Lecture notes of Algebra. Week 6

23. Rational roots of a polynomial with integer coefficients

There is a test which allows, with a finite amount of calculations, to find *all* rational roots of a polynomials with rational coefficients, or to conclude that none exists if none is found. It is a rather specialised test, but it is sometimes useful, and its proof is a good illustration of the use of Arithmetical Lemma B on divisibility.

Note that Arithmetical Lemma B can be applied repeatedly to a product of more than two factors, and hence: if an integer divides a product of several integers, and is coprime (separately) with each of the factors except one, then it divides that factor. For example, if a divides a product bcd, and $(a, b) = 1$ and $(a, c) = 1$, then a must divide d. In fact, because a divides $b(cd)$, and $(a, b) = 1$ we have that a divides cd, and then because $(a, c) = 1$ we have that a divides d.

Before we apply the test we we may reduce to the case of a polynomial with integer coefficients by multiplying our polynomial by a suitable integer (say the least common multiple of all denominators occurring in the coefficients). Then we may divide by any common factor of the coefficients; strictly speaking, this is not required for the validity of the following test, but it may avoid us lots of superfluous calculations.

THEOREM 38 (The Rational Root Test). *Consider a polynomial $f(x) = a_n x^n + \cdots + a_1 x + a_0$ with integer coefficients and $a_n a_0 \neq 0$. If r/s is a rational root of $f(x)$, written as a fraction of integers in lowest terms (that is, with $(r, s) = 1$), then r divides the constant term a_0, and s divides the leading coefficient a_n.*

PROOF. After expanding $s^n \cdot f(r/s) = 0$ we find

$$a_n r^n + a_{n-1} r^{n-1} s + a_{n-2} r^{n-2} s^2 + \cdots + a_2 r^2 s^{n-2} + a_1 r s^{n-1} + a_0 s^n = 0.$$

Because r divides all terms preceding the last one, it must divide the last term as well, that is, $r \mid a_0 s^n$. But because $(r, s) = 1$, Arithmetical Lemma B implies that r divides a_0.

In a similar way, because s divides all terms following the first one, it must divide the first term $a_n r^n$ as well. Because $(r, s) = 1$ it follows that s divides a_n. □

EXAMPLE. Find all the rational roots of the polynomial $f(x) = 2x^3 + 15x^2 + 27x + 10$, and then factorise it over $\mathbb{Q}$. According to the test, if $r/s \in \mathbb{Q}$ is a root of $f(x)$, with $\gcd(r, s) = 1$, then r divides 10 and s divides 2, hence $r \in \{\pm 1, \pm 2, \pm 5, \pm 10\}$ and $s \in \{\pm 1, \pm 2\}$. Consequently, the possibilities for r/s are

$$\pm 1,\ \pm 2,\ \pm 5,\ \pm 10,\ \pm\frac{1}{2},\ \pm\frac{5}{2}.$$

However, because the coefficients of the polynomial are all positive, no positive real number can be a root, and so we only have to test the negative ones. Going through the list from left to right, we find $f(-2) = f(-5) = f(-1/2) = 0$, at which point we can stop because $f(x)$ cannot have more than three roots, and we conclude that

$$f(x) = 2(x+2)(x+5)\big(x+\tfrac{1}{2}\big) = (x+2)(x+5)(2x+1),$$

which is the desired complete factorisation of $f(x)$ over $\mathbb{Q}$. The last expression is actually a complete factorisation over $\mathbb{Z}$. (It is a general fact, known as *Gauss' lemma,* that any factorisation over $\mathbb{Q}$ of a polynomial with integer coefficients leads to a corresponding factorisation over $\mathbb{Z}$ by suitably rearranging some scalar factors.) Alternatively, once we have found the first root -2 we may divide $f(x)$ by $x+2$, and then proceed to factorise the resulting quadratic polynomial.

We can use the Rational Root Test to prove that certain radicals represent irrational numbers, as follows.

EXAMPLE. We prove that $\sqrt{3}$ is irrational. We start with noting that $\sqrt{3}$ is a root of the polynomial $x^2 - 3$. By the Rational Root Test, if r/s is a rational root of $x^2 - 3$, with $r, s \in \mathbb{Z}$ and $(r, s) = 1$, then $r \mid 3$ and $s \mid 1$, and so $r/s \in \{\pm 1, \pm 3\}$. None of those numbers is a root, hence $x^2 - 3$ has no rational root, and so $\sqrt{3}$ is irrational.

EXAMPLE. We prove that $\sqrt[3]{25/3}$ is irrational. Here $\sqrt[3]{25/3}$ is a root of the polynomial $3x^3 - 25$. By the Rational Root Test, if r/s is a rational root of $3x^3 - 25$, with $r, s \in \mathbb{Z}$ and $(r, s) = 1$, then r divides 25 and s divides 3, and so $r/s \in \{\pm 1, \pm 5, \pm 25, \pm 1/3, \pm 5/3, \pm 25/3\}$.

