rubik's cube
- Performing two in sequence is equivalent to another operation
- Basically: a set ($\{FRL, \ldots\}$), and an operation ($\circ$)

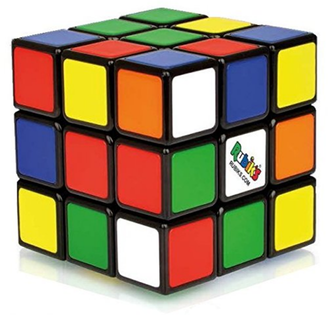


Figure: A Rubik's cube has 43,252,003,274,489,856,000 possible moves.

Definition of a Group

- A group G consists of:
  - A set UG
  - An associative operation $\circ$, closed in UG, with an identity and an inverse for each element of UG
- An *Abelian* group is one for which the operation $\circ$ is commutative

Definition of a Group

- A group G consists of:
  - A set UG
  - An associative operation $\circ$, closed in UG, with an identity and an inverse for each element of UG
- An *Abelian* group is one for which the operation $\circ$ is commutative
- More examples:
  - Permutations of students
  - Symmetries of a pentagon
  - Rotations of a sphere

Groups as Symmetries

- Recipe for a group:
  - Take any object
  - Find the set of all transformations which leave that object invariant
  - This set, under composition, forms the symmetry group of the object

Groups as Symmetries

- Recipe for a group:
  - Take any object
  - Find the set of all transformations which leave that object invariant
  - This set, under composition, forms the symmetry group of the object
- *All groups can be constructed in this way*

Groups as Symmetries

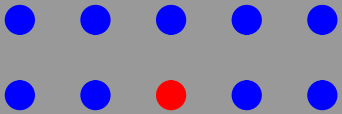
- Recipe for a group:
  - Take any object
  - Find the set of all transformations which leave that object invariant
  - This set, under composition, forms the symmetry group of the object
- *All groups can be constructed in this way*
- Group theory is a powerful method for studying symmetries in a general way

Group Actions

- Even if a group comes from symmetries, the group itself is not tied to an object
- A *group action* specifies how elements of a group act on some object
- Example: group of 3D rotations has an action on 3D space
- If part of the object is left alone by an element of the group, we say it is a *fixed point* of that element

Subgroups

- Groups can have smaller groups, called subgroups living inside them
- When a symmetry is partially broken, the leftover symmetry group is a subgroup of the original
- Example: permutations



Conjugacy Classes

- A group element g is said to be conjugate to h if $g = xhx^{-1}$ for some $x \in G$
- Elements of a group split into conjugacy classes of conjugate elements
- Example: rotations of a sphere are conjugate if they are by the same angle

$$R_z(45^\circ) = R_y(-90^\circ)R_x(45^\circ)R_y(90^\circ)$$

Normal Subgroups

- A subgroup is *normal* if it consists of full conjugacy classes
- Was the subgroup of permutations in the previous example normal?
- How about the subgroup of rotations about the z axis only?

Normal Subgroups

- A subgroup is *normal* if it consists of full conjugacy classes
- Was the subgroup of permutations in the previous example normal?
- How about the subgroup of rotations about the z axis only?
- Neither are normal. Do these groups have normal subgroups?

Normal Subgroups

- A subgroup is *normal* if it consists of full conjugacy classes
- Was the subgroup of permutations in the previous example normal?
- How about the subgroup of rotations about the z axis only?
- Neither are normal. Do these groups have normal subgroups?
- The permutations S_5 have the subgroup A_5

Normal Subgroups

- A subgroup is *normal* if it consists of full conjugacy classes
- Was the subgroup of permutations in the previous example normal?
- How about the subgroup of rotations about the z axis only?
- Neither are normal. Do these groups have normal subgroups?
- The permutations S_5 have the subgroup A_5
- The rotations $SO(3)$ have no nontrivial normal subgroup, so it is called *simple*

Finite Simple Group of Order Two

https://www.youtube.com/v/UTby_e4-Rhg?rel=0

Fields

- Groups are powerful, but can't capture everything
- Ordinary math involves two operations, multiplication and addition
- This can be captured by *fields*. A field is:
  - An Abelian group for the addition operation
  - A mutliplication operation, invertible for everything except 0, and distributive over addition
- Examples: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$

Other Fields

- Consider the set of all numbers of the form $a + b\sqrt{2}$, where a and b are rational

Other Fields

- Consider the set of all numbers of the form $a + b\sqrt{2}$, where a and b are rational
  - Are the operations closed?

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2},$$
$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$$

Other Fields

- Consider the set of all numbers of the form $a + b\sqrt{2}$, where a and b are rational
  - Are the operations closed?

