TODO: title

2025-07-31

TODO: intro

First degree

Here's one for my kindergarten fans out there. Can you solve this equation?

$$x + a = 0$$

What's x?

What's a?

...

Just kidding.

Hint: Subtract a from both sides... And try clicking me!

You might see boxes like this one throughout the article. If they have an arrow at the right end, it means they have hidden content and you can expand to see it by clicking on them.
Another thing worth mentioning. Writing a blog with aesthetically pleasant math formulas is totally not easy. They have to look good in all kinds of devices. For this reason, the safest workaround so that I don't risk someone seeing absolute rubbish is to use horizontal scroll bars when the formula might otherwise overflow the screen. This will rarely appear on a large monitor but will be quite frequent in mobile devices, and I think there's no way to force a scroll bar actually showing on mobile browsers, so I had to warn you. If you feel like a formula is going out of the screen, please try to scroll it even if you don't see a scroll bar! Here, an example:

I am not one of those who fear to die, and I will not go quietly to the grave without telling the truth. My lif

Second degree

I know that one

Our *good ol'* friends the Babylonians were already solving second degree equations… Ok, yeah, they didn't formulate them in the same way, but they really could solve them. For us, this is a second degree equation:

$$ax^2 + bx + c = 0$$

Now it's your time to shine… You do remember that formula you were forced to memorize in high school, don't you? Yes!

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Huh…

This is supposed to be an entry to Summer of Math Exposition #4. If you check this link, you'll find one part that goes like this:

> **Most Frequently Requested Topics**
>
> Foundation-Level Concepts (Ages 11-16):
>
> 1. Variables and algebra - Students don't understand that "x" represents an unknown value to find
>
> …

Well, well, we just started and I'm already digging my own pit. I think I'll just wait for someone else to address that in a whole post. If you happen to be one of those confused students and you end up here, well, good luck with that. You have all your time. Don't think the post will be an *easy* read. But as for the prerequisites, I don't expect from you anything more than the algebra and complex numbers you were taught in high school.

While you probably knew the above formula with the coefficients a, b, c just like that, I'm going to be using the same letter with subscripts, where a_i is the coefficient of the term x^i.

Moreover, note that the coefficient a_n of the highest degree term (here a_2) is useless: the equation obtained from dividing everything by that coefficient will have the same roots.

> **Why are the roots the same?**
>
> If x_1 is a solution of $a_2x^2 + a_1x + a_0 = 0$, then we have:
>
> $$a_2x_1^2 + a_1x_1 + a_0 = 0$$
>
> But zero divided by any number will still be zero, so we have:
>
> $$\frac{1}{a_2} \cdot (a_2x_1^2 + a_1x_1 + a_0) = \frac{1}{a_2} \cdot 0 = 0$$
>
> This is the same as:
>
> $$x_1^2 + \frac{a_1}{a_2}x + \frac{a_0}{a_2} = 0$$
>
> This last relation exactly means that x_1 is also a solution of the new equation, which has no coefficient for the x^2 term.

So the equation we'll work with looks like this:

$$x^2 + a_1x + a_0 = 0$$

We haven't talked about which values can the coefficients of the equation take. We could decide that they can be *any natural number* $(0, 1, 2 \ldots)$, *any integer* $(0, 1, -1, 2, -2 \ldots)$, *any rational*… From now on, we'll assume they're rational numbers.

> **What's a rational number?**
>
> This is just a fancy term for fractions, the result of dividing one integer by another. They are things like $0, \frac{1}{2}, -\frac{57}{3}, -2$… Of course, integers are also rationals because any integer a can be written as $\frac{a}{1}$.

And why not choosing, say, just integers? Because we need some freedom with the operations we do with coefficients. When we talked about dividing everything by a_2, we were already considering that the new coefficients had to be at least rational. Otherwise, depending on which division we perform, if we had integers initially, we could now end up with something that isn't an integer anymore. Thus, if we choose rational coefficients we're allowed to do basic operations (sum, subtract, multiply, divide) with them and always be sure that the result will still be a rational number.

> It's dividing fractions… What's dividing a fraction by a fraction anyway?
>
> — *Only yesterday* (1991)

No, I'm not going to explain how to divide fractions today. I just wanted an excuse to include a part of one of my favourite movies, where Taeko, the protagonist, shows her frustration of not being able to understand the logic behind dividing fractions. *Ok, I get what I have to do, but why is it like that?* This is a recurring theme in many fields, and math is no exception. I also feel like this, even while doing my research to write this post. Many suggest that math is something you start understanding while you do it, meaning that you shouldn't force yourself too far to get the logic behind some concepts until you have already spent quite some time working with them. While I do agree with this, and is partly how I accept my own knowledge gaps, I will try my best in this article to build some intuition.

So just for the last time, let's rewrite the equation and the solution with the new letters…

$$x^2 + a_1 x + a_0 = 0 \text{ where } a_0,\ a_1 \text{ are rationals}$$

$$x = \frac{-a_1 \pm \sqrt{a_1^2 - 4a_0}}{2}$$

But how did you get there?

Shut up and memorize!

Just joking. Let's see what we can do…

In the previous section we talked about equations and solutions. We might sometimes still use that terminology, but we're also going to talk about polynomials and roots. For our purposes, an equation can be expressed as $p(x) = 0$, where $p(x)$ is a polynomial. In the quadratic example, the polynomial would be $p(x) = x^2 + a_1 x + a_0$. A root of the polynomial is any value that gives an output of 0 when plugged as x into that polynomial. Therefore, a solution of the equation is a root of the polynomial.

Suppose we give names x_1, x_2 to our hypothetical roots. If something is a root, as we just said, it should evaluate the polynomial to 0. This must work for both roots, so when factored out, the polynomial should look like $(x - x_1)(x - x_2)$. Here, if we change x by either x_1 or x_2, the result will be 0 as expected. Can you express the coefficients a_1 and a_0 in terms of the roots x_1 and x_2?