To conclude that $\sqrt[3]{25/3}$ cannot be rational it is enough to check that none of those 12 rational numbers is a root of the polynomial (and so $\sqrt[3]{25/3}$ cannot be equal to any of those rational numbers). However, it may not be necessary to check them all. For example, no negative real number can possibly be a root of $3x^3 - 25$, and so we only need to check the positive ones. We can do even better if we are able to locate the real roots of the polynomial more precisely. For example, noting that $3 \cdot 2^3 - 25 = -1 < 0$, and $3 \cdot 3^3 - 25 = 56 > 0$, and that the function $x \mapsto x^3$ is increasing, any real root of $3x^3 - 25$ must be larger than 2 and less than 3. However, none of the candidates which we have found for rational roots is between 2 and 3, and so we conclude that $3x^2 - 25$ has no rational root, and hence that $\sqrt[3]{25/3}$ is irrational.

24. Some special polynomials: biquadratic polynomials

A *biquadratic polynomial* is a polynomial of degree four where the terms of odd degree are missing, and so has the form $ax^4 + bx^2 + c$, with $a \neq 0$. Because it can be viewed as $a(x^2)^2 + bx^2 + c$, the standard way of finding its roots is setting $y = x^2$, and then solving $ay^2 + by + c = 0$ (by completing the square, or by the explicit formula). If β_1, β_2 are the

roots of this quadratic equation in y, then the roots of the biquadratic polynomial are the solutions of either $x^2 = \beta_1$ or $x^2 = \beta_2$, and so they are the square roots of β_1 and the square roots of β_2.

EXAMPLE. To find the roots of the biquadratic polynomial $2x^4 + x^2 - 6$ we set $x^2 = y$ and then calculate the roots of the resulting quadratic polynomial $2y^2 + y - 6$, finding $y = 3/2$ or $y = -2$. In terms of x this means $x^2 = 3/2$ or $x^2 = -2$, which leads to $x = \pm\sqrt{3/2} = \pm\sqrt{6}/2$ or $x = \pm i\sqrt{2}$. Hence the full factorisation of the polynomial over $\mathbb{C}$ is

$$\begin{aligned} 2x^4 + x^2 - 6 &= 2(x - \sqrt{6}/2)(x + \sqrt{6}/2)(x - i\sqrt{2})(x + i\sqrt{2}) \\ &= (\sqrt{2}\,x - \sqrt{3})(\sqrt{2}\,x + \sqrt{3})(x - i\sqrt{2})(x + i\sqrt{2}), \end{aligned}$$

whichever form we prefer (as the latter has no denominators, but more radicals). Its complete factorisation over $\mathbb{R}$ is

$$2x^4 + x^2 - 6 = 2(x - \sqrt{6}/2)(x + \sqrt{6}/2)(x^2 + 2),$$

and $x^2 + 2$ is irreducible over $\mathbb{R}$ because it has degree two and has no real roots. Finally, its complete factorisation over $\mathbb{Q}$ is

$$2x^4 + x^2 - 6 = (2x^2 - 3)(x^2 + 2),$$

where again the two quadratic factors are irreducible over $\mathbb{Q}$ because they have no rational roots.

25. (Optional) Double radicals

A *double radical* is an expression of the form $\sqrt{a \pm \sqrt{b}}$. (This is a special case of a *nested radical*, see `https://en.wikipedia.org/wiki/Nested_radical`.) Such an expression may occur, for example, when solving biquadratic equations and quartic self-reciprocal equations, or already when solving quadratic equations if the coefficients involve radicals. A double radical can sometimes be expressed as a sum of difference of *simple radicals*, using the identity

(Double Radical Identity) $$\sqrt{a \pm \sqrt{b}} = \sqrt{\frac{a + \sqrt{a^2 - b}}{2}} \pm \sqrt{\frac{a - \sqrt{a^2 - b}}{2}}.$$

Of course the right-hand side is the sum or difference of two simple radicals only when $a^2 - b$ is an exact square, otherwise the identity expresses a double radical as a more complicated expression, a sum of two double radicals.

EXAMPLE. We have

$$\sqrt{5 \pm 2\sqrt{6}} = \sqrt{5 \pm \sqrt{24}} = \sqrt{\frac{5 + \sqrt{5^2 - 24}}{2}} \pm \sqrt{\frac{5 - \sqrt{5^2 - 24}}{2}} = \sqrt{3} \pm \sqrt{2}.$$

In fact, squaring $\sqrt{3} \pm \sqrt{2}$ we get

$$(\sqrt{3} \pm \sqrt{2})^2 = \sqrt{3}^2 \pm 2\sqrt{3}\sqrt{2} + \sqrt{2}^2 = 3 \pm 2\sqrt{6} + 2 = 5 \pm 2\sqrt{6}.$$

EXAMPLE. We have

$$\sqrt{6 \pm 2\sqrt{3}} = \sqrt{6 \pm \sqrt{12}} = \sqrt{\frac{6 + \sqrt{6^2 - 12}}{2}} \pm \sqrt{\frac{5 - \sqrt{6^2 - 12}}{2}} = \sqrt{3 + \sqrt{6}} \pm \sqrt{3 - \sqrt{6}}.$$

This is correct but not very useful.

For the Double Radical Identity to really make sense we should put proper limitations on the values allowed for a and b. Convenient limitations for the present exposition are that a, b are real numbers with $a \geq 0$ and $0 \leq b \leq a^2$. This ensures that all the square roots appearing in this formula (on either side, and both the inner ones and the outer ones) have a nonnegative real argument c. Recall here that $\sqrt{c}$ is assigned a unique meaning when c is a nonnegative real number: $\sqrt{c}$ is the unique *non-negative* real number whose square equals c (and so of the two solutions of $x^2 = c$ one *chooses* to denote by $\sqrt{c}$ the non-negative one, for convenience). Under these conditions on a and b one can simply verify the formula by noting (that all the involved square roots are defined in the real numbers, and) that the right-hand side is nonnegative, by squaring both sides and checking that they give the same result after simplification.

