Solutions to Solutions

Sample Answers to the Exercises

Alex Elzenaar

January 11, 2019

Contents

1 Introduction

This booklet consists of worked solutions to all exercises in *Solutions*. Please check the date on the cover of both texts and ensure it matches. They are designed to be read in conjunction with the main text.

Note that these solutions are most definitely not the only possible solutions! They are only indicative of what a solution to the problem could look like.

Notation

We use standard set notation: $\mathbb{N}$ stands for the natural numbers (excluding zero), $\mathbb{Z}$ for the integers, $\mathbb{Q}$ for the rationals, $\mathbb{R}$ for the reals, and $\mathbb{C}$ for the complex numbers. The symbol $\in$ is the set inclusion symbol, and $\subseteq$ is the subset symbol.

Sigma notation is also occasionally used: the notation

$$\sum_{n=0}^{N} f(n)$$

means the sum $f(0) + f(1) + \cdots + f(N)$. If $\sum$ is replaced by $\prod$, the intended meaning is $f(0)f(1)\cdots f(N)$.

Definitions

I apologise for using the following definitions occasionally without explanation:

- **Group:** A number system with one operation that is invertible, such that there is an identity. Example: the integers together with addition (the identity being the number 1).
- **Ring:** A number system in which we can carry out the operations of addition, subtraction, and multiplication. Example: the integers.
- **Field:** A number system in which we can carry out the operations of addition, subtraction, multiplication, and division. Example: the real numbers.

Induction

Axiom (The Axiom of Induction)**.** *Let S be a set. Then if $1 \in S$, and if $n \in S$ then $n + 1 \in S$, we must have $\mathbb{N} \subseteq S$.*

In other words, if a set contains 1, and it contains $n + 1$ whenever it contains n, then it contains all natural numbers. This is often an easy way to prove that a statement holds for all natural numbers (and, in fact, integers). We occasionally

make use of it here,[1] although we usually give an alternative proof without using induction. If one is interested, this is a standard proof technique and is thus easily Googleable.

I give the following standard example of induction:

Theorem. *The sum of the first n natural numbers is $\frac{n(n+1)}{2}$.*

Proof. Consider the case $n = 1$. Then the formula gives us $\frac{1(1+1)}{2} = 1$, which is correct.

Now, suppose the formula gives us the correct result for n. Then:

$$\frac{(n+1)(n+2)}{2} = \frac{n(n+1) + 2(n+1)}{2} = \frac{n(n+1)}{2} + (n+1)$$

so the formula gives us the correct result for $n + 1$.

Hence, by the principle of induction, the set of all natural numbers is a subset of the set of all n for which the formula holds true; so the formula works for all $n \in \mathbb{N}$. □

Recommended Further Reading

On algebra, I would recommend Charles C. Pinter's *A Book of Abstract Algebra* for the beginner (although I much prefer Michael Artin's *Algebra*, it is not as accessible for a high-school audience). On proof techniques and basic concepts of set theory and number theory, I recommend Kevin Houston's *How to Think Like a Mathematician*.

Of course, the books in the bibliography are recommended as well — but most of them require more sophisticated mathematical knowledge to be accessible and so the reader is kindly advised not to touch (for example) the textbooks on Galois Theory without consulting a professional! Ian Stewart's *Taming the Infinite* is recommended for the casual audience.

[1] Like real adults, we often leave the actual induction proof to the reader (in general it is obvious what the base and inductive steps look like.)

2 Quadratic Equations

1. **Find an example of a quadratic equation with the solutions:**
   - **a.** $x = 7$ **and** $x = 4$
   - **b.** $x = 7$ **and** $x = -4$
   - **c.** $x = -7$ **and** $x = -4$
   - **d. Only** $x = 3$

$$0 = (x-7)(x-4) = x^2 - 11x + 28,$$
$$0 = (x-7)(x+4) = x^2 - 3x - 28,$$
$$0 = (x+7)(x+4) = x^2 + 11x + 28, \text{ and}$$
$$0 = (x-3)^2 = x^2 - 6x + 9.$$

All constant multiples of these will also have the same roots.

2. **Use the discriminant Δ_2 of the following quadratics to find the number of distinct real roots each one has, without explicitly calulating those roots.**
   - **a.** $3x^2 + 6x + 3 = 0$
   - **b.** $x^2 + 10x + 1 = 0$
   - **c.** $x^2 + 5x + 9 = 0$
   - **d.** $x^2 - \frac{14x}{3} + \frac{49}{9} = 0$

Recall that the quadratic discriminant $\Delta_2 = b^2 - 4ac$ will "discriminate" between the three possibilities (two real roots, one repeated real root, or no real root).

For (a), $\Delta_2 = 6^2 - 4 \cdot 4 \cdot 9 = 0$, so the first equation has one repeated real root. For (b), $\Delta_2 = 10^2 - 4 > 0$, so the second equation has two distinct real roots. For (c), $\Delta_2 = 5^2 - 4 \cdot 9 < 0$, so the third equation has no real roots.

We multiply the fourth equation in (d) by 9 to clear the fractions and simplify our calculations. We then have $\Delta_2 = (-42)^2 - 4 \cdot 9 \cdot 49 = 0$, so it has one repeated real root.