Hint: try expanding the product $(x - x_1)(x - x_2)$

Let's expand the product:

$$(x - x_1)(x - x_2) = x^2 + (-x_1 - x_2)x + x_1x_2$$

But considering the original polynomial looked like $x^2 + a_1x + a_0$, that means we have the following equalities for our roots:

$$\begin{cases} x_1 + x_2 = -a_1 \\ x_1x_2 = a_0 \end{cases}$$

The cool thing about these relations is that the result of adding or multiplying the roots is again a rational number (because our coefficients were rationals), even if the roots themselves might not be rational. In fact, knowing that, any weird expression made up of sums and products of roots, say $\frac{(x_1+x_2)^3}{3x_1x_2} - 4(x_1 + x_2)(x_1x_2)^6$, will be *rationally known*. I'm using these words on purpose, because that's how Galois himself referred to quantities that ultimately evaluate to a rational number, even if the operands themselves aren't necessarily rationals (like our roots). Keep this cool observation in mind, you'll see why in just a while.

So we have to figure out a formula for both roots. They're just two now, yes, but you know this is going further, right? We will work with higher degree equations later. Wouldn't it be cool if we could just find the value of *one* thing, and then get the value of all roots *for free* just from that? Of course, besides this weird value, we're also allowed to use the original coefficients of the polynomial or any other known numbers.

I'll help you with that. There are probably a lot of values we could choose to find, but I'll give you this one:

$$t = x_1 - x_2$$

Of course you're now supposed to check that this does *encode* everything about the roots x_1 and x_2. Can you write them in terms of t?

Hint: use also $-a_1 = x_1 + x_2$

Remember learning how to solve systems of equations in high school? Reduction method, is that you?

$$\left.\begin{aligned} t &= x_1 - x_2 \\ -a_1 &= x_1 + x_2 \end{aligned}\right\} \Rightarrow \begin{cases} x_1 = \dfrac{-a_1 + t}{2} \\ x_2 = \dfrac{-a_1 - t}{2} \end{cases}$$

Do you see where this is going? Of course, we'll now try to find the value of t! But why would this be easier?

> **Hint: try to find the value of t^2 first**
>
> Well, instead of computing t, let's try with t^2:
>
> $$t^2 = (x_1 - x_2)^2 = x_1^2 + x_2^2 - 2x_1x_2 = (x_1 + x_2)^2 - 4x_1x_2 \overset{\text{cool obs.}}{=} a_1^2 - 4a_0$$
>
> You do know what happened in the last step, right? The cool observation we made earlier. We put everything in terms of $x_1 + x_2$ and x_1x_2, so we can then use the known rational coefficients, and we're done. We know what t^2 is, so we can now pick a square root and have $t = \sqrt{a_1^2 - 4a_0}$.

Now that we know the value of t, getting back the values of the original roots x_1 and x_2 is routine substitution in the equalities we stated earlier.

But before claiming our trophy in the form of a final result, let's expand our perspective a bit. Suppose we craft another equation, of which we're sure that t is a root, and we know how to solve this new equation. That way we would get the value of t, just like above, hoping that it would be easier than trying to solve the original equation.

So… How does such an equation look like? The one I'll show you won't be too surprising, and you'll even think I'm just making fun of you, but keep in mind I'm trying to prepare a recipe for future sections. Alright, the equation:

$$(x - t)(x + t) = 0$$

Of course this equation makes sense. We already made a useful observation before. If t has to be a root, there must be a factor like $(x - t)$ out there. The reason we also included $(x + t)$ is that now this product will give a neat result, as you might expect from before. Yes, we just happen to know that because we already calculated t^2 before, and this seems to be some circular reasoning, but bear with me, this will be a useful reinterpretation later…

$$\begin{gathered}(x - t)(x + t) = 0 \\ \Downarrow \\ x^2 - t^2 = 0 \\ \Downarrow \\ x^2 = t^2 \\ \Downarrow \\ x = \sqrt{t^2} = \sqrt{a_1^2 - 4a_0} = t\end{gathered}$$

At this point you might be wondering why I never bother to write the typical sign $\pm$ to represent that we could take either the positive or the negative value, in this case, when taking the square root. At least for our quadratic example, this is irrelevant! Why? Well, you just look back at the relations:

$$\begin{cases} x_1 = \dfrac{-a_1 + t}{2} \\ x_2 = \dfrac{-a_1 - t}{2} \end{cases}$$

If we take the positive value, that is, $t = \sqrt{a_1^2 - 4a_0}$, then we get the solutions:

$$\begin{cases} x_1 = \dfrac{-a_1 + \sqrt{a_1^2 - 4a_0}}{2} \\ x_2 = \dfrac{-a_1 - \sqrt{a_1^2 - 4a_0}}{2} \end{cases}$$

If we instead take the negative value, i.e., $t = -\sqrt{a_1^2 - 4a_0}$, then our solutions will be:

$$\begin{cases} x_1 = \dfrac{-a_1 - \sqrt{a_1^2 - 4a_0}}{2} \\ x_2 = \dfrac{-a_1 + \sqrt{a_1^2 - 4a_0}}{2} \end{cases}$$

They're the same but swapped! So who cares? We just wanted to find the roots in the first place, we didn't even define what should be called x_1 and what x_2, there's just no difference. This also somehow addresses another question you might have had. We want to find the value of the root t from the new equation. *But how do we even know which one of the roots is t?* Well, as we just said, it turns out any of them works… The more general answer to this question isn't that easy, but will play a crucial role in our understanding of these equations, and we'll get back to it later. *No spoilers.*

First symmetry

I bet you know what's coming next… But before we try to tame that naughty cubic equation, we need some polynomial machinery. We'll find some symmetries along the way, I hope you're excited!