PROOF OF THE DOUBLE RADICAL IDENTITY. Writing $R = \sqrt{a^2 - b}$ for brevity, the square of the right-hand side equals

$$\left(\sqrt{\frac{a+R}{2}} \pm \sqrt{\frac{a-R}{2}}\right) = \frac{a+R}{2} + \frac{a-R}{2} \pm 2\sqrt{\frac{a+R}{2}}\sqrt{\frac{a-R}{2}}$$
$$= a \pm \sqrt{a^2 - R^2} = a \pm \sqrt{b}.$$

Hence the square of the right-hand side of the Double Radical Identity equals the square of the left-hand side of the Double Radical Identity. To conclude a proof of the Double Radical Identity we need to make sure that both sides have the same signs (or are both zero). In fact, our assumptions $a \geq 0$ and $0 \leq b \leq a^2$ imply that all radicals involved are real and non-negative (by convention we choose the non-negative root of a non-negative real number). In particular, the left-hand side is non-negative. Also, of the two radicals at the right-hand side the first is not less than the second (because $a + R \geq a - R$), so their difference is non-negative (in case of the minus sign out of $\pm$). □

This procedure gives a correct and perfectly rigorous *proof* of the identity, but has the drawback that it does not tell us where the identity comes from: we apparently have to recall the identity by heart before we can verify it.

We now show how the identity can be derived from scratch. Hence if we happen to forget it, here is how it can be recovered. As a motivation we may preliminarly note that

if we square a sum $\sqrt{x}+\sqrt{y}$ we get $x+y+2\sqrt{xy}$. Now this latter expression is easily recognisable as the square of $\sqrt{x}+\sqrt{y}$ as long as the terms x and y of the sum are written separately, but not anymore once they are added together. Taking them apart is exactly what our identity aims to achieve. So, given a double radical $\sqrt{a\pm\sqrt{b}}$ (with $0\le b\le a^2$) it is natural to try and express it in the form $\sqrt{a\pm\sqrt{b}}=\sqrt{x}\pm\sqrt{y}$, for some x and y to be determined. Squaring both sides we find $a\pm\sqrt{b}=x+y\pm 2\sqrt{xy}$, at which point we are led to impose

$$\begin{cases} x+y=a \\ 4xy=b. \end{cases}$$

Hence the required x and y are the roots of the quadratic polynomial $z^2-az+b/4$ in the indeterminate z, which of course are $\big(a\pm\sqrt{a^2-b}\big)/2$, leading to the desired identity after choosing $y\le x$.

Example. Let us experiment with the Double Radical Identity on a case where the conditions $a\ge 0$ and $a^2\ge b$ are *not* satisfied. For example, the double radical $\sqrt{2-\sqrt{5}}$ does not represent a real number, because $2-\sqrt{5}<0$. In fact, the condition $a^2\ge b$ is not satisfied here. If we change sign to what is under the square root we get a real radical $\sqrt{-2+\sqrt{5}}$, but the condition $a^2\ge b$ is still not satisfied, and actually $a\ge 0$ is not satisfied either. The Double Radical Identity would give

$$\sqrt{-2+\sqrt{5}}=\sqrt{\frac{-2+\sqrt{(-2)^2-5}}{2}}+\sqrt{\frac{-2-\sqrt{(-2)^2-5}}{2}}=\sqrt{\frac{-2+i}{2}}+\sqrt{\frac{-2-i}{2}},$$

which is not particularly useful as they the simple radicals involve complex numbers. Similarly for the real radical $\sqrt{2+\sqrt{5}}$ the condition $a\ge 0$ is satisfied, but $a\ge 0$ is not, and the Double Radical Identity would give $\sqrt{+2+\sqrt{5}}=\sqrt{1+i/2}+\sqrt{1-i/2}$. The Double Radical Identity may be less useful when complex numbers are involved, but is still correct if properly interpreted. We explore that in the next section.

26. (Optional) Double radicals in the complex case

Now we take a look at the Double Radical Identity more generally, without the above assumptions on a and b. The identity remains valid for a and b any complex numbers, provided we are careful with the meaning of the square roots. In fact, while $\sqrt{a}$ has, by convention, a unique meaning when a is a nonnegative real number, namely, the only positive root of x^2-a, for arbitrary complex $a\neq 0$ the symbol $\sqrt{a}$ actually takes two opposite values, the roots of x^2-a, as it is not possible to make a consistent choice of one root or the other based on algebraic means. In particular, we usually think of $\sqrt{-1}$ as the imaginary unit i, but we could detect no difference in any calculation if we had set

$\sqrt{-1}$ to be $-i$ (as long as we are consistent). [10] When correctly interpreted, the following identity remains valid for any complex numbers a and b:

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

Here any of the six radicals appearing may take two values, which leads to many possible interpretations, only some of which are correct. However, the same radical $\sqrt{a^2-b}$ appears twice on the right-hand side, and whenever that occurs in a formula there is a convention to use the same value for that in both instances (which one being immaterial as it appears with a + sign in one case and a − sign in the other). [11] So in the end the right-hand side generally takes four values, depending on a choice between two values for each of the outside radicals. The left-hand side also generally takes four possible values, depending on a choice between two values for $\sqrt{b}$, and once that choice has been made, on a choice between two values of $\sqrt{a+\sqrt{b}}$. How to match each of the two opposite pairs of values for the right-hand side to each of the two opposite pairs of values for the left-hand side must be made by looking at the arguments of the complex numbers involved, as both possible matches are algebraically equivalent (that is, there is no algebraic way to choose the appropriate match). [12] With this interpretation, the above identity for complex a, b can be simply verified by squaring both sides as we did for the real case.