3. **Use the *difference of two squares* identity $x^2 - b^2 = (x - b)(x + b)$ to factorise and hence solve the following equations for x:**

   a. $x^2 - 9 = 0$

   b. $x^2 - 7 = 0$

   c. $x^2 - 15 = 1$

   d. $x^2 - 2ab = a^2 + b^2$

$x^2 - 9 = (x + 3)(x - 3)$, so $x = \pm 3$;
$x^2 - 7 = (x + \sqrt{7})x - \sqrt{7}$, so $x = \pm\sqrt{7}$;
$x^2 - 16 = (x + 4)(x - 4)$, so $x = \pm 4$; and
$x^2 - a^2 - 2ab - b^2 = x^2 - (a+b)^2 = (x + a + b)(x - a - b)$, so $x = \pm(a + b)$.

4. **Prove that $ax^2 + bx + c = Ax^2 + Bx + C$ implies that $a = A$, $b = B$, and $c = C$. This result allows us to *match coefficients*, an important tool which we can use to reason about the symmetries of polynomials.**

Both polynomials agree everywhere, so in particular they agree at $x = 0$. By direct substitution, we have therefore got that $c = C$. Hence $ax^2 + bx = Ax^2 + Bx$. These polynomials agree at $x = 1$, so $a + b = A + B$; similarly, these polynomials agree at $x = -1$ and so $a - b = A - B$. Adding, $2a = 2A \implies a = A$; by subtraction, $2b = 2B \implies b = B$.

5. **Show that if α and β are the two solutions of $x^2 + bx + c = 0$, then we have $-b = \alpha + \beta$ and $c = \alpha\beta$.**

We simply match coefficients: $x^2 + bx + c = (x - \alpha)(x - \beta) = x^2 - (\alpha + \beta)x + \alpha\beta$.

6. **Factorise $x^2 - 3x - 40$ by inspecting the coefficients and using the identity that a quadratic with the two solutions a and b is given by $(x - a)(x - b) = x^2 - (a + b)x + ab$ (note the change of sign in the factors).**

We have that $ab = -40$ and $a + b = 3$. We know that $5 \times 8 = 40$ - and $5 - 8 = -3$. Hence $b = 8$ and $a = -5$.

7. **For which values of k does the graph of the quadratic function $y = x^2 + (3k - 1)x + (2k + 10)$ not touch the x-axis?**

We need $\Delta_2 < 0$. $\Delta_2 = (3k - 1)^2 - 4(2k + 10) = 9k^2 - 14k - 39$, and using the quadratic formula we have the two solutions for this as $k = 3$ and $k = -\frac{13}{9}$. Since our polynomial for Δ_2 is concave up (positive coefficent on the x^2 term), $\Delta_2 < 0$ for $-\frac{19}{3} < k < 3$.

8. **Do the zeroes of a function uniquely identify that function? Why/why not?**

It is easily seen that given n roots $x_0, x_1, ..., x_n$, one polynomial with those roots will be $y = (x - x_0)(x - x_1)...(x - x_n)$. However, we also see that $y = K(x - x_0)(x - x_1)...(x - x_n)$ (where $K \neq 0$ is an arbitrary constant) has exactly those roots as well (when $y = 0$, K can be divided out). So the zeroes of a function do not uniquely identify the function.

9. Solve the following equations in the real numbers: a. $w^4+30w^2+29=0$, and b. $3e^{2x}-24e^x-8=0$.

The first equation is a quadratic in w^2, so $w^2=-1$ and $w^2=-29$ (by inspection or by the quadratic formula); hence this equation has no solutions in the real numbers.

$e^{2x}=(e^x)^2$ so the second formula is a quadratic in e^x. Solving this with the quadratic formula, we obtain $e^x=\frac{12\pm 2\sqrt{42}}{3}$. Since we cannot yet take the logarithm of a negative number, the only solution is $x=\ln\frac{12+m2\sqrt{42}}{3}$.

10. Write each of the following in the form $(x+p)^2=q$ for some p and q, and hence find their solutions by completing the square.

a. $x^2-3x+4=0$

b. $x^2-6x-10=0$

c. $x^2-26x+47=0$

d. $6x^2-12x+13=0$

e. $-2x^2+3x+5=0$

$$x^2-3x+4=0 \implies (x-\tfrac{3}{2})^2-\tfrac{7}{4} \implies x=\pm\sqrt{\tfrac{7}{4}}+\tfrac{3}{2}$$
$$x^2-6x-10=0 \implies (x-3)^2=19 \implies x=\pm\sqrt{19}+3$$
$$x^2-26x+47=0 \implies (x-13)^2=122 \implies x=\pm\sqrt{122}+13$$
$$6x^2-12x+13=0 \implies x^2-3x+\frac{13}{6}=0 \implies (x-\tfrac{3}{2})^2=\tfrac{1}{12} \implies x=\pm\sqrt{\tfrac{1}{12}}+\tfrac{3}{2}$$
$$-2x^2+3x+5=0 \implies x^2-\tfrac{3}{2}x-\tfrac{5}{2}=0 \implies (x-\tfrac{3}{4})^2=\tfrac{49}{16} \implies x=\tfrac{3}{4}\pm\tfrac{7}{4}$$

11. Suppose that $x^2+bx+c=0$ has two roots, α and β.

a. Show that $\alpha^2+\beta^2=b^2-2c$.

b. Show that $\Delta_2\left[x^2+bx+c\right]=(\alpha-\beta)^2$.

(a) We have that $x^2+bx+c=(x-\alpha)(x-\beta)=x^2-(\alpha+\beta)x+\alpha\beta$, so $\alpha+\beta=-b$. Hence $b^2=(\alpha+\beta)^2=\alpha^2+\beta^2+2\alpha\beta$ and so (since $\alpha\beta=c$) we have $\alpha^2+\beta^2=b^2-2c$.