Let's recall the cool observation from previous section:

$$\begin{cases} x_1 + x_2 = -a_1 \\ x_1 x_2 = a_0 \end{cases}$$

The question is obvious… Can we find something similar for the cubic equation?

$$x^3 + a_2x^2 + a_1x + a_0 = 0 \text{ where } a_0,\ a_1,\ a_2 \text{ are rationals}$$

Yes we can! Hint: expand $(x - x_1)(x - x_2)(x - x_3)$

We proceed the same way as for the quadratic. If the roots are x_1, x_2 and x_3, we should be able to factor the equation like $(x - x_1)(x - x_2)(x - x_3)$. What do we get from here? You can check it yourself:

$$(x - x_1)(x - x_2)(x - x_3) = x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_1x_3 + x_2x_3)x - x_1x_2x_3$$

We got our relations!

$$\begin{cases} x_1 + x_2 + x_3 = -a_2 \\ x_1x_2 + x_1x_3 + x_2x_3 = a_1 \\ x_1x_2x_3 = -a_0 \end{cases}$$

I know you're seeing the pattern for the coefficients:

- Sum of all roots, negative sign
- Sum of all products of two different roots, positive sign
- Sum of all products of three different roots, negative sign
- …

Now pay attention to this. If we have an equation of degree n, in coefficient a_i, we have all possible different ways of choosing $n - i$ roots. What happens if we swap any two of the roots? Of course, nothing! We rearranged some sums and products, but since the order doesn't matter, and we were including all possible products, we still have the same result! We say that these expressions are *symmetric* polynomials. A polynomial on the roots $x_1, x_2, \ldots, x_n$ is *symmetric* if it doesn't change no matter how we rearrange the roots.

The symmetric polynomials we've been working with actually have a special name: they're called *elementary symmetric polynomials*. Any guess for why they have this name? I'll give you a few examples to think.

Let's take for example this obviously symmetric polynomial:

$$x_1^2 + x_2^2 + x_3^2$$

Can we know its value? Let's rewrite it…

Hint: try to relate this value with $(x_1 + x_2 + x_3)^2$

$$x_1^2 + x_2^2 + x_3^2 = (x_1 + x_2 + x_3)^2 - 4(x_1x_2 + x_1x_3 + x_2x_3) = a_2^2 - 4a_1$$

Yes! That's a known rational number.

Let's try another symmetric polynomial:

$$x_1^3x_2 + x_2^3x_3 + x_3^3x_1$$

Oops! This is not a symmetric polynomial! Can you see why? It needs a small fix:

$$x_1^3x_2x_3 + x_1x_2^3x_3 + x_1x_2x_3^3$$

Yes, much better now. Can you prove this one is indeed symmetric? Hint: it's enough to check swaps of two roots. That's because any rearrangement of roots can be explained as a series of swaps of two roots. Now, is this also a known value?

Hint: is this a product of two familiar expressions…?

$$x_1^3x_2x_3 + x_1x_2^3x_3 + x_1x_2x_3^3 = (x_1^2 + x_2^2 + x_3^2)(x_1x_2x_3) = (a_2^2 - 4a_1) \cdot (-a_0)$$

Well, this one also worked. Do you see where I'm going?

We were already observing in a previous section that any expression written in terms of these elementary symmetric polynomials has a known rational value, no matter how complicated the expression may be. An expression written in terms of elementary symmetric polynomials is of course symmetric, because each of these terms is. But can we go further?

Any symmetric polynomial can be written in terms of elementary symmetric polynomials.

I hope you agree this is not obvious at all. And the statement just like that doesn't seem too interesting. Because we know that elementary symmetric polynomials are known rational numbers, then we get this more insightful result for free:

Any symmetric polynomial on the roots is a known number.

We'll use this result a few times later. Of course, we should prove the first statement about elementary symmetric polynomials. In Galois' time, this was such a well-known fact that he didn't even bother including it in the prerequisites for his memoir.

Why is this true?

TODO: sketch of proof

Third degree

Déjà vu

Time for the cubic! Just to recap, this is what we have to start with:

$$x^3 + a_2x^2 + a_1x + a_0 = 0 \text{ where } a_0,\ a_1,\ a_2 \text{ are rationals}$$

$$\begin{cases} x_1 + x_2 + x_3 = -a_2 \\ x_1x_2 + x_1x_3 + x_2x_3 = a_1 \\ x_1x_2x_3 = -a_0 \end{cases}$$

Remember what we did in the Second degree section? We were discussing the possibility of finding a special value t which could encode all the information about our roots, in the sense that we could find their values just from t itself and other known values. For the quadratic we used $t = x_1 - x_2$. Can we find such a value for the cubic?

Hint: Can you use the solutions of the equation $x^3 = 1$?

Yes we can! Did you think about complex roots of unity? If you like following the pattern, for the quadratic we have $t = \alpha_1 x_1 + \alpha_2 x_2$ where α_1, α_2 are the solutions of the equation $x^2 = 1$. These are of course 1 and -1.
What are the solutions of $x^3 = 1$? They're 1, ω and ω^2, where ω is a complex root of $x^2 + x + 1 = 0$. Then, again just following the pattern, we could think of the following special value:

$$t = x_1 + \omega x_2 + \omega^2 x_3$$

This is just a hunch! In order to use this, we should actually show that all x_1, x_2, x_3 can be expressed in terms of this t and other known values.

Now that we got the value, it's time to show that the roots can be expressed in terms of this t… Or that's what I thought while writing this. Too optimistic… I'm not saying it's not possible, but it can be quite difficult to get those formulas. Instead of trying to narrow down to a single value t, let's try for a moment to use two values, the other being very similar to t. I'll help you with this one.