One application of the double radical identity for complex numbers is to computing square roots of complex numbers. Consider a complex number written in the usual form $a+ib$, where a, b are real numbers. Together with its complex conjugate it can be thought of as $a \pm ib = a + \sqrt{-b^2}$, and the double radical formula gives

$$\begin{aligned}\sqrt{a \pm \sqrt{-b^2}} &= \sqrt{\frac{a+\sqrt{a^2+b^2}}{2}} \pm \sqrt{\frac{a-\sqrt{a^2+b^2}}{2}} \\ &= \sqrt{\frac{\sqrt{a^2+b^2}+a}{2}} \pm i\sqrt{\frac{\sqrt{a^2+b^2}-a}{2}}.\end{aligned}$$

Note that both $\sqrt{a^2+b^2}+a$ and $\sqrt{a^2+b^2}-a$ are nonnegative real numbers, and so both outer radicals in the final expression are square roots of nonnegative real numbers, where we have a convention in place that they usually represent the nonnegative square root. However, because of how we have obtained this expression they should still be considered as complex radicals, each taking two opposite values. Hence the above formula should be

[10] This issue is a little delicate to be discussed further at this point, but it is related with the *conjugation* map $a+ib \mapsto a-ib$ being an *automorphism* of the complex field $\mathbb{C}$.

[11] A similar situation occurs, for example, in Cardano's formulas for the solutions of cubic equations.

[12] In the double radical identity seen at the beginning of the subsection all radicals took nonnegative real values, which amounts to their arguments being 0, rather than the other possible choice π.

interpreted as

$$\pm\sqrt{a \pm \sqrt{-b^2}} = \pm\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}} \pm i\sqrt{\frac{\sqrt{a^2+b^2}-a}{2}},$$

where all the outer radicals are now read as single-valued real radicals. As discussed above, all four $\pm$ signs in the equation are independent (they need not match), and so each side takes four possible values, namely two pairs of opposite values, and the only way to match them correctly is to look at the arguments of the complex numbers involved.

27. Square roots of complex numbers

Solving a quadratic equation with complex coefficients may require taking square roots of complex numbers. Now we look at the problem of computing square roots of complex numbers again, independently of the previous (optional) section on complex double radicals. We will see how computing those square roots in terms of real radicals leads to a biquadratic equation.

Consider a complex number written in the standard form $a + ib$, where $a, b \in \mathbb{R}$, and assume $a + ib \neq 0$ as we may. Of course if the number is written in polar form $a + ib = \rho \cdot (\cos\theta + i \sin\theta)$, where $\rho = \sqrt{a^2+b^2} > 0$ is its modulus and $0 \leq \theta < 2\pi$ is its argument, then we have general formulas for all the nth roots of $a + ib$, namely,

$$\rho^{1/n} \cdot \left(\cos\left(\frac{\theta+2k\pi}{n}\right) + i\sin\left(\frac{\theta+2k\pi}{n}\right)\right), \qquad \text{for } k = 0, \ldots, n-1$$

(or $-n/2 < k \leq n/2$ if we prefer). However, we would like to find the square roots of $a + ib$ algebraically, without using trigonometric functions. More precisely, $a + ib \neq 0$ will have two distinct square roots in the complex numbers, say $x + iy$ and $-x - iy$, with $x, y \in \mathbb{R}$. We would like to compute the real numbers x and y from a and b in an algebraic way, using the four basic operations and possibly radicals.

We have $(x + iy)^2 = a + ib$, that is,

$$x^2 - y^2 + 2ixy = a + ib.$$

Because x, y, a, b are real, this equation is equivalent to the system of equations [13]

$$\begin{cases} x^2 - y^2 = a \\ 2xy = b \end{cases}$$

[13]Note that this is a system of degree $2 \cdot 2 = 4$, and in general we could expect it to have four solutions in the complex numbers. For example, in the special case where $b = 0$ one finds that either $x = 0$ and $y^2 = -a$, or $y = 0$ and $x^2 = a$. However, if $a \neq 0$ then depending on the sign of a exactly one of these two cases will lead to real solutions for both x and y, which are the only acceptable ones for our problem, and produce the two square roots of a in each case.

