

Simple Polynomials For 5 Year Olds

Warren Jin

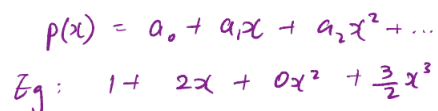
24 March 2023

1 Introduction

Modern mathematical education is in a sad state. If you walk on the street and ask anyone what a radical field extension is they will only return you weird looks. To amend this I propose a simple plan to revitalize mathematical pedagogy for preschoolers in order to spark their interest in math. Below I shall highlight a comprehensive curriculum on low-order polynomials and abstract algebra accessible to children between the ages of 2 and 5.¹

2 Quadratics

If a 2 year old knows their abc's, they're ready to know their $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$'s. This is a good time to start introducing the concept of polynomials to a child. We define polynomials as such: a polynomial of a single variable $p(x)$ of degree n can be represented as $\sum_{k=0}^n a_k x^k, a_k \in \mathbf{R}$.


$$p(x) = a_0 + a_1x + a_2x^2 + \dots$$

Eg: $1 + 2x + 0x^2 + \frac{3}{2}x^3$

Figure 1: The simple polynomial, written in a more readable form.

The quadratic formula above is used to find the solutions to the equation $p(x) = 0$ for $n = 2$. However, when the child attempts to solve certain equations, interesting things that they have not met before might surface. If $\exists q \in \mathbf{Q}$ such that $\Delta = b^2 - 4ac = q^2$, everything is fine. But let's say Δ is not the square of some rational number, then (if it is positive) we end up with a square root in the value of x . Why this is important will become clear later. Another problem is if $\Delta < 0$. Now we get into the realm of complex numbers, which might not make

¹In all seriousness, this article assumes the reader is somewhat familiar with group theory and algebra. The article will talk generally about polynomials of the 2nd to 5th degree, and use some results of Galois theory in a very general and simplified way to demonstrate certain results regarding quintics; however, as simplified as they are, it is very difficult to make Galois theory understandable to a non-specialist audience. But of course I will try my best.

much sense to your 2 year old, who must now count $\text{Re}(x)$ with their fingers and $\text{Im}(x)$ with their toes.

3 Cubics

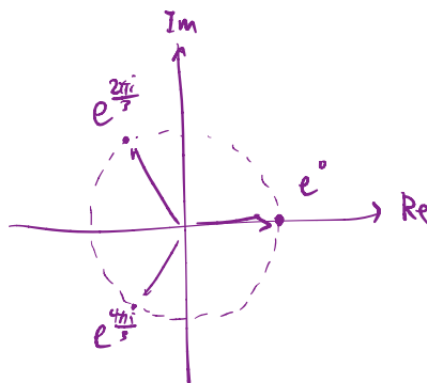


Figure 2: The 3rd roots of unity on the complex plane.

At this stage the child is most likely around 3 years old and getting bored of quadratics. He or she will now try to solve a cubic; however, without having the proper tools, they will have to derive the answer themselves. We give them a real monic polynomial $t^3 + at^2 + bt + c = 0$. After counting on their fingers for a while, they will inevitably stumble upon the Tschirnhausen transformation:

$$t = y - \frac{a}{3}$$

$$y^3 + \frac{-a^2 + 3b}{3}y + \frac{2a^3 - 9ab + 27c}{27} = 0$$

We can reasonably assume that the child knows Vieta's formulas, so they will try to manipulate this equation into something of the form $a + b = m$ and $ab = n$. The parent, who probably knows Cardano's formula, can now suggest the substitution:

$$y = \sqrt[3]{u} + \sqrt[3]{v}$$

which is inspired by the final form we are searching for. By choosing certain values of u and v , we can get:

$$-(u + v) = \frac{2a^3 - 9ab + 27c}{27} = q$$

$$uv = -\left(\frac{-a^2 + 3b}{3 \cdot 3}\right)^3 = -\frac{p^3}{27} (*)$$

We can define the fractions in terms of q and p for simplicity. If you plug the two solutions u and v into a quadratic formula using Vieta's, we get that the two roots of $k^2 + qk - \frac{p^3}{27} = 0$ are $-\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$. Plug this back into our substitution for y (then t) to obtain:

$$t = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} - \frac{a}{3}$$

Handwritten diagram showing the derivation of the cubic formula. It starts with the cubic equation $t^3 + at^2 + bt + c = 0$. A purple arrow points down to $y^3 + py + q = 0$. Another purple arrow points down to $y = \sqrt[3]{u} + \sqrt[3]{v}$. A red dashed arrow points from this equation to the quadratic equation $k^2 + qk - \frac{p^3}{27} = 0$. A purple arrow points up from the quadratic equation to the text "Solve for u & v ". A red dashed arrow points from the quadratic equation to the equations $-(u+v) = q$ and $uv = -\frac{p^3}{27}$.

Figure 3: A short summary of our derivation, in case you are lost before you can teach your 3 year old kid. Purple arrows indicate forward direction to reduce the cubic into a quadratic; red lines indicate backward solving.

That was relatively simple. However, remember Figure 2: every cubic will seem to have a bunch of weird complex solutions. If we take $\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} = z$, then $\omega_3 z$ and $\omega_3^2 z$ (where ω_3 is the 3rd root of unity, or $e^{\frac{2\pi i}{3}}$) are also valid cube roots of the term inside the root. So then we seem to run into a problem: if we let $t = u + v - \frac{a}{3}$, then each of u and v can be permuted in one of 3 ways ($u, \omega_3 u, \omega_3^2 u$) to give a total of 9 solutions. The ingenious child will now point back to (*) and realize that if $p \in \mathbf{R}$, then the products of whatever permutations are chosen for u and v must have the roots of unity cancelling each other out by becoming 1. We know $\omega_3^3 = 1$, so the only valid solutions are of the forms: $t \in \{u + v - \frac{a}{3}, \omega_3 u + \omega_3^2 v - \frac{a}{3}, \omega_3^2 u + \omega_3 v - \frac{a}{3}\}$.

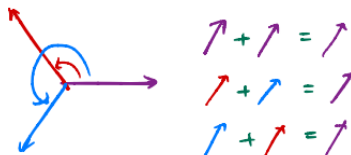


Figure 4: Visualize ω in terms of these arrows and it becomes clearer: ω_3 maps to the red arrow, and ω_3^2 is the blue arrow. To get a real number, we must somehow make a purple arrow from the rotations; hence, something like red + red will not work because it becomes blue.

4 Quartics

So the child is now 4, and wants to do something other than cubics. They now venture onto degree 4 polynomials. For brevity I shall not elaborate on the exact method used, except to note that after fiddling one's thumbs for sufficiently long, the child must inevitably come to the Tschirnhausen transformation again, except now $t = y - \frac{a}{4}$. Some manipulation will yield a very long equation, where we apply the method of completing the square to yield a cubic. Since we know how to solve a cubic already, we can easily derive the answer from here.

5 Quintic

By now the child must be very eager to try a quintic equation at the mature age of 5. So we let them apply the Tschirnhausen transformation $t = y - \frac{a}{5}$, and this yields the following equation:

$$y^5 + py^3 + qy^2 + ry + s = 0$$

for some complicated fractions p, q, r , and s . The child goes along trying to figure out how they can choose some substitution or reduce the equation into a quartic. Unfortunately, they do not know that centuries before them Lagrange tried the same thing and only managed to turn the degree-5 polynomial into a degree-6 polynomial.² So we have played a little trick on the kid! Let's see why it is.

²Ian Stewart, Galois Theory (3rd Edition), p12.

$$\begin{aligned}
& \star \quad \forall \nearrow_1, \nearrow_2 \in \{ \text{purple } \nearrow, \text{red } \nearrow, \text{blue } \nearrow \}, \\
& \quad \nearrow_1 + \nearrow_2 \in \{ \text{purple } \nearrow, \text{red } \nearrow, \text{blue } \nearrow \}. \\
& \quad \quad \quad \text{(closure)} \\
& \star \quad \forall \nearrow_1, \exists \nearrow_2 \in \{ \text{purple } \nearrow, \text{red } \nearrow, \text{blue } \nearrow \}, \\
& \quad \nearrow_1 + \nearrow_2 = \text{purple } \nearrow; \nearrow + \text{purple } \nearrow = \nearrow \quad \forall \nearrow. \\
& \quad \quad \quad (\text{purple } \nearrow \text{ is the identity element and } \nearrow_1, \nearrow_2 \text{ are inverses}) \\
& \star \quad (\nearrow_1 + \nearrow_2) + \nearrow_3 = \nearrow_1 + (\nearrow_2 + \nearrow_3) \\
& \quad \quad \quad (\text{the operation "+" is associative}) \\
& \star \quad \nearrow_1 + \nearrow_2 = \nearrow_2 + \nearrow_1 \\
& \quad \quad \quad ("+" \text{ is commutative})
\end{aligned}$$