Check these relations

$$\begin{cases} t = x_1 + \omega x_2 + \omega^2 x_3 \\ t' = x_1 + \omega^2 x_2 + \omega x_3 \\ -a_2 = x_1 + x_2 + x_3 \end{cases}$$

Can you now find the roots by using t, t', ω and the coefficients?

Hint: Can you use the fact that $1 + \omega + \omega^2 = 0$?

We can try to sum all three equations multiplied by specific coefficients so that our root remains there and the other two are cancelled out à la reduction method, because of the given relation of ω.
Doing that, we get these formulas for the roots:

$$\begin{cases} x_1 = \dfrac{t + t' - a_2}{3} \\ x_2 = \dfrac{\omega^2 t + \omega t' - a_2}{3} \\ x_3 = \dfrac{\omega t + \omega^2 t' - a_2}{3} \end{cases}$$

OK, so we can get the roots by using both t and t'. Yes, I know what you're thinking. We now have to find two values instead of one, but trust me, this is justified, since these values seem so similar that I hope we'll be able to find both of them *at the same time*.

You already know how this goes, now we have to build a polynomial for which t is a root, and hopefully, just hopefully, t' will also be one of its roots. Let's recall, or rather expand, the way we built the polynomial for the quadratic case. I told you it would be helpful later, and the time has come.

Remember that we had $t = x_1 - x_2$. Our special polynomial for the quadratic was this:

$$(x-t)(x+t) = (x-(x_1-x_2))(x+(x_1-x_2)) = (x-(x_1-x_2))(x-(x_2-x_1)) = x^2-((x_1-x_2)+(x_2-x_1))x+(x_1-x_2)(x_2$$

You already know what the actual polynomial is, but I left it in this last form to notice something: the coefficients are symmetric polynomials on the roots! If you try swapping x_1 and x_2 in both expressions $((x_1 - x_2) + (x_2 - x_1))$ and $(x_1 - x_2)(x_2 - x_1)$, you get the same result. In the previous section, we just saw that all symmetric polynomials on the roots are actually known values. They're made from the coefficients of the original equation, which were rational, so we got a new equation with rational coefficients.

Of course, there *is* one concern. Perhaps this new equation is just as hard to solve as the original one, and then we did something completely useless. While that's a possibility, we were hoping that our choice of t would make the new equation sufficiently easy to solve. In the case of the quadratic, you know that this was true because we were able to lose the term of x, and get a simpler quadratic $x^2 - t^2 = 0$, which only requires to take a square root to solve.

We saw the coefficients we got in the end are symmetric polynomials, but we could have deduced that from the start, from the way we defined the polynomial as a product. Yes, in the quadratic example it was easier to see why we would benefit from choosing both t and $-t$ (sum times difference is the difference of squares). Another way to look at this is that $-t$ is the result of swapping the roots in t:

$$(x - (\text{t with no swaps}))(x - (\text{t with roots swapped}))$$

This form is telling us that this is a symmetric polynomial *on the roots*, and therefore, that its final coefficients will be known rational values. Can you see why? I'll let you figure that out, because now it's your turn again… Can you use this idea to find a suitable new polynomial for the cubic, for which t and t' are two of its roots? Just to remember, these are their expressions:

$$\begin{cases} t = x_1 + \omega x_2 + \omega^2 x_3 \\ t' = x_1 + \omega^2 x_2 + \omega x_3 \end{cases} \quad \text{The value } \omega \text{ is such that } 1 + \omega + \omega^2 = 0$$

Come on, try to find the polynomial!

Hint: Why is the quadratic example a symmetric polynomial on its roots?

We defined it as the product of two terms. Note that the order of the product doesn't matter. What happens to the expression if we swap the roots x_1 and x_2? Then we get:

$$(x - (\text{t with roots swapped}))(x - (\text{t with no swaps}))$$

And this is certainly the same polynomial. For the quadratic, all the possible rearrangements are only swapping both roots or leaving them the same way. Since all these rearrangements give the same polynomial, we can say the polynomial is symmetric in the roots x_1 and x_2. Do you see how this helps for the cubic?

Hint: You'll get a wild expression for the cubic, but try to simplify as much as possible.

The previous hint talked about *all rearrangements* of the roots. This should already be a really good hint. Yes, we're doing exactly that. Let's start from t and find all possible expressions that come from rearrangements of x_1, x_2 and x_3 in t:

$$\begin{cases} x_1 + \omega x_2 + \omega^2 x_3 = t \\ x_1 + \omega x_3 + \omega^2 x_2 = t' \\ x_3 + \omega x_1 + \omega^2 x_2 = \omega t \\ x_2 + \omega x_1 + \omega^2 x_3 = \omega t' \\ x_2 + \omega x_3 + \omega^2 x_1 = \omega^2 t \\ x_3 + \omega x_2 + \omega^2 x_1 = \omega^2 t' \end{cases}$$

There are quite some things going on there, so you'd better pause and check those relations hold. Note that we also included t' in there! We now see that t' was just one of the expressions obtained from the rearrangements of the roots in t. Of course, now we'll build a polynomial that has all of these as roots, so in particular it will have both t and t' as roots, just like we wanted! The reason I wrote the equalities above is so that we now don't have to write the absolute beast that this polynomial would be as a product. We will instead just write the right side of the equalities:

$$(x-t)(x-t')(x-\omega t)(x-\omega t')(x-\omega^2 t)(x-\omega^2 t')$$

Oh, yeah, we're going to have fun trying to simplify this… But by now we should know that, no matter how complicated it looks, in the end, this should be a polynomial with rational coefficients. It's a symmetric polynomial on the roots, *we* made it like that by multiplying all rearrangements of roots.