(b) We have $(\alpha-\beta)^2=\alpha^2+\beta^2-2\alpha\beta=b^2-2c-2c=b^2-4c=\Delta_2\left[x^2+bx+c\right]$ as required.

12. Flesh out the following alternative proof of the quadratic formula from [6]. Let α and β be the two roots of the equation $x^2+bx+c=0$.

a. Then $x = \frac{1}{2}\left((\alpha+\beta)+(\alpha-\beta)\right) = \frac{1}{2}\left((\alpha+\beta)+\sqrt{(\alpha-\beta)^2}\right)$.

b. Note that $\sqrt{(\alpha-\beta)^2}$ has two values and show that taking the negative value still gives a root.

c. But $\alpha+\beta=-b$ and $(\alpha-\beta)^2=b^2-4c$.

d. So $x = \frac{1}{2}\left(-b \pm \sqrt{b^2-4c}\right)$, which is the quadratic formula.

(a) We have $\frac{1}{2}\left((\alpha+\beta)+(\alpha-\beta)\right) = \alpha$, which is one value of x. Likewise, $\frac{1}{2}\left((\alpha+\beta)+\sqrt{(\alpha-\beta)^2}\right) = \alpha$ if we take the positive square root.

(b) If we take the negative root, we find $x = \beta$.

(c) This step comes from the identity $(x-\alpha)(x-\beta) = x^2-(\alpha+\beta)+\alpha\beta = x^2+bx+c$. We have that $-b = \alpha+\beta$, and that $(\alpha-\beta)^2 = (\alpha+\beta)^2-4\alpha\beta = b^2-4c$.

(d) We simply substitute (c) into (a), taking into account the fact from (b) that both roots can be found by switching the sign of the square root.

3 Higher-degree Polynomials

1. Find three different polynomials with variable x that have roots $x = 2$ and $x = 3$.

We could, for example, take

$$\begin{aligned}(x-2)(x-3) &= x^2 - 5x + 6\\ 17(x-2)(x-3) &= 17x^2 - 85x + 102\\ (x-2)(x-3)(x-17) &= x^3 - 22x^2 + 9x - 102.\end{aligned}$$

2. Show that $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ divided by $x^3 + 7$ gives a quotient of $x^3 + x^2 + x - 6$ and a remainder of $-6x^2 - 6x - 41$ by expanding and simplifying $(x^3+7)(x^3+x^2+x-6)+(-6x^2-6x-41)$.

Expanding the product, we find that

$$(x^3 + 7)(x^3 + x^2 + x - 6) = x^6 + x^5 + x^4 - 6x^3 + 7x^3 + 7x^2 + 7x + 42.$$

Adding on the remainder, we have

$$x^6+x^5+x^4-6x^3+7x^3+7x^2+7x+42-6x^2-6x-41 = x^6+x^5+x^4+x^3+x^2+x+1,$$

as expected.

3. Divide, finding the quotient and remainder polynomials: a. x^2-4 by $x-2$, b. x^2-4 by $x-3$, and c. t^7-t^3+5 by t^3+7.

$$\begin{array}{r|l} x-2 & x+2 \\ \hline x^2 - 4 & \\ -x^2+2x & \\ \hline 2x-4 & \\ -2x+4 & \\ \hline 0 & \end{array}$$

$$\begin{array}{r|l} x-3 & x+3 \\ \hline x^2 - 4 & \\ -x^2+3x & \\ \hline 3x-4 & \\ -3x+9 & \\ \hline 5 & \end{array}$$

$$\begin{array}{r|l} t^3+7 & t^4 - 7t - 1 \\ \hline t^7 - t^3 + 5 & \\ -t^7 - 7t^4 & \\ \hline -7t^4 - t^3 & \\ 7t^4 + 49t & \\ \hline -t^3 + 49t + 5 & \\ t^3 + 7 & \\ \hline 49t + 12 & \end{array}$$

4. If $x = 3$ is one zero of $x^3 - 3x^2 - 4x + 12$, find the other two.

$$\begin{array}{r|l} x-3 & x^2 - 4 \\ \hline x^3 - 3x^2 - 4x + 12 & \\ -x^3 + 3x^2 & \\ \hline -4x + 12 & \\ 4x - 12 & \\ \hline 0 & \end{array}$$

Dividing through by $(x - 3)$ using long division, we find the other two roots satisfy $x^2 - 4 = 0$. They are therefore $x = \pm 2$.

5. Solve $x^3 - x^2 - 3x + 3 = 0$.

We check to see if 0 or ± 1 are solutions, and it turs out that $x = 1$ is indeed a solution. We divide through by $x - 1$:

$$\begin{array}{r|l} & x^2 \quad\quad - 3 \\ \hline x-1 & x^3 - x^2 - 3x + 3 \\ & \underline{-x^3 + x^2} \\ & \quad\quad - 3x + 3 \\ & \quad\quad \underline{3x - 3} \\ & \quad\quad\quad 0 \end{array}$$

The other two solutions are therefore $x = \pm 3$.