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2},$$
$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$$

  - Is multiplication invertible?

$$\frac{1}{a + b\sqrt{2}} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}$$

Other Fields

- Consider the set of all numbers of the form $a + b\sqrt{2}$, where a and b are rational
  - Are the operations closed?

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2},$$
$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$$

  - Is multiplication invertible?

$$\frac{1}{a + b\sqrt{2}} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}$$

  - All other properties inherit from the ambient field $\mathbb{R}$. So yes, this is a field.

Other Fields

- Consider the set of all numbers of the form $a + b\sqrt{2}$, where a and b are rational
  - Are the operations closed?

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2},$$
$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$$

  - Is multiplication invertible?

$$\frac{1}{a + b\sqrt{2}} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}$$

  - All other properties inherit from the ambient field $\mathbb{R}$. So yes, this is a field.
- This is a *field extension* over the rationals, denoted $\mathbb{Q}(\sqrt{2})$

Degree of Extension

- For any (finite) field extension, we can define a *degree*
- Intuitively, a field extension is composed of elements like $a_1 + a_2\alpha + \ldots + a_n\zeta$, and n is the degree

Degree of Extension

- For any (finite) field extension, we can define a *degree*
- Intuitively, a field extension is composed of elements like $a_1 + a_2\alpha + \ldots + a_n\zeta$, and n is the degree
- Degree of $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$ is 2, since elements are $a_1 + a_2\sqrt{2}$

Degree of Extension

- For any (finite) field extension, we can define a *degree*
- Intuitively, a field extension is composed of elements like $a_1 + a_2\alpha + \ldots + a_n\zeta$, and n is the degree
- Degree of $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$ is 2, since elements are $a_1 + a_2\sqrt{2}$
- Degree is written as $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$

Construction by Compass and Straightedge

- You may have heard that it is impossible to trisect an angle via compass and straightedge
- To prove this, you can show that a compass and straightedge only permits degree 2 field extensions
- Trisection of angles requires a degree 3 field extension

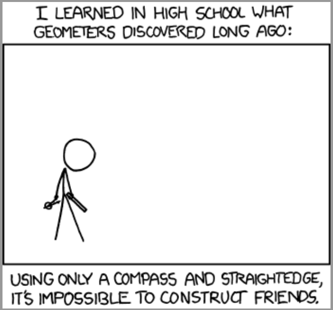


Figure: Impossiblity theorems are sad.

Splitting Fields

- Recipe for a field extension: take a polynomial, and adjoin all its roots to the base field
- Example: $x^2 - 2$ over $\mathbb{Q}$. Adjoin $\pm\sqrt{2}$ to $\mathbb{Q}$ to form $\mathbb{Q}(\sqrt{2})$
- In the splitting field, a polynomial splits: $x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$

Splitting Fields

- Recipe for a field extension: take a polynomial, and adjoin all its roots to the base field
- Example: $x^2 - 2$ over $\mathbb{Q}$. Adjoin $\pm\sqrt{2}$ to $\mathbb{Q}$ to form $\mathbb{Q}(\sqrt{2})$
- In the splitting field, a polynomial splits: $x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$
- The degree $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ equals the degree of the *minimum polynomial* of α over $\mathbb{Q}$

Towers of Extensions

- What is the degree of the splitting field of $x^4 - 2 = 0$?

Towers of Extensions

- What is the degree of the splitting field of $x^4 - 2 = 0$?
- The degree of $\mathbb{Q}(\sqrt[4]{2})$ is 4...but that's not the splitting field.

Towers of Extensions

- What is the degree of the splitting field of $x^4 - 2 = 0$?
- The degree of $\mathbb{Q}(\sqrt[4]{2})$ is 4...but that's not the splitting field.
- The roots are $\{\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}\}$, so we need $\mathbb{Q}(\sqrt[4]{2}, i)$

$$\mathbb{Q}(\sqrt[4]{2}, i)$$

2

$$\mathbb{Q}(\sqrt[4]{2})$$

4

$$\mathbb{Q}$$

Towers of Extensions

- What is the degree of the splitting field of $x^4 - 2 = 0$?
- The degree of $\mathbb{Q}(\sqrt[4]{2})$ is 4...but that's not the splitting field.
- The roots are $\{\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}\}$, so we need $\mathbb{Q}(\sqrt[4]{2}, i)$

$$\mathbb{Q}(\sqrt[4]{2}, i)$$

2

$$\mathbb{Q}(\sqrt[4]{2})$$

4

$$\mathbb{Q}$$

Towers of Extensions

- What is the degree of the splitting field of $x^4 - 2 = 0$?
- The degree of $\mathbb{Q}(\sqrt[4]{2})$ is 4...but that's not the splitting field.
- The roots are $\{\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}\}$, so we need $\mathbb{Q}(\sqrt[4]{2}, i)$

$$\mathbb{Q}(\sqrt[4]{2}, i)$$

2

$$\mathbb{Q}(\sqrt[4]{2})$$

4

$$\mathbb{Q}$$

- Total degree:
$[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4 \cdot 2 = 8$