What happens if we try to multiply only those terms having t? I'll let you check that, but the product simplifies nicely because of the relations $1 + \omega + \omega^2 = 0$ and $\omega^3 = 1$:

$$(x-t)(x-\omega t)(x-\omega^2 t) = x^3 - t^3$$

We can of course do the same with the terms involving t':

$$(x-t')(x-\omega t')(x-\omega^2 t') = x^3 - t'^3$$

So because of the useful relations that we got from the roots of unity, our product simplified into this much cleaner expression:

$$(x^3 - t^3)(x^3 - t'^3)$$

Yes, we still have some work to do to simplify that…

I ain't doing that

I really like these *boxes* that help hiding *spoilers* and try to encourage you, my dear lazy reader, to work through some of the steps on your own. Of course, we can't hide everything inside these boxes and the text must keep flowing. I'll now have to show how the polynomial we were looking for in the previous section looks like, but I'm showing a simplified expression. The moral of the story is that the *spoiler* isn't the polynomial itself, because it's simplified. The real *spoiler* is the series of steps you needed to get there! Remember we're trying to build intuition.

And in fact, we already got a lot of intuition from the previous section! This section is only meant to show you that we can actually end and get the solutions of the cubic, although it's more of a rutinary calculation from here on. You and me are both lazy human beings that don't bother doing those mundane calculations, do we? Let's see what we can do...

We left at this point:

$$(x^3 - t^3)(x^3 - t'^3)$$

We can expand that product and get this:

$$x^6 - (t^3 + t'^3)x^3 + t^3t'^3$$

See, the values t^3 and t'^3 don't have to be rationals themselves, but since this came from a symmetric polynomial on the roots, the coefficients must be rationals! And we want to try solving a polynomial with known coefficients... OK, OK, you don't have to calculate those coefficients if you don't want to. I'll tell you what they really are, but we'll give them short names u and v for a while after that:

$$\begin{cases} u = t^3 + t'^3 = -27a_0 + 9a_1a_2 - 2a_2^3 \\ v = t^3t'^3 = (-3a_1 + a_2^2)^3 \end{cases}$$

i So you still want to know how I got them...

Let the computer do the boring stuff for you! We can use the `sympy` package available in Python. If you're interested but never used Python, it's fine, most of it reads more or less like math, so you can probably still read through the steps below.
We first define all the symbols we need in our expressions:

```python
import sympy

x1, x2, x3, a0, a1, a2, w = sympy.symbols("x1 x2 x3 a0 a1 a2 w")
t = x1 + w * x2 + w**2 * x3
t_prime = x1 + w**2 * x2 + w * x3
```

Here I tried to guess that $t \cdot t'$ is already a symmetric polynomial. If that's true, then we only need to raise that to the third power.

```python
from sympy.polys.polyfuncs import symmetrize

expr, _ = symmetrize(t * t_prime, [x1, x2, x3])

expr = expr.subs(
    {
        x1 + x2 + x3: -a2,
        x1 * x2 + x2 * x3 + x3 * x1: a1,
        x1 * x2 * x3: -a0,
    }
)

expr
```

$a_1\left(w^2 + w - 2\right) + a_2^2$

Looks like poor `sympy` needs some help with ω… Of course! It doesn't even know what ω is yet.

```python
expr.subs(1 + w + w**2, 0)
```

$-3a_1 + a_2^2$

And $t \cdot t'$ was indeed a symmetric polynomial! Then we also got the desired value:

$$t^3 t'^3 = (-3a_1 + a_2^2)^3$$

Let's do the same for $t^3 + t'^3$:

```
expr, _ = symmetrize(t**3 + t_prime**3, [x1, x2, x3])

expr = expr.subs(
    {
        x1 + x2 + x3: -a2,
        x1 * x2 + x2 * x3 + x3 * x1: a1,
        x1 * x2 * x3: -a0,
    }
)

expr
```

$-a_0\left(12w^3 - 9w^2 - 9w + 6\right) - a_1a_2\left(3w^2 + 3w - 6\right) - 2a_2^3$
We can first get rid of the ω^3 part:

```
expr = expr.subs(w**3, 1)
expr
```

$-a_0\left(-9w^2 - 9w + 18\right) - a_1a_2\left(3w^2 + 3w - 6\right) - 2a_2^3$

```
expr.subs(1 + w + w**2, 0)
```

$-a_0\left(-9w^2 - 9w + 18\right) - a_1a_2\left(3w^2 + 3w - 6\right) - 2a_2^3$
You naughty `sympy`, why won't you listen to me? Well, let's try simplifying first…

```
expr.simplify().subs(1 + w + w**2, 0)
```

$-27a_0 + 9a_1a_2 - 2a_2^3$
Yes! We got a really neat expression:

$$t^3 + t'^3 = -27a_0 + 9a_1a_2 - 2a_2^3$$

We'll use the actual values of u and v later, just to not write too long equations. It turns out we end up with a surprisingly cool equation:

$$x^6 - ux^3 + v = 0$$

Another way to look at it is this:

$$(x^3)^2 - u(x^3) + v = 0$$

Can you see it? This is really just a quadratic equation!

$$x^3 = \frac{u \pm \sqrt{u^2 - 4v}}{2}$$

We can obviously just take a cube root now and obtain a solution:

$$x = \sqrt[3]{\frac{u \pm \sqrt{u^2 - 4v}}{2}}$$

No, this isn't one solution, these are a lot of solutions! Yes, that's right. We already had this kind of discussion before, right? In this case, we have two possible values for the inner square root, and three possible values for the outer cube root. The six possible solutions! Which ones are t and t'? Unfortunately, in this case, we can't just choose any combination.