6. Find the roots of $x^4 - x^3 - 43x^2 + 85x - 42$.

Notice that $x = 1$ is a solution. Dividing through as above:

$$\begin{array}{r|l} & x^3 \quad\quad\quad - 43x + 42 \\ \hline x-1 & x^4 - x^3 - 43x^2 + 85x - 42 \\ & \underline{-x^4 + x^3} \\ & \quad\quad - 43x^2 + 85x \\ & \quad\quad \underline{43x^2 - 43x} \\ & \quad\quad\quad\quad 42x - 42 \\ & \quad\quad\quad\quad \underline{-42x + 42} \\ & \quad\quad\quad\quad\quad 0 \end{array}$$

Note that $x = 1$ is again a solution. Dividing again:

$$\begin{array}{r|l} & x^2 \quad + x - 42 \\ \hline x-1 & x^3 \quad\quad - 43x + 42 \\ & \underline{-x^3 + x^2} \\ & \quad\quad x^2 - 43x \\ & \quad\quad \underline{-x^2 \quad + x} \\ & \quad\quad\quad - 42x + 42 \\ & \quad\quad\quad \underline{42x - 42} \\ & \quad\quad\quad\quad 0 \end{array}$$

We solve $x^2 + x - 42 = 0$ using the quadratic formula, or by inspection see that it factorises to $(x - 6)(x + 7)$. The roots of the original quartic are therefore $x \in \{-7, 1, 6\}$ (with $x = 1$ repeated).

7. How many distinct solutions does $(x^2 - 2x - 24)(x^2 + 5x) = (x^2 - 2x - 24)(4x + 12)$ have?

Rearranging, we have that the solutions satisfy

$$(x^2 - 2x - 24)(x^2 + 5x - 4x - 12) = (x^2 - 2x - 24)(x^2 + x - 12) = 0$$

which is easily solvable with the quadratic formula; the two quadratic factors share the solution $x = -4$, and so there are in total three distinct solutions: $x \in \{-4, 3, 6\}$.

8. Show that $t = 4$ is a zero of $t^4 - (6 + \sqrt{3})t^3 + 6\sqrt{3}t^2 + 32t - 32\sqrt{3}$.

$4^4 - (6 + \sqrt{3}) \cdot 4^3 + 6\sqrt{3} \cdot 4^2 + 32 \cdot 4 - 32\sqrt{3} = 0$.

9. Find the remainder after dividing $x^7 + 5x - 9$ by $(x - 6)$.

By the remainder theorem, the remainder will be $6^7 + 5 \times 6 - 9 = 179957$.

10. Find four polynomials $p_a(x)$, $p_b(x)$, $p_c(x)$, $p_d(x)$ with integer coefficients such that:

a. $p_a\left(\frac{1}{2}\right) = 0$;

b. $p_b\left(\frac{1}{2} + \frac{1}{2}\sqrt{3}\right) = 0$;

c. $p_c\left(2i - \sqrt{2}\right) = 0$; **and**

d. $p_d\left(\sqrt{i} + \frac{1}{\sqrt[3]{2}}\right) = 0$.

(a) $p(x) = 2x - 1$ is one such polynomial.

(b) Let $\alpha = \frac{1}{2} + \frac{1}{2}\sqrt{3}$. Then:

$$\begin{aligned} 2\alpha &= 1 + \sqrt{3} \\ (2\alpha - 1)^2 &= 3 \\ 4\alpha^2 - 4\alpha + 1 &= 3 \end{aligned}$$

so $p(x) = 4x^2 - 4x - 2$ is one such polynomial.

(c) Let $\beta = 2i - \sqrt{2}$. Then:

$$\begin{aligned} (\beta + \sqrt{2})^2 &= (2i)^2 = -4 \\ \beta^2 + 2\beta\sqrt{2} + 2 &= -4 \\ 2 &= \left(\frac{-6 - \beta^2}{2\beta}\right)^2 \\ 8\beta^4 &= 36 + 12\beta^2 + \beta^4 \end{aligned}$$

so $p(x) = -7x^4 + 12x^2 + 36$ is one such polynomial.

(d) This one is evil. It can be shown that such a polynomial is

$$p(x) = 16x^{12} - 32x^9 + 48x^8 + 24x^6 + 384x^5 + 48x^4 - 8x^3 + 120x^2 - 96x + 17$$

but we leave to the reader the unenviable job of deriving this result.

11. If x^2+bx+c and x^2+dx+e have a common factor of $(x-p)$, show that $\frac{e-c}{b-d}=p$.

$$\begin{aligned}
x^2+bx+x &= (x-p)(x-\alpha) = x^2-(\alpha+p)x+\alpha p \\
&\Rightarrow b = -(\alpha+p) \\
&\Rightarrow c = \alpha p \\
x^2+dx+e &= (x-p)(x-\beta) = x^2-(\beta+p)x+\beta p \\
&\Rightarrow d = -(\beta+p) \\
&\Rightarrow e = \beta p \\
\frac{e-c}{b-d} &= \frac{\beta p-\alpha p}{-\alpha-p+\beta+p} = \frac{p(\beta-\alpha)}{\beta-\alpha} = p
\end{aligned}$$

12. Let $p(x)=(x^2-25)^5$. One root of $p(x)$ is $x=5$. What is the multiplicity of this root?

We have $(x^2-25)^5=((x-5)(x+5))^5=(x-5)^5(x+5)^5$, so the multiplicity of the root $x=5$ is 5.

13. Is $(x+3)$ a factor of $2x^3+x^2-5x+7$?

By the remainder theorem: $2(-3)^3+(-3)^2-5(-3)+7=-23\neq 0$ so $x+3$ is not a factor.

14. Use the remainder theorem to compute $f(3)$ for $f(x)=x^4+x-10$.

We divide $f(x)$ by $x-3$:

$$\begin{array}{r|l}
 & x^3+3x^2+9x+28 \\
\hline
x-3 & x^4\qquad\qquad\quad +x-10 \\
 & \underline{-x^4+3x^3\qquad\quad\ } \\
 & \quad 3x^3 \\
 & \quad \underline{-3x^3+9x^2\ \ } \\
 & \qquad\quad 9x^2+x \\
 & \qquad\quad \underline{-9x^2+27x} \\
 & \qquad\qquad\quad 28x-10 \\
 & \qquad\qquad\quad \underline{-28x+84} \\
 & \qquad\qquad\qquad\quad 74
\end{array}$$

The remainder is 74, so $f(3)=74$.