If we assume $b \neq 0$, which is reasonable because otherwise $a+ib$ is a real number and its square roots are easy to find, then neither x nor y can be zero, and so from the second equation we find $y = b/(2x)$. Substituting this into the first equation we get

$$x^2 - \Big(\frac{b}{2x}\Big)^2 = a,$$

that is,

$$4x^4 - 4ax^2 - b^2 = 0.$$

This is a biquadratic equation, and solving it (without even performing the usual substitution and back, now that we know how it works) we find

$$x^2 = \frac{2a \pm \sqrt{(2a)^2 + 4b^2}}{4} = \frac{a \pm \sqrt{a^2+b^2}}{2}.$$

Because $a^2 < a^2 + b^2$, the right-hand side will only be nonnegative (and actually positive) when we take the + sign in front of the radical, and because our x needs to be real only that case leads to acceptable solutions. Hence $x^2 = \big(a + \sqrt{a^2+b^2}\big)/2$ and, consequently, $y^2 = x^2 - a = \big(-a + \sqrt{a^2+b^2}\big)/2$. In conclusion, the two square roots $\pm(x+iy)$ of $a+ib$ are obtained by taking

$$x = \pm\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}}, \quad \text{and} \quad y = \pm\sqrt{\frac{\sqrt{a^2+b^2}-a}{2}},$$

with matching signs in front of the two main radicals if $b > 0$, and with opposite signs if $b < 0$, as one recognises from the second equation of the system. This can be summarized in the formula

$$\pm\sqrt{a \pm ib} = \pm\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}} \pm i\sqrt{\frac{\sqrt{a^2+b^2}-a}{2}},$$

where the signs have to be appropriately matched as discussed.

Note that there is no need to memorise such complicated formulas: to compute the square roots of a given complex number, just apply the procedure described (see the example below). Nevertheless, let us play with those formulas a bit.

If we write the nonzero complex number $a+ib$ in polar form $a+ib = \rho\cdot(\cos\theta + i\sin\theta)$, where $\rho = \sqrt{a^2+b^2}$ is its modulus and $0 \leq \theta < 2\pi$ is its argument, we can read off the above formulas the halving formulas for sin and cos. In fact, as discussed more generally for nth roots at the beginning of this section, the square roots of $a+ib = \rho(\cos\theta + i\sin\theta)$ will be $\pm\sqrt{\rho}\cdot\big(\cos(\theta/2) + i\sin(\theta/2)\big)$, and so our formulas for the square roots of $a+ib$ imply

$$\cos\Big(\frac{\theta}{2}\Big) = \pm\sqrt{\frac{1+\cos\theta}{2}}, \quad \text{and} \quad \sin\Big(\frac{\theta}{2}\Big) = \pm\sqrt{\frac{1-\cos\theta}{2}},$$

where the signs have to be taken appropriately. Of course these angle halving formulas can also be obtained more directly by inverting the angle duplication formulas

$$\cos\theta = 2\cos^2\Big(\frac{\theta}{2}\Big) - 1 = 1 - 2\sin^2\Big(\frac{\theta}{2}\Big).$$

EXAMPLE. Compute the square roots of the complex number $-3+4i$, expressing them using only square roots of real numbers (that is, expressing their real and complex part using only algebraic operations on real numbers).

We look for real numbers x and y such that $(x+iy)^2 = -3+4i$, that is,

$$x^2 - y^2 + 2ixy = -3 + 4i.$$

Because x, y are real, this equation is equivalent to the system of equations

$$\begin{cases} x^2 - y^2 = -3 \\ 2xy = 4 \end{cases}$$

From the second equation we find $y = 2/x$. Substituting this into the first equation we get $x^2 - (2/x)^2 = -3$, that is, $x^4 + 3x^2 - 4 = 0$, or $(x^2-1)(x^2+4) = 0$. This has roots ± 1 and $\pm 2i$, but because x must be real for our problem we may only take $x = \pm 1$, and correspondingly $y = \pm 2$. In conclusion, the square roots of $-3+4i$ are $1+2i$ and $-1-2i$.

If we had forgotten that x and y are real, and so we accepted $x = \pm 2i$, and correspondingly $y = \mp i$, the argument would not be quite correct but we would still get the correct square roots, as $2i + i(-i) = 1 + 2i$ and its opposite.

REMARK 39. (Optional) It is also possible to compute the square roots of $-3+4i$ by writing it as $-3 + \sqrt{-16}$ and applying the Double Radical Identity:

$$\sqrt{-3+4i} = \sqrt{-3+\sqrt{-16}} = \sqrt{\frac{3+\sqrt{3^2+16}}{2}} + \sqrt{\frac{3-\sqrt{3^2+16}}{2}} = \sqrt{1} + \sqrt{-4}.$$

However, as explained in the previous section using the Double Radical Identity leaves sign ambiguities when working with complex numbers, namely, $\sqrt{1}$ can mean 1 or -1, and $\sqrt{-4}$ can mean $2i$ or -21: we now must decide how to correctly match the signs by looking at arguments of the complex numbers involved (or guessing one possible match and square the result to check if it was the correct choice). In essence, the ambiguity which we have is between the square roots of $-3+4i$ and those of $-3-4i$, which are their conjugates.

28. Some special polynomials: self-reciprocal polynomials

The reason why biquadratic polynomials are much easier to factorise than arbitrary quartic polynomials is that they satisfy a special symmetry: they satisfy $f(-x) = f(x)$ (this condition is what, more generally, characterises *even* functions). A similar condition, but involving reciprocals instead of opposites, defines *self-reciprocal* polynomials.