Figure 5: The set of arrows we previously introduced in Figure 4 can be considered a group (by the first 3 stars alone - the last pink star is optional). If you do not understand why, then a quick refresher on groups is in order. Remember that a group is a set with an operator (let's call it +, though this symbol doesn't *have* to represent addition) such that it is closed under the application of this operator to two elements of itself. It also has an identity element e such that for any element g , $e + g = g + e = g$, and there exists some element h such that $h + g = e$. Lastly, $(f + g) + h = f + (g + h)$, so the operation is associative. A certain type of groups is also commutative, i.e. $f + g = g + f$. These are called abelian groups, and \mathbf{Q} , $(\mathbf{Z}/n\mathbf{Z})^\times$ (group of integers modulo n under multiplication), and the group of purple, red, and blue arrows above are all examples of this.

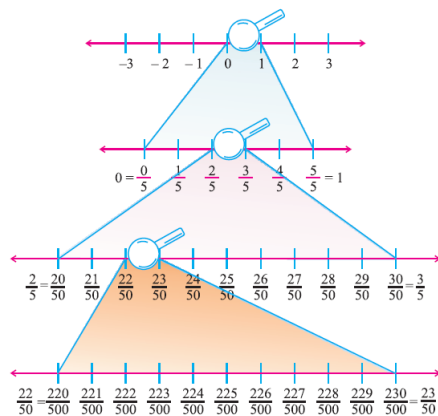


Figure 6: (Image from onlinemath4all.com) A slightly more complex algebraic structure is a field. Put simply, a field F is a set with *two* operations (which we can call $+$ and $*$, though they need not be addition and multiplication in the normal sense). The first operation $+$ forms an abelian group over F (look at Figure 5 if you forgot what this means). We can call e , the identity element for this operation, 0. The second operation $*$ also forms an abelian group over $F \setminus \{0\}$ and satisfies a distributive property whereby $a * (b + c) = a * b + a * c$. So if we look at \mathbf{Q} , we know that $\mathbf{Z} \subset \mathbf{Q}$, so for any integer n , since $\mathbf{Q} \setminus \{0\}$ is a group under $*$, and $n * \frac{1}{n} = 1$, then $\frac{1}{n}$ must be in \mathbf{Q} . And since we can choose any other integer m , by the property of closure we know $\frac{m}{n} \in \mathbf{Q}$. Thus \mathbf{Q} is a field that contains every rational number expressible as the fraction of two integers.

By now it is imperative to explain some Galois theory.³ We define a field extension F on \mathbf{Q} , which we denote as F/\mathbf{Q} , such that $\mathbf{Q} \subseteq F$ and has the same operations as F . Complicated? Let's see an example. So let's say we want to add $\sqrt{2}$ to the rationals. This field extension F (also denoted as $\mathbf{Q}(\sqrt{2})$) can be considered as the field of all real numbers of the form $a + b\sqrt{2}$, for $a, b \in \mathbf{Q}$. It is easy to see that $\mathbf{Q} \subseteq F$ as any element $r \in \mathbf{Q}$ satisfies $r = r + 0\sqrt{2}$.

We also call $\mathbf{Q}(\sqrt{2})$ a radical field extension, which is a type of field extension that that only be obtained by constructing a *tower* of field extensions F/K where F contains k for some $k^n \in K$, and where K is another field extension, such that at the bottom of this tower of field extensions we have the rational field \mathbf{Q} . Each step along the way, the extension F/K is called a simple radical extension. For example, $\mathbf{Q}(\sqrt{1 + \sqrt{2}}, \sqrt{3})$ is a radical field extension which can be arrived at by the following tower of simple radical extensions:

³Which I will arduously attempt to simplify within a little over 1000 words. But please look at Figures 5 and 6, they are immensely helpful if you are not familiar with group theory and field theory.