By now I think it's time we get rid of t'. How come? Well, we already derived a useful relation:

$$\begin{gathered} t \cdot t' = -3a_1 + a_2^2 \\ \Downarrow \\ t' = \tfrac{-3a_1 + a_2^2}{t} \end{gathered}$$

Let's go back to our original equations for the roots. We originally wanted to get back the roots by just using one quantity t and other known values. We finally made it!

$$\begin{cases} x_1 = \dfrac{t + \frac{k}{t} - a_2}{3} \\ x_2 = \dfrac{\omega^2 t + \omega \frac{k}{t} - a_2}{3} \\ x_3 = \dfrac{\omega t + \omega^2 \frac{k}{t} - a_2}{3} \end{cases} \quad \text{where } k = -3a_1 + a_2^2$$

Did the question change in any way? How do we know which root of the new polynomial is the t we want? Of course, we could always try all six possible values in these equations for x_1, x_2 and x_3, and double check if they really are solutions of the original cubic equation.

Will you do that for me? Well...

Before we die in the attempt, let's try to give some short expressions for all six roots. We will fix one of them and get the others in terms of that one. We'll call this one t, but this is just a name for a fixed root, it could be any of them. Suppose then that t is this:

$$t = \sqrt[3]{\frac{u + \sqrt{u^2 - 4v}}{2}}$$

When taking cube roots, one way of writing all three of them is to fix one and multiply by roots of unity to get the others (because of course you get the same if you again raise to the third power). That means another two roots are ωt and $\omega^2 t$.

What about the other three? We should take the negative sign for the square root inside. If we call that one t', we then have the relation we defined earlier:

$$t \cdot t' = k \Rightarrow t' = \frac{k}{t} \quad \text{where } k = -3a_1 + a_2^2$$

So another root is $\frac{k}{t}$. Since there's also a cube root there, we can pick another two roots to be $\omega \frac{k}{t}$ and $\omega^2 \frac{k}{t}$. So after fixing one root t, all six of them can be expressed like this:

$$\left\{ t, \omega t, \omega^2 t, \frac{k}{t}, \omega \frac{k}{t}, \omega^2 \frac{k}{t} \right\}$$

Remember this t was just some fixed root. If we use this one, in the equations above for the roots, we would get x_1, x_2 and x_3 in that order. That's basically just the definition. How about trying to input ωt where t appears in the equations?

Hint: Try to relate with the original expressions in t

$$\begin{cases} \dfrac{(\omega t) + \frac{k}{(\omega t)} - a_2}{3} = \dfrac{\omega t + \omega^2 \frac{k}{t} - a_2}{3} = x_3 \\ \dfrac{\omega^2 (\omega t) + \omega \frac{k}{(\omega t)} - a_2}{3} = \dfrac{t + \frac{k}{t} - a_2}{3} = x_1 \\ \dfrac{\omega(\omega t) + \omega^2 \frac{k}{(\omega t)} - a_2}{3} = \dfrac{\omega^2 t + \omega \frac{k}{t} - a_2}{3} = x_2 \end{cases}$$

In the first one we used the equality $\frac{1}{\omega} = \frac{\omega^2}{\omega^2} \cdot \frac{1}{\omega} = \omega^2$.

Perhaps unexpectedly, we got the same set of solutions, but in a different arrangement! Let's try with another one, for example, $\frac{k}{t}$:

Hint: same idea as before

$$\begin{cases} \dfrac{(\frac{k}{t}) + \frac{k}{(\frac{k}{t})} - a_2}{3} = \dfrac{\frac{k}{t} + t - a_2}{3} = x_1 \\ \dfrac{\omega^2(\frac{k}{t}) + \omega\frac{k}{\frac{k}{t}} - a_2}{3} = \dfrac{\omega^2\frac{k}{t} + \omega t - a_2}{3} = x_3 \\ \dfrac{\omega(\frac{k}{t}) + \omega^2\frac{k}{(\frac{k}{t})} - a_2}{3} = \dfrac{\omega\frac{k}{t} + \omega^2 t - a_2}{3} = x_2 \end{cases}$$

We got another rearrangement of the roots! What kind of witchery is this? Well, I don't know about you, but I'm starting to become tired of writing these equations… I claim that each one of the roots of the new polynomial gives a different rearrangement of the roots x_1, x_2 and x_3 when introduced in the formulae of the roots. Thus, *any* root of the new polynomial will give us valid solutions for the original equation, no matter which one we take. Of course, you don't need to trust me, you can check it yourself!

All the rearrangements

$$\begin{cases} t \mapsto (x_1, x_2, x_3) \\ \omega t \mapsto (x_3, x_1, x_2) \\ \omega^2 t \mapsto (x_2, x_3, x_1) \\ \dfrac{k}{t} \mapsto (x_1, x_3, x_2) \\ \omega\dfrac{k}{t} \mapsto (x_2, x_1, x_3) \\ \omega^2\dfrac{k}{t} \mapsto (x_3, x_2, x_1) \end{cases}$$

Yes, we have the cool result that any root of the new polynomial is valid for getting the original solutions of the cubic. But what do you think about these neat rearrangements? Are they only useful for the above conclusion, or can we do more with them? Was this a coincidence, or a more general result? Save some popcorn for later. I warned you.

Fourth degree

Ha! Did you really think I was going to do this again? Nope.

The journey is challenging, but if you're willing to venture further… You know what to do!

Which special value t can we use for an equation of fourth degree?

You see the pattern. We should use the roots of $x^4 = 1$. These are $1, i, -1, -i$, where i is the imaginary number ($i^2 = -1$). Then the special value you should try to use is the familiar:

$$t = x_1 + i \cdot x_2 - x_3 - i \cdot x_4$$

Trust me, it works!

For those who don't find excitement in the too specific formula for a quartic equation, just keep reading…

Second symmetry

Cubic, *u still there*?