Field Automorphisms

- Consider the field extension $\mathbb{Q}(\sqrt{2})$ and the map $f(a + b\sqrt{2}) = a - b\sqrt{2}$
- This respects multiplication and addition:

$$f(x) + f(y) = f(x + y)$$
$$f(x) \cdot f(y) = f(x \cdot y)$$

- It also leaves elements of the base field $\mathbb{Q}$ alone
- We call such a map a $\mathbb{Q}$-automorphism

Field Automorphisms

- Remember the recipe for groups? Take an object, look at transformations leaving its structure invariant.
- Field automorphisms are exactly this kind of construction
- The F-automorphisms of an extension E over a field F are called the *Galois group* of E over F

Enter Galois

- Évariste Galois (1811–1832) was one of the most badass mathematicians ever

Figure: Évariste Galois at age 15.

Enter Galois

- Évariste Galois (1811–1832) was one of the most badass mathematicians ever
- Tried to gain admission to École Polytechnique, but was rejected since the examiner couldn't understand his logical leaps

Figure: Évariste Galois at age 15.

Enter Galois

- Évariste Galois (1811–1832) was one of the most badass mathematicians ever
- Tried to gain admission to École Polytechnique, but was rejected since the examiner couldn't understand his logical leaps
- Staunch revolutionary; after being expelled from École Normale for criticizing its director, he joined the National Guard

Figure: Évariste Galois at age 15.

Enter Galois

- Évariste Galois (1811–1832) was one of the most badass mathematicians ever
- Tried to gain admission to École Polytechnique, but was rejected since the examiner couldn't understand his logical leaps
- Staunch revolutionary; after being expelled from École Normale for criticizing its director, he joined the National Guard
- Arrested for threatening the life of King Louis Philippe; later served six months in prison, where he continued his mathematical work

Figure: Évariste Galois at age 15.

Galois' Final Days

- In 1832, Galois was somehow talked into a duel

Figure: Évariste Galois at age 15.

Galois' Final Days

- In 1832, Galois was somehow talked into a duel
- He was shot in the abdomen, and died the next morning

Figure: Évariste Galois at age 15.

Galois' Final Days

- In 1832, Galois was somehow talked into a duel
- He was shot in the abdomen, and died the next morning
- But, beforehand, he had collected all his mathematical thoughts in a letter

Figure: Évariste Galois at age 15.

Galois' Final Days

- In 1832, Galois was somehow talked into a duel
- He was shot in the abdomen, and died the next morning
- But, beforehand, he had collected all his mathematical thoughts in a letter
- "This letter, if judged by the novelty and profundity of ideas it contains, is perhaps the most substantial piece of writing in the whole literature of mankind."

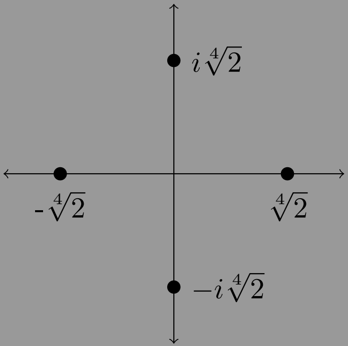
Figure: Évariste Galois at age 15.

The Galois Correspondence

- We have seen the Galois group, $\mathrm{Gal}(E/F)$: the group of F-automorphisms of E
- Galois showed that the subgroups of $\mathrm{Gal}(E/F)$ correspond to field extensions living between E and F
- This is the fundamental theorem of Galois theory

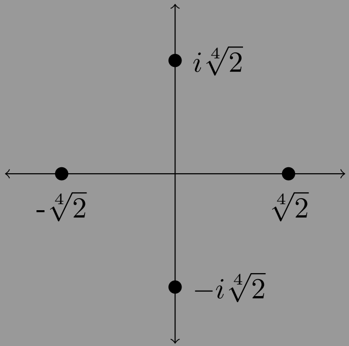
Example: $x^4 - 5x^2 + 6$

- We have already seen that the splitting field of $x^4 - 2$ is $\mathbb{Q}(\sqrt[4]{2}, i)$
- What are the $\mathbb{Q}$-automorphisms?



Example: $x^4 - 5x^2 + 6$

- We have already seen that the splitting field of $x^4 - 2$ is $\mathbb{Q}(\sqrt[4]{2}, i)$
- What are the $\mathbb{Q}$-automorphisms?