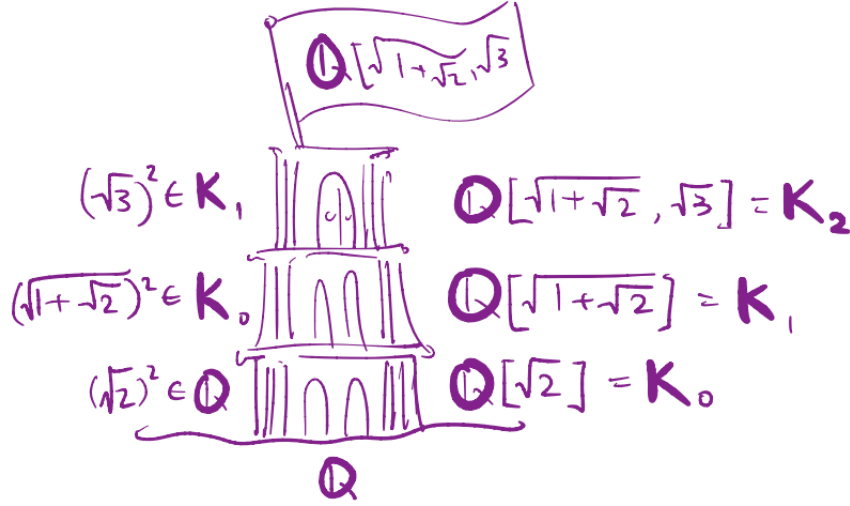


Figure 7: Each layer adds of a radical that was not in the previous layer. The end result is a radical field extension of \mathbb{Q} .

Recall that we were talking about polynomials. In this article we consider polynomials $p(x) \in \mathbb{Q}(x)$.⁴ If we look at the quadratic $p(x) = x^2 - 2$, we see that its roots are in $\mathbb{Q}(\sqrt{2})$. We thus call $\mathbb{Q} \subseteq F$ a *splitting field* of $p(x)$. Formally, the splitting field of any polynomial $p(x)$ is the smallest field extension of \mathbb{Q} that contains *all* the roots of $p(x)$. Recall what we said in the quadratics section: if Δ is not the square of a rational, we end up with roots that are no longer in \mathbb{Q} even if our polynomial is in $\mathbb{Q}(x)$.

Another example: we have $p(x) = (x^2 - 2)(x^2 + 1)$. Its splitting field is $\mathbb{Q}(\sqrt{2}, i)$, because this will contain everything of the form $a + b\sqrt{2} + ci + di\sqrt{2}$.

Now consider a bijective function $f : F \rightarrow F$ defined over our field extension. If this function satisfies the condition $f(q) = q \forall q \in \mathbb{Q}$, or equivalently that it *fixes* the subfield \mathbb{Q} , then it is called a \mathbb{Q} -automorphism. In simple English: $f(x)$ maps the field F to itself by rearranging (or not) the elements while keeping \mathbb{Q} unchanged, it is a \mathbb{Q} -automorphism. Example: we can define $f(a + b\sqrt{2}) = a - b\sqrt{2}$ and $g(a + bi) = a - bi$. These are \mathbb{Q} -automorphisms of $\mathbb{Q}(\sqrt{2}, i)$. So is $h(x) = x$ - remember how I said we don't need to rearrange anything for it to be an automorphism?

⁴Polynomials with rational coefficients.