15. Show that if $\alpha \neq 0$ and β are roots of $x^n - x = 0$ (for $n > 1$), then α^{-1} and $\alpha\beta$ are also roots. Why does this not imply that $x^2 - x = 0$ and $x^3 - x = 0$ have at least four roots?

Firstly, $(\alpha^{-1})^n - \alpha^{-1} = \alpha^{-1}\left[(\alpha^{-1})^{n-1} - 1\right]$. We must therefore show that $(\alpha^{-1})^{n-1} - 1 = 0$:

$$\begin{aligned}(\alpha^{-1})^{n-1} - 1 &= (\alpha^{n-1})^{-1} - 1 \\ &= \frac{1}{\alpha^{n-1}} - \frac{\alpha^{n-1}}{\alpha^{n-1}} \\ &= \frac{1 - \alpha^{n-1}}{\alpha^{n-1}}\end{aligned}$$

But $\alpha^n - \alpha = 0$ implies that $\alpha^{n-1} - 1 = 0$ since $\alpha \neq 0$, so $\frac{1-\alpha^{n-1}}{\alpha^{n-1}} = 0$ and α^{-1} is a root.

If $\beta = 0$ then it is trivial that $\alpha\beta = 0$ is a root, so assume that $\beta \neq 0$. Consider:

$$0 = (\alpha^n - \alpha) = \alpha(\alpha^{n-1} - 1) = \alpha(\alpha^{n-1} - 1)$$

So $\alpha^{n-1} = 1$. Similarly, $\beta^{n-1} = 1$. Then:

$$\begin{aligned}0 = (\alpha^n - \alpha)(\beta^n - \beta) &= \alpha^n\beta^n - \alpha\beta^n - \beta\alpha^n + \alpha\beta \\ &= \alpha^n\beta^n + \alpha\beta(1 - \beta^{n-1} - \alpha^{n-1}) \\ &= (\alpha\beta)^n + \alpha\beta(1 - 1 - 1) \\ &= (\alpha\beta)^n - \alpha\beta\end{aligned}$$

and $\alpha\beta$ is a root as required even if $\beta \neq 0$.

This argument does not show that $x^2 - x = 0$ has four roots, because the only two roots of this polynomial are 0 and 1; clearly $0 \times 1 = 0$ is also a root, and $1/1 = 1$ is a root — hence the theorem holds. (In other words, we do not claim that α, β, α^{-1}, and $\alpha\beta$ are **distinct** roots.)

Similarly, the three roots 0, 1, and -1 of $x^3 - x = 0$ are closed under multiplication and inversion.

Since the roots of the equation $x^n - x = 0$ are simply the $n-1$th roots of unity together with zero, exercise 6.19 makes this exercise trivial. If we restrict n to be a prime power (i.e. $n = p^m$ for some integer m), then it is possible to impose an addition structure on the roots as well if $\alpha + \beta$ is reduced modulo p. In fact, the roots of $x^{p^m} - x = 0$ modulo p form the (unique) finite field of order p^m denoted $GF(p^m)$ — the Galois field of order p^m).

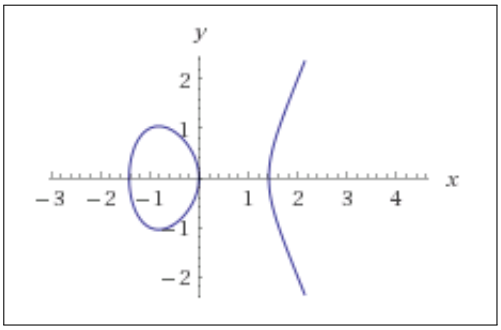
16. Elliptic curves are a form of cubic; they are equations of the form $y^2 = x^3 + ax + b$.

a. Find the x-intercepts of $y^2 = x^3 - 2x$.

b. Find the z-intercepts of $y^2 = x^3 - \frac{4}{3}x - \frac{16}{27}$, given that $z = x - \frac{1}{3}$.

c. Consider an elliptic curve $\mathcal{E}$, and let P and Q be two rational points (i.e. points whose coordinates are rational) which are lying on the curve. Let $\mathcal{L}$ be the chord line uniquely determined by P and Q. Show that if $\mathcal{L}$ and $\mathcal{E}$ intersect at a third point R, then this third point is rational.

(a) We solve these by setting $y = 0$, but taking care we don't lose solutions or gain solutions. For the first equation, $0 = x^3 - 2x$. Noting the first solution, $x = 0$, we divide through by x and find that the other two solutions are $x = \pm\sqrt{2}$.