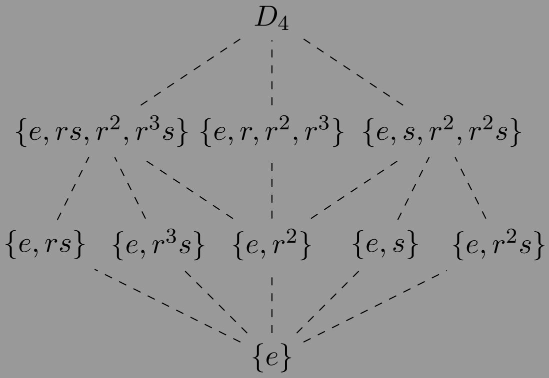
- The automorphisms are the symmetries of the square, generated by rotations $\sqrt[4]{2} \to i\sqrt[4]{2}$ and reflections $i \to -i$

Example: $x^4 - 2$

- This group is called D_4 (in general, D_n are the $2n$ symmetries of an n-gon)
- Let's call the rotation r and the reflection s. What are the subgroups?

Example: $x^4 - 2$

- This group is called D_4 (in general, D_n are the $2n$ symmetries of an n-gon)
- Let's call the rotation r and the reflection s. What are the subgroups?



Example: $x^4 - 2$

- Consider one of these subgroups, $\{e, rs\}$. Which field elements does it leave invariant?

Example: $x^4 - 2$

- Consider one of these subgroups, $\{e, rs\}$. Which field elements does it leave invariant?
- Any element of the form $a + b(1-i)\sqrt[4]{2}$ is invariant

Example: $x^4 - 2$

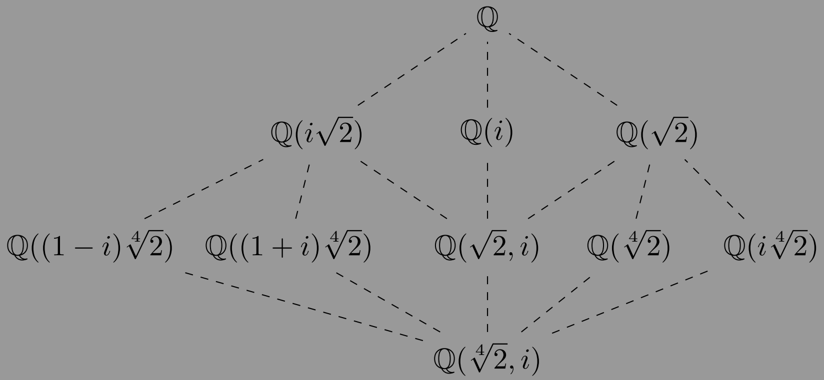
- Consider one of these subgroups, $\{e, rs\}$. Which field elements does it leave invariant?
- Any element of the form $a + b(1-i)\sqrt[4]{2}$ is invariant
- Galois associates the field extension $\mathbb{Q}((1-i)\sqrt[4]{2})$ with this subgroup

Example: $x^4 - 2$

- Consider one of these subgroups, $\{e, rs\}$. Which field elements does it leave invariant?
- Any element of the form $a + b(1-i)\sqrt[4]{2}$ is invariant
- Galois associates the field extension $\mathbb{Q}((1-i)\sqrt[4]{2})$ with this subgroup
- What happens if we make this association for each subgroup?

Example: $x^4 - 2$

- Every field extension between $\mathbb{Q}$ and $\mathbb{Q}(\sqrt[4]{2}, i)$ appears
- Inclusion is reversed



Solution by Radicals

- To solve a polynomial equation corresponds to descending the lattice on the previous slide to build the splitting field
- Galois's theorem relates this to a sequence of groups with a particular property

Solution by Radicals

- To solve a polynomial equation corresponds to descending the lattice on the previous slide to build the splitting field
- Galois's theorem relates this to a sequence of groups with a particular property
- Such a sequence does not exist for all groups

Solution by Radicals

- To solve a polynomial equation corresponds to descending the lattice on the previous slide to build the splitting field
- Galois's theorem relates this to a sequence of groups with a particular property
- Such a sequence does not exist for all groups
- Galois shows that the Galois group for the general quintic polynomial does not have such a sequence

Solution by Radicals

- To solve a polynomial equation corresponds to descending the lattice on the previous slide to build the splitting field
- Galois's theorem relates this to a sequence of groups with a particular property
- Such a sequence does not exist for all groups
- Galois shows that the Galois group for the general quintic polynomial does not have such a sequence
- This proves the Abel-Ruffini theorem: there exists no general method of solution by radicals for quintic and higher polynomials