A polynomial $f(x)$ of positive degree n is called *self-reciprocal* if $x^n \cdot f(1/x) = f(x)$. If $f(x) = a_n x^n + \cdots + a_1 x + a_0$ then *its reciprocal polynomial* is

$$x^n \cdot f\left(\frac{1}{x}\right) = a_n + a_{n-1}x + a_{n-2}x^2 + \cdots + a_1 x^{n-1} + a_0 x^n,$$

and so $x^n \cdot f(1/x)$ is a polynomial of degree n, whose coefficients are the coefficients of $f(x)$ read in the opposite order. Hence a polynomial $f(x)$ is self-reciprocal if it equals its reciprocal polynomial, and that means that its sequence of coefficients reads the same backwards as forwards: $a_n = a_0$, $a_{n-1} = a_1$, etc.

The definition of self-reciprocal shows that all roots α are nonzero (because $a_0 = a_n \neq 0$), and that whenever α is a root, its *reciprocal* $1/\alpha$ is a root as well. (This is the reason of the name *self-reciprocal*.) If $f(x)$ is self-reciprocal of odd degree, then one sees at once that -1 is a root, hence $f(x)$ is divisible by $x + 1$, and one can show that the quotient is also self-reciprocal, but of course of even degree. Hence it is enough to see how to deal with a self-reciprocal polynomial of even degree n. We could start with the case of quadratic polynomials, but because we already know how to find their roots in general we pass directly to the case of degree four.

A quartic self-reciprocal polynomial will have the form $ax^4+bx^3+cx^2+bx+a$. The idea for finding its roots, that is, for solving the corresponding equations, is to suitably match x and $1/x$, by taking their sum $x+1/x$. We may start with dividing by x^2 the corresponding equation (as we know that 0 cannot be a root), obtaining $ax^2 + bx + c + b/x + a/x^2 = 0$, that is,

$$a\left(x^2 + \frac{1}{x^2}\right) + b\left(x + \frac{1}{x}\right) + c = 0.$$

Now note that we can express $x^2 + 1/x^2$ in terms of $x + 1/x$,

$$x^2 + \frac{1}{x^2} = \left(x + \frac{1}{x}\right)^2 - 2,$$

and so we can write our equation in the equivalent form

$$a\left(x + \frac{1}{x}\right)^2 + b\left(x + \frac{1}{x}\right) + c - 2a = 0.$$

Now we may set $y = x + 1/x$, and solve the quadratic equation $ay^2 + by + c - 2a = 0$. It may not have any solutions in F, and in that case our quartic self-reciprocal equations cannot have any solutions in F either (because if $\alpha \in F$ were a solution, then $\beta = \alpha+1/\alpha$ would be a solution of the quadratic equation). If it does have solutions, say β_1 and β_2 (which may be equal), then we may try and solve $x + 1/x = \beta_1$ and $x + 1/x = \beta_2$. Each of these may or may not have solutions in F, giving at most four solutions of our quartic equation. [14]

[14] A self-reciprocal equation of degree six may be dealt with in a similar way, and solving it reduces to solving a cubic equation. In this case we would also have to deal with an expression $x^3 + 1/x^3$, which

EXAMPLE. We use the above method to find all complex roots of the self-reciprocal polynomial $6x^4 + 5x^3 - 38x^2 + 5x + 6$. After equating the polynomial to zero we divide by x^2, rearrange the terms and get

$$6\left(x^2 + \frac{1}{x^2}\right) + 5\left(x + \frac{1}{x}\right) - 38 = 0.$$

Using $(x + 1/x)^2 = x^2 + 2 + 1/x^2$ the equation becomes

$$6\left(x + \frac{1}{x}\right)^2 + 5\left(x + \frac{1}{x}\right) - 50 = 0,$$

which reads $6y^2 + 5y - 50 = 0$ after setting $x + 1/x = y$. This quadratic equation has roots $5/2$ and $-10/3$, and by substituting $y = x + 1/x$ again we find the two equations

$$x + \frac{1}{x} = \frac{5}{2}, \quad \text{and} \quad x + \frac{1}{x} = -\frac{10}{3}.$$

After multiplying by $2x$ or $3x$ they become

$$2x^2 - 5x + 2 = 0, \quad \text{and} \quad 3x^2 + 10x + 3 = 0,$$

whose solutions are 2, $1/2$, and -3, $-1/3$, respectively. Hence these four numbers are the roots of the original polynomial. Because they are all four real, the polynomial factorises into a product of four linear factors already over $\mathbb{R}$, namely,

$$\begin{aligned} 6x^4 + 5x^3 - 38x^2 + 5x + 6 &= 6(x - 2)(x - 1/2)(x + 3)(x + 1/3) \\ &= (x - 2)(2x - 1)(x + 3)(3x + 1). \end{aligned}$$

Because the roots have turned out to be all rational in this example, we could of course also have found them by the Rational Root Test. But we have used a general method for quartic self-reciprocal polynomials, which would work even if there were no rational roots.