In the third degree section we found ourselves solving the general cubic equation thanks to this special value $t = x_1 + \omega x_2 + \omega^2 x_3$. I think we managed to justify why this special one is quite helpful for solving the cubic. I mean this in the sense that, the new equation we have to solve is simple enough, so that finding one of its roots is easier than finding a root of the original equation, even if the new one has sixth degree.

Anyway, a natural question would be: *Are there other special values that allow us to solve the original equation in the same way?* And we're now only interested in the theoretical question. We don't mind if the new equation is hard to solve or not. We really only want to know if there are other special values which encode all information about the roots.

Let's try ourselves! I'm a bit tired of writing monstrous equations though. We'll try with a specific example, of which we could even know the roots in advance. Remember this is just a sort of thought experiment. OK, so our cubic equation will be this:

$$x^3 - x^2 - x - 2 = 0$$

We can quickly check if there is an integer solution by only trying the values $\pm 1, \pm 2$ for x. Maybe you even recall doing this in high school!

Can you see why?

We can rewrite the equation like this:

$$x \cdot (x^2 - x - 1) = 2$$

If x was an integer, we would have $x \cdot \text{other integer} = 2$, so x must be a divisor of 2. The only possible values would then be $\pm 1, \pm 2$.

It turns out that $x = 2$ is a valid solution (you can verify it). That means the cubic polynomial will have a factor $(x - 2)$. Were you told how to perform polynomial long division? If so, go ahead, factor this cubic! If not, don't worry, we have some workarounds. We can try to write the factorization like this:

$$x^3 - x^2 - x - 2 = (x - 2)(x^2 + a_1 x + a_0)$$

Can you find a_1 and a_0? Hint: expand the product and compare coefficients

$$x^3 + (a_1 - 2)x^2 + (a_0 - 2a_1)x - 2a_0$$

Following the coefficients of the original polynomial, we must have $-2a_0 = -2$, so $a_0 = 1$. Likewise, $a_1 - 2 = -1$, so $a_1 = 1$. These also give the expected result for $a_0 - 2a_1 = -1$, so we got the coefficients. The factorization is then:

$$x^3 - x^2 - x - 2 = (x - 2)(x^2 + x + 1) = (x - 2)(x - \omega)(x - \omega^2)$$

We also know the last equality! The polynomial $x^2 + x + 1$ is already familiar to us, and we defined its solutions as ω and ω^2.

So we now know the three solutions of this equation. We're cheating! Who cares? Let's try a different special value! If you recall, we used $t = x_1 - x_2$ for the quadratic equation. Well, let's just try it with the cubic as well, and see what happens.

Suppose we like defining $x_1 = 2$, $x_2 = \omega$, $x_3 = \omega^2$. Then we can have these relations:

$$\begin{cases} t = x_1 - x_2 \\ \dfrac{7}{t} = x_1 - x_3 \\ 1 = x_1 + x_2 + x_3 \end{cases}$$

Where did those come from?

The first one is just the current definition for t. The last one comes from the coefficient relation $x_1 + x_2 + x_3 = -a_2$ we already saw in a previous section. The second one comes from a product:

$$(x_1 - x_2)(x_1 - x_3) = (2 - \omega)(2 - \omega^2) = 4 - 2\omega - 2\omega^2 + \omega^3 = 6 - 2(1 + \omega + \omega^2) + 1 = 7$$

Then we have

$$(x_1 - x_3) = \frac{7}{x_1 - x_2} = \frac{7}{t}$$

Using the above relations, can you obtain all roots in terms of t?

Hint: Use reduction method!

As in other examples, this is a matter of summing all equations, each one multiplied by a certain number to cancel out the roots we don't want. After you find the correct numbers you get:

$$\begin{cases} x_1 = \dfrac{t + \frac{7}{t} + 1}{3} \\ x_2 = \dfrac{-2t + \frac{7}{t} + 1}{3} \\ x_3 = \dfrac{t - 2 \cdot \frac{7}{t} + 1}{3} \end{cases}$$

Yes! It turns out we can use a different special value, and still be able to encode the information of all roots. Now that we have the roots in terms of t, we only need the values of t. You know what to do now, don't you? The new equation from which we get the values of t is that one with products of all possible rearrangements of x_1, x_2 and x_3 in t. Since we're cheating and we already know the roots of the original polynomial, we can save ourselves from building that new polynomial monstrosity and directly write down all its six roots. In case you're a bit lost, I'll tell you the first one, which comes from no rearrangement: $t = x_1 - x_2 = 2 - \omega$.

Which are the rearrangements?

$$\begin{cases} t = x_1 - x_2 = 2 - \omega \\ \dfrac{7}{t} = x_1 - x_3 = 2 - \omega^2 \\ -t = x_2 - x_1 = \omega - 2 \\ -\dfrac{7}{t} = x_3 - x_1 = \omega^2 - 2 \\ -t + \dfrac{7}{t} = x_2 - x_3 = \omega - \omega^2 \\ t - \dfrac{7}{t} = x_3 - x_2 = \omega^2 - \omega \end{cases}$$

The right side of each equation is the actual rearrangement of the roots. I only wrote the left side to show you they can be written in terms of t, and in case these alternative expressions are useful to you to more easily plug them into the root relations to calculate x_1, x_2 and x_3.

Now for the final step! Let's try to get those roots back from the values of t. I said values in plural on purpose. In the general cubic, we somehow got the striking result that all values of t are valid because they just give back a different arrangement of x_1, x_2 and x_3. Here we're interested in seeing if this still holds for a different special value t. Alright, I'll also include this one in a spoiler just in case you're in the mood for some calculations.