(b) For the second, we first substitute for x, obtaining $y^2 = (z + \frac{1}{3})^3 - \frac{4}{3}(z + \frac{1}{3}) - \frac{16}{27}$. This simplifies to $y^2 = z^3 + z^2 - z - 1$. Noticing that one solution to this is $z = 1$, we divide:

$$
\begin{array}{r|l}
z-1 & z^2+2z+1 \\
\hline
z^3+z^2-z-1 & \\
-z^3+z^2 & \\
\hline
2z^2-z & \\
-2z^2+2z & \\
\hline
z-1 & \\
-z+1 & \\
\hline
0 &
\end{array}
$$

The resulting quadratic has a single repeated root, $z = -1$. Hence, it seems that we have two solutions for z: $z = -1$ and $z = 1$. If we take $z = -1$ we have $x = -\frac{2}{3}$, which gives us $y^2 = \left(-\frac{2}{3}\right)^3 - \frac{4}{3}\left(-\frac{2}{3}\right) - \frac{16}{27} = 0$ and so $z = 1$ satisfies the original equation; and if we take $z = 1$ we have $x = \frac{4}{3}$ and $y^2 = \left(\frac{4}{3}\right)^3 - \frac{4}{3}\left(\frac{4}{3}\right) - \frac{16}{27} = 0$.

At the time of writing, WolframAlpha only finds a single solution ($x = -\frac{2}{3}$).

The substitution $z = x - \frac{b}{3a}$ is a standard one to remove the quadratic term from a cubic equation $az^3 + bz^2 + cz + d = 0$; see exercise 18.

(c) Let $\mathcal{E}$ be the curve $y^2 = x^3 + ax + c$, and let $\mathcal{L}$ be the line $y = mx + c$. Then we wish to find the solutions to $(mx + c)^2 = x^3 + ax + b$. Expanding and rearranging, we find that

$$0 = x^3 + m^2x^2 + (a + 2mc)x + b + c^2.$$

We know that two solutions to this equation are rational. However, note that m^2 is the sum of the three solutions (why?) and is itself rational; hence the third solution must also be rational (and so the two coordinates of the corresponding point on $\mathcal{E}$ are rational).

17. The polynomial $x^3 + px - 1$ has three real non-zero roots, α, β, and γ.

a. Find the value of $\alpha^2 + \beta^2 + \gamma^2$ in terms of p, and hence show that p is negative.

b. Find the cubic polynomial with coefficients in terms of p with the roots α^2, β^2, and γ^2.

(a) We first have that $(x-\alpha)(x-\beta)(x-\gamma) = x^3 - (\alpha+\beta+\gamma)x^2 + (\alpha\gamma+\beta\gamma+\alpha\beta)x - \alpha\beta\gamma$. Matching coefficients, $0 = \alpha+\beta+\gamma$ and $p = \alpha\gamma+\beta\gamma+\alpha\beta$. Squaring the first: $(\alpha+\beta+\gamma)^2 = \alpha^2+\beta^2+\gamma^2+2(\alpha\gamma+\beta\gamma+\alpha\beta) = \alpha^2+\beta^2+\gamma^2+2p$. So $0 = \alpha^2+\beta^2+\gamma^2+2p$, and $-2p = \alpha^2+\beta^2+\gamma^2$. But since the roots are all real and non-zero, $\alpha^2+\beta^2+\gamma^2 > 0$ and therefore p must be negative.

(b) In order to find the polynomial, we let $z = x^2$ and substitute. We have:

$$\begin{aligned} x^3 + px &= 1 \\ x(x^2+p) &= 1 \\ x^2(x^2+p)^2 &= 1^2 = 1 \\ z(z+p)^2 &= 1 \\ z^3 + 2pz^2 + zp^2 - 1 &= 0. \end{aligned}$$

Alternatively, we can form $(x-\alpha^2)(x-\beta^2)(x-\gamma^2)$ and then substitute in the identities $\alpha^2+\beta^2+\gamma^2 = -2p$, $\alpha^2\beta^2\gamma^2 = (\alpha\beta\gamma)^2 = 1$, and $(\alpha^2\beta^2+\alpha^2\gamma^2+\beta^2\gamma^2) = (\alpha\beta+\alpha\beta+\beta\gamma)^2 = p^2$ to find the same polynomial.

18. Take the general cubic, at^3+bt^2+ct+d. Show that the substitution $t = y - \frac{b}{3a}$ will give a cubic in y with no quadratic term (this is known as a Tschirnhaus substitution and is the first step to create a general formula to solve the cubic).

We have:

$$\begin{aligned} t^2 &= \left(y - \frac{b}{3a}\right)^2 \\ &= y^2 - \frac{2b}{3a}y + \frac{b^2}{9a^2} \\ t^3 &= \left(y^2 - \frac{2b}{3a}y + \frac{b^2}{9a^2}\right)\left(y - \frac{b}{3a}\right) \\ &= y^3 - \frac{2b}{3a}y^2 + \frac{b^2}{9a^2}y - \frac{b}{3a}y^2 + \frac{2b^2}{9a^2}y - \frac{b^3}{27a^3} \\ &= y^3 - \frac{b}{a}y^2 + \frac{b^2}{3a^2}y - \frac{b^3}{27a^3}. \end{aligned}$$

Substituting, we have

$$a\left(y^3 - \frac{b}{a}y^2 + \frac{b^2}{3a^2}y - \frac{b^3}{27a^3}\right) + b\left(y^2 - \frac{2b}{3a}y + \frac{b^2}{9a^2}\right) + c\left(y - \frac{b}{3a}\right) + d$$

which we regroup to obtain

$$ay^3 + y^2(-b+b) + y\left(\frac{b^2}{3a} - \frac{2b^2}{3a} + c\right) - \frac{b^3}{27a^2} + \frac{b^3}{9a^2} - \frac{bc}{3a} + d$$

in which the quadratic term obviously vanishes.