29. (Optional) An application: exact trig values of the angle $2\pi/5$

We will compute the exact values of the trigonometric functions (sin and cos, from which the others follows easily) of multiples of the angle $\pi/5$, that is, $36°$. These can be found through geometric arguments. As a general rule, formulas for trigonometric functions are best dealt with by working with the exponential form of complex numbers, and so we set

$$\omega := \exp(2\pi\, i/5) = \cos(2\pi/5) + i\, \sin(2\pi/5).$$

---

can be done by noting that

$$\left(x + \frac{1}{x}\right)^3 = x^3 + 3x + \frac{3}{x} + \frac{1}{x^3} = \left(x^3 + \frac{1}{x^3}\right) + 3\left(x + \frac{1}{x}\right),$$

whence $x^3 + 1/x^3 = (x + 1/x)^3 - 3(x + 1/x) = y^3 - 3y$, etc. There is a formula for solving cubic equations, but we will not see that, and so we stop here with this observation.

Now $\omega^5 = \exp(2\pi\, i/5)^5 = \exp(2\pi\, i) = 1$, and so ω is a fifth root of unity, and hence a root of the polynomial $x^5 - 1$. Because $x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1)$ and $\omega \neq 1$, we deduce that ω is a root of $x^4 + x^3 + x^2 + x + 1$. Each of ω^2, $\omega^3 = \omega^{-2}$, and $\omega^4 = \omega^{-1}$ is also a fifth root of unity different from 1, hence these numbers are also roots of $x^4 + x^3 + x^2 + x + 1$. Being all distinct, they must be all complex roots of this polynomial, and so

$$x^4 + x^3 + x^2 + x + 1 = (x-\omega)(x-\omega^2)(x-\omega^{-2})(x-\omega^{-1}).$$

Because this polynomial is self-reciprocal polynomial, we have learnt how to compute its roots. After equating the polynomial to zero we divide by x^2, rearrange the terms and get

$$x^2 + \frac{1}{x^2} + x + \frac{1}{x} + 1 = 0.$$

Now because $(x+1/x)^2 = x^2+2+1/x^2$ we can transform the equation into the equivalent equation

$$\left(x + \frac{1}{x}\right)^2 + \left(x + \frac{1}{x}\right) - 1 = 0.$$

After setting $x + 1/x = y$ we solve the resulting equation $y^2 + y - 1 = 0$, and find

$$y = \frac{-1 \pm \sqrt{5}}{2}.$$

Now we substitute $y = x + 1/x$ and solve the two equations

$$x + \frac{1}{x} = \frac{-1 \pm \sqrt{5}}{2},$$

which after multiplication by $2x$ become

$$2x^2 - (-1 \pm \sqrt{5})x + 2 = 0.$$

The equation $2x^2 - (-1 + \sqrt{5})x + 2 = 0$ has solutions

$$\frac{\sqrt{5} - 1 \pm \sqrt{(\sqrt{5}-1)^2 - 16}}{4} = \frac{\sqrt{5} - 1 \pm \sqrt{-10 - 2\sqrt{5}}}{4} = \frac{\sqrt{5}-1}{4} \pm i\frac{\sqrt{10+2\sqrt{5}}}{4},$$

and so we conclude that

$$\cos(2\pi/5) = \frac{\sqrt{5}-1}{4}, \quad \text{and} \quad \sin(2\pi/5) = \frac{\sqrt{10+2\sqrt{5}}}{4}.$$

Of course $\sin(2\pi/5)$ could also be computed from $\cos(2\pi/5)$ using the relation $\cos^2\alpha + \sin^2\alpha = 1$. The double radical $\sqrt{10+2\sqrt{5}}$ here cannot be simplified, as $10^2 - (2\sqrt{5})^2 = 80$ is not a perfect square.

Similarly, by solving $2x^2 - (-1 + \sqrt{5})x + 2 = 0$ we find that

$$\cos(4\pi/5) = \frac{-1-\sqrt{5}}{4}, \quad \text{and} \quad \sin(4\pi/5) = \frac{\sqrt{10-2\sqrt{5}}}{4}.$$

From this we obtain

$$\cos(\pi/5) = \frac{1+\sqrt{5}}{4}, \quad \text{and} \quad \sin(\pi/5) = \frac{\sqrt{10-2\sqrt{5}}}{4}.$$

Hence each side of a regular pentagon of radius 1 has length $2\sin(\pi/5) = \big(\sqrt{10-2\sqrt{5}}\big)/2$.

30. Symmetric functions of the roots of quadratic polynomials

In this and the next section we study an important relation between the coefficients of a polynomial and its roots. We start with discussing the case of quadratic polynomials. If the quadratic polynomial ax^2+bx+c (hence with $a \neq 0$) has at least one root in the field F, then we have seen earlier on that it factorises as the product of two polynomials of degree one. By collecting suitable scalar factors those two factors can be taken to have the form $x-\alpha$ and $x-\beta$, and so we have

$$ax^2+bx+c = a(x-\alpha)(x-\beta) = a\big(x^2-(\alpha+\beta)x+\alpha\beta\big).$$

Hence $-b/a = \alpha+\beta$ (the sum of the roots), and $c/a = \alpha\beta$ (the product of the roots). This can be used to guess the roots of a quadratic polynomial in simple cases, but also, more usefully, to use a quadratic equation for solving systems of two equations as in the following example.

Example. Solving the system

$$\begin{cases} x+y = s \\ \quad xy = p \end{cases}$$

in the unknowns x and y, means finding all pairs of numbers x, y whose sum equals s and whose product equals p. One could express y in terms of x using the first equation, hence $y = s-x$, substitute for y in the second equation, solve the corresponding quadratic equation in x obtained, etc., but it is more efficient to exploit the symmetry of the system and to proceed as follows.