Find the roots for each possible value of t

$$\begin{cases} t = 2 - \omega \mapsto (1, \omega, \omega^2) \\ \dfrac{7}{t} = 2 - \omega^2 \mapsto (1, \omega^2, \omega) \\ -t = \omega - 2 \mapsto \left(-\dfrac{4}{3}, \dfrac{2}{3} - \omega, \dfrac{5}{3} + \omega\right) \\ -\dfrac{7}{t} = \omega^2 - 2 \mapsto \left(-\dfrac{4}{3}, \dfrac{2}{3} - \omega^2, \dfrac{5}{3} + \omega^2\right) \\ -t + \dfrac{7}{t} = \omega - \omega^2 \mapsto \left(\dfrac{1}{3} - \dfrac{4}{9}(\omega - \omega^2), \dfrac{1}{3} - \dfrac{13}{9}(\omega - \omega^2), \dfrac{1}{3} + \dfrac{17}{9}(\omega - \omega^2)\right) \\ t - \dfrac{7}{t} = \omega^2 - \omega \mapsto \left(\dfrac{1}{3} + \dfrac{4}{9}(\omega - \omega^2), \dfrac{1}{3} + \dfrac{13}{9}(\omega - \omega^2), \dfrac{1}{3} - \dfrac{17}{9}(\omega - \omega^2)\right) \end{cases}$$

Huh... What is this absolute rubbish? We expected some neat rearrangements of the roots 2, ω, ω^2, and, well, we got that for the first two possible values of t, but we got some ugly results for the others... Unfortunately, we'll have to conclude from this that not all solutions of the new equation can be used to get the solutions of the original one.

But we can certainly use *some* of them. You see, the ones corresponding to $2 - \omega = t$ and $2 - \omega^2 = \frac{7}{t}$ did give the intended solutions. Now the next question should be: *Is there some rule to know exactly which solutions of the new equation do retrieve the solutions for the original one?*

In this case, let's consider a smaller part of the new equation. Let's compute the product of only those two factors including the roots that worked:

$$(x - (2 - \omega))(x - (2 - \omega^2)) = x^2 - (2 - \omega + 2 - \omega^2)x + (2 - \omega)(2 - \omega^2)$$

In fact, this is already a polynomial with known coefficients! The coefficient for x simplifies thanks to $1 + \omega + \omega^2 = 0$, and we already computed the product $(2 - \omega)(2 - \omega^2)$ before. The polynomial is then:

$$x^2 - 3x + 7$$

The whole point of computing a huge product of all rearrangements was that we were sure the resulting polynomial would have known coefficients. We didn't expect that, at least in this case, a smaller polynomial containing t would already have known coefficients. We could already find t from this even easier polynomial, since it's just quadratic. And thanks to our half-failure from before, we also know that the other four roots were completely useless.

Following on that idea, remember when we factored the original polynomial because one of the roots was an integer. The other part would then be $x^2 + x + 1$, and we know from quadratics that $x_2 + x_3 = -1$ and $x_2 \cdot x_3 = 1$. In the First symmetry section we learned that:

Any symmetric polynomial on the roots is a known number.

In this example, because of the root x_1 already being rational, we can use the same reasoning for only the other two roots, so we can be even more specific:

Any symmetric polynomial on the roots x_2 and x_3 is a known number.

This shows that, at least sometimes, if we confirm a polynomial on the roots is unchanged by some of the rearrangements, not necessarily all of them, we can already be sure that its result is a known number.

What about the other way around? If we know a polynomial on the roots is a known number, will it always be unchanged by those specific rearrangements?

> **i** In our specific example, the answer is yes! Why?
>
> Any polynomial on the roots $x_2 = \omega$ and $x_3 = \omega^2$ can actually be written as $a + b\omega$, where a and b are rationals. How? We can just rewrite ω^2 as $-1 - \omega$ because of the relation $1 + \omega + \omega^2 = 0$, and then group all terms based on whether they multiply an ω or not.

> If the polynomial is written like that, then being a known rational value means that b must be an expression that simplifies to zero. This again means that swapping ω and ω^2 in this expression doesn't change the result, since that would only change $a + b\omega$ to $a + b\omega^2$, but we still have b simplifying to zero anyway.

So what have we learned?

- The roots of our original polynomial $x^3 - x^2 - x - 2$ are 2, ω and ω^2.
- Any polynomial expression on these roots satisfies a special property related to rearranging the roots of the expression.
- This property is that the operations of "*not rearranging any root*" and "*swapping ω and ω^2*" together completely determine when a polynomial on the roots simplifies to a known rational number.
- We got these two operations from the rearrangements obtained by plugging the roots of the polynomial with known coefficients $x^2 - 3x + 7$ (which was smaller than expected) into the expressions for x_1, x_2 and x_3 in terms of t.
- From the monstrous polynomial with all rearrangements of roots in t, the polynomial $x^2 - 3x + 7$ is actually the factor with lowest degree that has known rational coefficients and includes $t = 1 - \omega$ as one of its roots. It can't have degree 1 because that would mean $1 - \omega$ is a rational number. Maybe this "polynomial with lowest degree that has t as a root" is a good rule of thumb in general?

But we already learned how to solve cubics... Why should I care about all of this? There's a high chance you're asking yourself that question. I'll clarify shortly. We're on the verge of finding an *invariant* of the original polynomial. This is how mathematicians refer to some special property that is inherent to an object. Something that doesn't change.

But what could change here? Well, in the above example we chose a specific labeling of the roots (we said that $x_1 = 2$, $x_2 = \omega$ and $x_3 = \omega^2$) and we also chose a certain special value $t = x_1 - x_2$. And we now know there might be more than one such value that works. Just imagine being able to create the same object, no matter which choice we wake on the order of the roots or the value of t.

// Start of TV-drama cliffhanger.

Will we succeed? Find out in the next episode!

// End of TV-drama cliffhanger.

Descending into abstractness

TODO

You can't solve it

TODO