19. Show that $\sqrt{2}+\sqrt{3} = \sqrt{5+\sqrt{6}}$.

Note $\sqrt{5+\sqrt{6}} = \sqrt{2+\sqrt{2}\sqrt{3}+3} = \sqrt{(\sqrt{2}+\sqrt{3})^2} = \left|\sqrt{2}+\sqrt{3}\right|$; but square roots are positive, so $\left|\sqrt{2}+\sqrt{3}\right| = \sqrt{2}+\sqrt{3}$.

20. Prove the following identity.[2]

$$\sqrt[3]{-18+\sqrt{325}}+\sqrt[3]{-18-\sqrt{325}}=-3$$

Let $u=-18+\sqrt{325}$ and $v=-18-\sqrt{325}$. In order to prove this identity, we first require the following lemma:

Lemma. *The two roots of $p=t^2+3t-1$ can be expressed as $\sqrt[3]{u}$ and $\sqrt[3]{v}$.*

Call the two roots of p α and β. By the quadratic formula, $\alpha=\frac{-3+\sqrt{13}}{2}$. We now show that $\alpha^3=u$, and therefore (since we are working in the reals and so each number has a single unique cube root) $\alpha=\sqrt[3]{u}$:

$$\begin{aligned}\alpha^3&=\left(\frac{-3}{2}+\frac{\sqrt{13}}{2}\right)^3\\&=-\frac{27}{8}+3\cdot\frac{9}{4}\cdot\frac{\sqrt{13}}{2}-3\cdot\frac{3}{2}\cdot\frac{13}{4}+\frac{13\sqrt{13}}{8}\\&=-\frac{27}{8}+\frac{27\sqrt{13}}{8}-\frac{117}{8}+\frac{13\sqrt{13}}{8}\\&=\frac{1}{8}(-144+40\sqrt{13})\\&=-18+5\sqrt{13}=u.\end{aligned}$$

Likewise, $\beta=\frac{-3-\sqrt{13}}{2}=\sqrt[3]{v}$.

Theorem. *That $\sqrt[3]{-18+\sqrt{325}}+\sqrt[3]{-18-\sqrt{325}}=-3$.*

From the lemma, we have $p=\left(t-\sqrt[3]{u}\right)\left(t-\sqrt[3]{v}\right)$. Expanding, $p=t^2-\left(\sqrt[3]{u}+\sqrt[3]{v}\right)t+\sqrt[3]{u}\sqrt[3]{v}$, and matching coefficients with the definition of p in the lemma we have $-3=\sqrt[3]{u}+\sqrt[3]{v}$.

21. Let $w=a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$, where a, b, c, and d are rational. Find rational numbers p, q, r and s such that

$$w=p+q(\sqrt{2}+\sqrt{3})+r(\sqrt{2}+\sqrt{3})^2+s(\sqrt{2}+\sqrt{3})^3.$$

Note that $(\sqrt{2}+\sqrt{3})^2=5+2\sqrt{6}$ and $(\sqrt{2}+\sqrt{3})^3=11\sqrt{2}+9\sqrt{3}$, so we are trying to find p, q, r, and s such that

$$\begin{aligned}a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}&=p+5r+q\sqrt{2}+q\sqrt{3}+2r\sqrt{6}+11s\sqrt{2}+9s\sqrt{3}\\&=(p+5r)+(q+11s)\sqrt{2}+(q+9s)\sqrt{3}+2r\sqrt{6}.\end{aligned}$$

Hence $r=d/2$, $p=a-5r=a-\frac{5}{2}d$, $s=\frac{b-c}{2}$, and $q=b\left(1-\frac{11(b-c)}{2}\right)$.

[2] See chapter 1 of Stewart (2004) for historical context, but note that the identity as stated there is in error (and not listed in errata).

22. Show that there are no integers r and s such that $\sqrt{2} = \frac{r}{s}\sqrt{3}$.

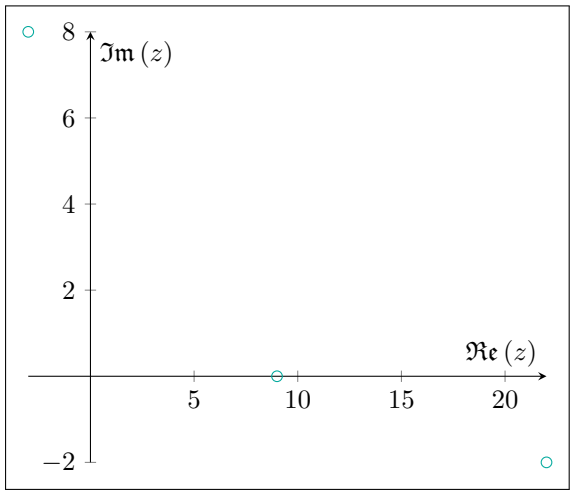
Suppose that such integers exist, and that they are coprime (i.e. r/s is in lowest form); then we play the familar game. In particular, we note that $3r^2 = 2s^2$. By Euclid's lemma, s must be a multiple of 3; let's write $s = 3^n p$ for the largest possible n (so p is not a multiple of 3). Substituting back in, we have $r^2 = \frac{2(3^n p)^2}{3} = 2 \times 3^{2n-1} p^2$. But looking at this carefully, we have an odd power of 3 on the right, and all the prime powers of r^2 must be even! This is a contradiction, and so there exists no rational number r/s.

In particular, we have shown that if we consider $\mathbb{R}$ a vector space over the rational numbers, then $\sqrt{2}$ and $\sqrt{3}$ are linearly independent. This is a counterexample to the intuitive 'theorem' that the real field has no non-identity automorphisms over the rationals: simply take the function that swaps $\sqrt{2}$ and $\sqrt{3}$!