The desired x and y will be the roots of the polynomial $(z-x)(z-y)$ in the indeterminate z, which can be written as $z^2-(x+y)z+xy$, and hence equals z^2-sz+p. Therefore, its complex roots are given by the formula $\big(s \pm \sqrt{s^2-4p}\big)/2$. One of the roots will be x, and the other will be y. Of course if the roots are distinct then there are two ways to match x and y to the two roots, and this gives us two solutions (x,y) for our symmetric system. The roots will be equal exactly when $s^2 = 4p$, and in that case the system has a 'double' solution $(x,y) = (s/2, s/2)$.

The polynomials $x+y$ and xy are examples of *symmetric polynomials* in the indeterminates x and y. More generally, a polynomial $f(x,y)$ in x and y is a *symmetric polynomial* if it is unchanged by interchanging the indeterminates x and y, which means

$f(y,x) = f(x,y)$. For example, $x^3 + 2x^2y + 2xy^2 + y^3 + 5xy - 4x - 4y + 7$ is a symmetric polynomial. The special polynomials $x + y$ and xy are called the *elementary symmetric polynomials*.

THEOREM 40. *Every symmetric polynomial $f(x,y)$ (with coefficients in any field F) can be expressed as a polynomial (also with coefficients in F) in the elementary symmetric polynomials $x + y$ and xy.*

This means that if $f(x,y)$ is a symmetric polynomial in x and y (hence with the condition $f(y,x) = f(x,y)$), then $f(x,y) = g(x+y, xy)$, for some polynomial $g(s,p)$ in two indeterminates s and p. More is true: if $f(x,y)$ has integer coefficients, then $g(s,p)$ has integer coefficients as well. We will not prove these statements in general, but just illustrate them with a couple of special cases which can be guessed at once:

$$x^2 + y^2 = (x+y)^2 - 2xy, \qquad x^3 + y^3 = (x+y)^3 - 3xy(x+y).$$

The next case takes a bit more work,

$$\begin{aligned} x^4 + y^4 &= (x+y)^4 - xy(4x^2 + 6xy + 4y^2) \\ &= (x+y)^4 - xy\big(4(x+y)^2 - 2xy\big) \\ &= (x+y)^4 - 4xy(x+y)^2 + 2(xy)^2. \end{aligned}$$

Hence, in the notation of Theorem 40, the symmetric polynomial $f(x,y) = x^4 + y^4$ can be written as $f(x,y) = g(x+y, xy)$, where $g(s,p) = s^4 - 4s^2p + 2p^2$.

More generally, according to Theorem 40 sums $x^n + y^n$ of higher powers can also be expressed as polynomials in $x+y$ and xy (with integer coefficients): one need to do some work as above and use the analogous expressions for smaller values of n. A different and more efficient way of achieving this same goal is described in a later section.

EXAMPLE. The symmetric polynomial $f(x,y) = x^3+2x^2y+2xy^2+y^3+5xy-4x-4y+7$ can be written as

$$f(x,y) = (x+y)^3 - xy(x+y) + 5xy - 4(x+y) + 7 = g(x+y, xy),$$

where $g(s,p) = s^3 - sp - 4s + 5p + 7$.

31. (Optional) The symmetries involved in biquadratic and self-reciprocal polynomials

The methods which we used to solve biquadratic and quartic self-reciprocal equations can be justified in terms of symmetric polynomials.

Indeed, the fact that a biquadratic polynomial $f(x)$ is unchanged when replacing x with $-x$ (that is, $f(-x) = f(x)$, which more generally characterises the *even* polynomials, as opposed to the *odd* polynomials, satisfying $f(-x) = -f(x)$), suggests expressing it in

terms of the 'elementary symmetric polynomials' in x and $-x$, which are $x+(-x)=0$ and $x\cdot(-x)=-x^2$. (We have slightly abused language here, as x and $-x$ are not independent indeterminates.) This is, in fact, what we did, thinking of a biquadratic polynomial as a polynomial in x^2 (which makes no practical difference from using $-x^2$ instead).

Similarly, a self-reciprocal polynomial $f(x)$ of degree n satisfies $x^n \cdot f(1/x) = f(x)$, hence it is not quite left unchanged by replacing x with $1/x$, but almost. In fact, our first step in finding the roots of $f(x)$ (and then factorising it), for even n, was dividing $f(x)$ by $x^{n/2}$. Now the rational expression (that is, quotient of two polynomials) $g(x) = f(x)/x^{n/2}$ satisfies $g(1/x) = g(x)$, because

$$g(1/x) = \frac{f(1/x)}{(1/x)^{n/2}} = x^{n/2} \cdot f(1/x) = f(x)/x^{n/2} = g(x).$$

Hence $g(x)$ is left unchanged by replacing x with $1/x$, and as a consequence of Theorem 40 (which extends to quotients of polynomials) it can be expressed in terms of the 'elementary symmetric polynomials' in x and $1/x$, which are $x+1/x$ and $x\cdot 1/x = 1$. This is precisely what we did when finding the roots of self-reciprocal polynomials: we expressed x^2+1/x^2 as a polynomial in $x+1/x$ (and we would do the same with each x^k+1/x^k if we wished to deal with self-reciprocal polynomials of even degree higher than 4).