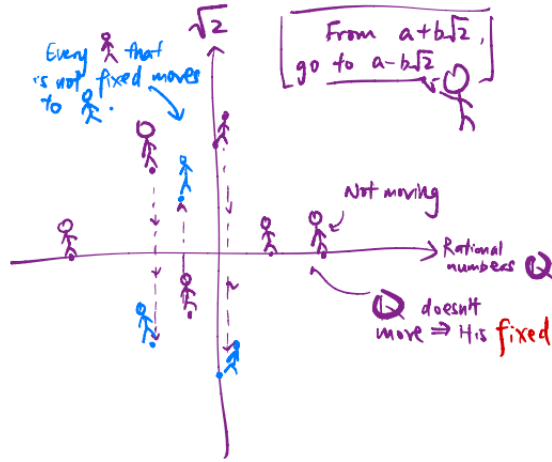


Figure 8: Illustration explaining a \mathbb{Q} -automorphism of $\mathbb{Q}(\sqrt{2})$. Purple guys on the rational number axis do not move, and those above or below it move to their mirror image (the conjugate). This is \mathbb{Q} -automorphism since \mathbb{Q} can be seen to be *fixed*, and because this mapping will make every stickman end up somewhere else on this same graph, instead of sending them to some other graph like the complex plane. Etymologically, ‘auto-’ means ‘self’, and ‘morph’ means ‘form’, so it makes sense that everything must stay with its original ‘form’ or ‘space’.

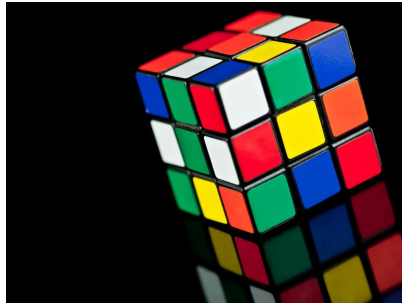


Figure 9: (Image from the Smithsonian Magazine) An analogy to understand field automorphisms is the Rubik’s cube. Let the 6 center squares be analogous to the base field, which in our article is \mathbb{Q} . Let the field extension be analogous to the squares that border an edge of the cube. If you’ve ever played with a cube before, you know that no matter how you twist the cube’s faces, you cannot change the relative positions of the center squares. Similarly, if we have a field automorphism, no matter how it changes stuff around in the field extension, it leaves the base field fixed. Our combinations of Rubik’s cube moves also meets the other criterion for automorphisms, which is that a Rubik’s cube after some twists is still a Rubik’s cube, and not, for example, a soccer ball.

And finally, we come to the Galois group of the field extension F/\mathbf{Q} , which is the group of all \mathbf{Q} -automorphisms. We are working in the realm of polynomials, so we can also say that for a splitting field F of $p(x)$, $\text{Gal}(p)$ is the group of all automorphisms of F that fix \mathbf{Q} . Still using $p(x) = (x^2 - 2)(x^2 + 1)$, we have $\text{Gal}(p) = \{1, f, g, fg\}$ (same functions as above) where 1 is the identity element (i.e. $h(x) = x$) and the group operator \cdot means $f \cdot g = f(g(x))$. It is quite easy to verify that this is a group, since the way we defined f and g (conjugation) mean that applying either to itself yields the identity element (i.e. they are self-inverse).

Very simple so far. So how does this apply to our polynomials? Recall the tricks we used to solve cubics and quartics. What these tricks essentially do are to take the roots of these polynomials and swap them around in some way. The same is said of a \mathbf{Q} -automorphism, as it takes some root in the field extension and maps it to some other root on the field extension. Thus, if you view the roots of $p(x) = (x^2 - 2)(x^2 + 1)$, we know that any element of $\text{Gal}(p)$ will take one of its roots and turn it into another root. Because the roots are just being permuted, $\text{Gal}(p) \subseteq S_4$ (the group of all permutations of 4 elements). For our particular $p(x)$, $\text{Gal}(p)$ is the Klein 4-group (K_4), as f and g are their own inverses and $f \cdot g$ is the last element.⁵

\cdot	1	f	g	fg
1	1	f	g	fg
f	f	1	fg	g
g	g	fg	1	f
fg	fg	g	f	1

Figure 10: A graph showing the outcomes of combining two functions from $\text{Gal}(p) = \{1, f, g, fg\}$. Remember that f takes $a + b\sqrt{2}$ to its conjugate, whereas g takes a complex number to its conjugate (and fg thus takes the conjugate of both). Since $\text{Gal}(p) \simeq K_4$, this group is abelian and so it doesn't matter whether you read the column or the row first, but for simplicity let's just say that if f is the row and g is the column, then we read $f \cdot g = fg$ from this chart.

The problem when we try to do this to quintics is that, put simply, permuting the roots will result in more possible combinations than when we started, whereas doing this for cubics and quartics gives us *less* possibilities than what we started with, which allows us to apply some tricks to turn a cubic into a quadratic, and a quartic into a cubic.

⁵That is quite literally the definition of K_4 , which is a four-element group where every element is its own inverse and any two elements (other than 1) can be combined to make the last element. This is easy to show from the fact that $f \cdot f = 1$ and that the operation is commutative.

The Galois theory way of expressing this is that S_5 is not solvable.⁶ A solvable group is one which can be constructed by a tower of field extensions on abelian groups⁷ and if we have some quintic polynomial $q(x)$ such that $\text{Gal}(q) \simeq S_5$ (the two are isomorphic, i.e. a 1-to-1 mapping exists to pair up any element of $\text{Gal}(q)$ with its buddy in S_5), then $\text{Gal}(q)$ is not solvable. Note that this implies the existence of solvable quintics, so long as its Galois group is not isomorphic to S_5 .

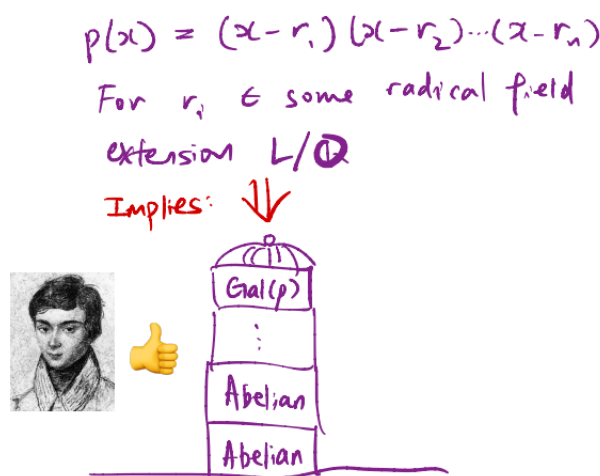


Figure 11: If some polynomial is solvable by using only plus, minus, multiply, divide, and n^{th} roots, this implies that its Galois group can be constructed as a tower of abelian subgroups.

I know this all sounds extremely complicated, but for the article let's just assume that if $p(x) = 0$ is solvable with some combination of (possibly nested) radical roots then $\text{Gal}(p)$ is solvable.⁸ From the previous paragraph, we can take a contrapositive: if a group cannot be constructed by a tower of field extensions on abelian groups, then it is **not solvable**. Therefore, if I can prove that some group in the tower that builds up to S_5 is not abelian, and that $\text{Gal}(q) \simeq S_5$, then we can very lazily conclude that this class of quintics is not solvable, meaning that there is no *general* radical solution to quintics.

So at this point we need to define how we construct our tower.⁹ I posit that for any floor, the floor beneath it must be the subgroup containing all the elements k on this floor that satisfy $h \cdot g \cdot k = g \cdot h$. This is called a commutator subgroup. If our floor is the commutator subgroup of itself, then the floor below

⁶Recall that this is the permutation set of 5 elements.

⁷There are some other conditions that I will not delve into. Just assume that they hold in our case.

⁸Implying that if $\text{Gal}(p)$ is not solvable, then our polynomial does not have roots that can be represented with radicals.

⁹Technically there can be more than one way, but by the Jordan-Holder Theorem they are all equivalent.

will be the trivial subgroup $\{e\}$, which will be the ‘ground level’.¹⁰

We already know the symmetric group S_n is the permutation set of n elements. We now introduce the alternating group A_n , which is the set of all *even* permutations of n elements. An even permutation is one which can be represented by an even number of swaps between elements. If we have the ordering $\{1, 2, 3\}$, $\{2, 1, 3\}$ is not an even permutation because no matter how many times you try to swap the numbers around, you will never get the latter permutation with an even number of swaps. On the other hand, $\{3, 1, 2\}$ is an even permutation. In general, if (a, b) means we swap the a^{th} and b^{th} elements in the set, $\{2, 1, 3\} = \{1, 2, 3\}(1, 2)$ and $\{3, 1, 2\} = \{1, 2, 3\}(2, 3)(1, 2)$. All elements of A_5 are expressible as $(a_1, b_1)(a_2, b_2)\dots(a_{2k}, b_{2k})$.

I posit that A_5 is the commutator subgroup of S_5 , because for swaps denoted A and B in S_5 , $BAA^{-1}B^{-1}AB = AB$, and $A^{-1}B^{-1}AB$ an even permutation!¹¹ So A_5 is the floor below S_5 , and below A_5 is E as A_5 is its own commutator subgroup.¹² Here is the problem: A_5 is not abelian, as $\{1, 2, 3, 4, 5\}(1, 2)(2, 3) = \{2, 3, 1, 4, 5\}$ which $\neq \{1, 2, 3, 4, 5\}(2, 3)(1, 2) = \{3, 1, 2, 4, 5\}$. As one example suffices to show that the operation is not commutative, A_5 is not abelian. So, this ‘floor’ of our tower is not abelian, and thus S_5 is **not solvable**!

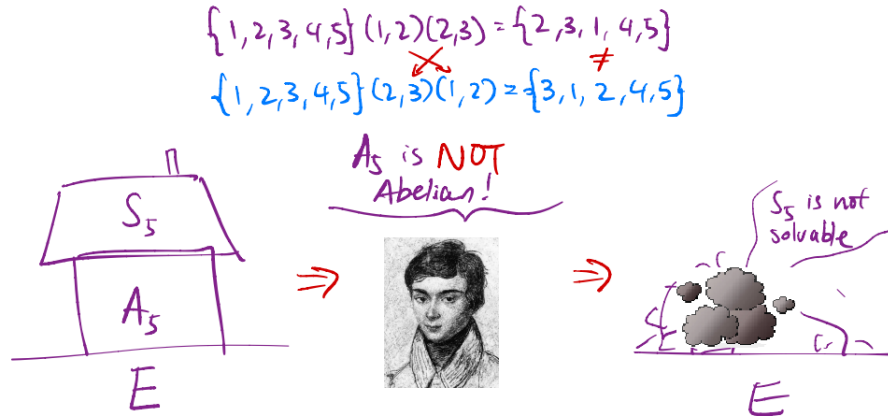


Figure 12: In case you still don’t get why A_5 is nonabelian, try doing this with the pens on your table. We conclude that if $\text{Gal}(p) \simeq S_5$, its corresponding tower will collapse from structural weakness caused by noncommutativity!

¹⁰Also denoted as E , which is the group that contains only one element which is the identity and is self-inverse. This is so obviously a group that it is kind of trivial, so we call it the trivial group.

¹¹It is actually a bit more complicated to prove that the commutator subgroup of S_5 and A_5 are exactly equal, but intuitively this should make sense.

¹²I leave this as an exercise to the reader.

High level overview

Now let's talk a bit more generally about radical field extensions. We can use a result of Galois theory to enlarge the splitting field of a solvable polynomial $p(x)$ into a Galois extension that is also radical.¹³ Since the Galois group of any simple radical extension is cyclic¹⁴ and any cyclic group is abelian, thus the tower of compositions must all consist of abelian 'floors' and we have our solvable group.

If we apply this to our proof, we only need to posit that the Galois group of a radical field extension is solvable.¹⁵ We proved that S_5 is not solvable. So, similar to our reasoning above, if $\text{Gal}(p) \simeq S_5$, it's unsolvable, so by contrapositive the splitting field of $p(x)$ is not a radical field extension.

We can extend our proof to polynomials of degrees higher than 5. Generally, there are some higher-degree polynomials that are solvable by radicals, but our unfortunate kid can never find a formula for them as they could for quadratics, cubics, and quartics.

6 Conclusion

Simple polynomials are fascinating, but we have shown that there is only so much you can do with algebra alone. Galois theory, on the other hand, bridges field theory and group theory, and can be used to prove many other things I have not included. So, I suggest, 6 year olds should start learning some Galois theory.

¹³A Galois extension F/K is the splitting field of an n th-degree polynomial with n *distinct* roots in the field K . Thus a Galois extension is normal and separable, a splitting field extension is normal but not necessarily separable. We enlarge it until it is separable. We also know that the splitting field can be thought of as a way to represent any root of our polynomial as a linear combination of a finite number of factors; see page 7.

¹⁴It can be generated by a single element, known as the generator.

¹⁵I will not attempt to prove this, as it involves a complicated induction proof and I have less than 150 words left.