4 Complex Numbers

1. **Evaluate the following expressions, and plot the answers on an Argand diagram:**
   a. $(3 + 2i) + (6 - 2i)$
   b. $24 - (6 + 2i)$
   c. $2(2 + i) + 6i - 7$

The three points are 9, $22 - 2i$, and $-3 + 8i$.



2. **If we add two real numbers, can we obtain an imaginary number? If we add two imaginary numbers, can we obtain a real number?**

If we add two real numbers, we cannot obtain an imaginary number; however, it is possible to add two imaginary numbers, and obtain zero (a real number). For example, $-i + i = 0 \in \mathbb{R}$.

3. Let $v = 3 - 7i$ and $w = -4 + 6i$.

a. Find the real numbers p and q such that $pv + qw = 6.5 - 11i$.

b. Show that any complex number z can be written as $z = pv + qw$ for some real p and q.

(a) We have $p(3 - 7i) + q(-4 + 6i) = (3p - 4q) + i(-7p + 6q)$, and so:

$$\begin{aligned} 3p - 4q &= 6.5 \\ -7p + 6q &= -11 \end{aligned}$$

Hence $p = \frac{1}{2}$ and $q = -\frac{5}{4}$.

(b) We wish to find a and b such that $1 = a(3 - 7i) + b(-4 + 6i)$. This gives us the set of simultaneous equations

$$\begin{aligned} 1 &= 3a - 4b \\ 0 &= 6b - 7a \end{aligned}$$

which is easily solved to give $1 = -0.6v - 0.7w$. Similarly, $i = -0.4v - 0.3w$. Hence if $z = a + bi$, then $z = (-0.6v - 0.7w)a + (-0.4v - 0.3w)b = (-0.6a - 0.4b)v + (-0.7a - 0.3b)w$.

4. Solve the quadratic equation $x^2 + 4 = 0$.

$x = \pm 2i$.

5. Prove that $z + \bar{z} = 2 \cdot \mathfrak{Re}(z)$ and $z - \bar{z} = 2i \cdot \mathfrak{Im}(z)$.

Let $z = x + yi$. Then $z + \bar{z} = x + yi + x - yi = 2x = 2\mathfrak{Re}(z)$.

Similarly, $z - \bar{z} = x + yi - x + yi = 2yi = 2i\mathfrak{Im}(z)$.

6. Verify the following properties of conjugation.

a. $\bar{\bar{z}} = z$

b. $\bar{w} + \bar{z} = \overline{w + z}$

c. $\bar{w}\bar{z} = \overline{wz}$

Suppose $w = a + bi$ and $z = c + di$.

(a)

$$\bar{\bar{z}} = \overline{c - di} = c + di.$$

(b)

$$\bar{w} + \bar{z} = a - bi + c - di = (a + c) - (b + d)i = \overline{w + z}.$$

(c)

$\bar{w}\bar{z} = (a-bi)(c-di) = (ac-bd)-(bc+ad)i = \overline{(ac-bd)+(bc+ad)i} = \overline{(a+bi)(c+di)} = \overline{wz}.$

7. Find i^{957}.

First, note that $957 = 956 + 1 = 4(239) + 1$. So $i^{957} = i^{4(239+1)} = (i^4)^{957}i = 1^{957}i = i$.

8. Show that $|a+bi| \geq |a|$ and $|a+bi| \geq |b|$.

We have $|a+bi| = \sqrt{a^2+b^2} \geq \sqrt{a^2} = |a|$. Similarly $|a+bi| = \sqrt{a^2+b^2} \geq \sqrt{b^2} = |b|$.

9. Find $(3+2i)(6+8i)$ in rectangular form.

$(3+2i)(6+8i) = 18 + 12i + 24i + 16i^2 = 2 + 36i$.

10. a. Convert $1+i$ into polar form.

b. Find $(1+i)(\sqrt{2}\operatorname{cis}\frac{3\pi}{4})$ in both polar form and rectangular form.

(a) We have $1 + i = \sqrt{2}\operatorname{cis}\frac{\pi}{4}$.

(b)

$$\begin{aligned}(1+i)(\sqrt{2}\operatorname{cis}\frac{3\pi}{4}) &= (\sqrt{2}\operatorname{cis}\frac{\pi}{4})(\sqrt{2}\operatorname{cis}\frac{3\pi}{4}) \\ &= 2\operatorname{cis}\pi \qquad\qquad = -2.\end{aligned}$$

11. Compute $(6\operatorname{cis}\frac{23\pi}{24})(9\operatorname{cis}\frac{14\pi}{17})$, leaving your answer in polar form.

$$54\operatorname{cis}\left(\frac{23\pi}{24} + \frac{14\pi}{17}\right) = 54\operatorname{cis}\frac{727\pi}{408}.$$

12. a. Prove that $(r\operatorname{cis}\theta)(t\operatorname{cis}\varphi) = (rt)\operatorname{cis}(\theta+\varphi)$.

b. Describe the geometric meaning of the multiplication of complex numbers.

(a) Trigonometric Proof:

$$\begin{aligned}(r\operatorname{cis}\theta)(t\operatorname{cis}\varphi) &= r(\cos\theta + i\sin\theta) \times t(\cos\varphi + i\sin\varphi)\\ &= rt((\cos\theta)(\cos\varphi) - (\sin\theta)(\sin\varphi) + i(\sin\theta\cos\varphi + \cos\theta\sin\varphi))\\ &= rt(\cos(\theta+\varphi) + i(\sin(\theta+\varphi)))\\ &= rt\operatorname{cis}(\theta+\varphi).\end{aligned}$$

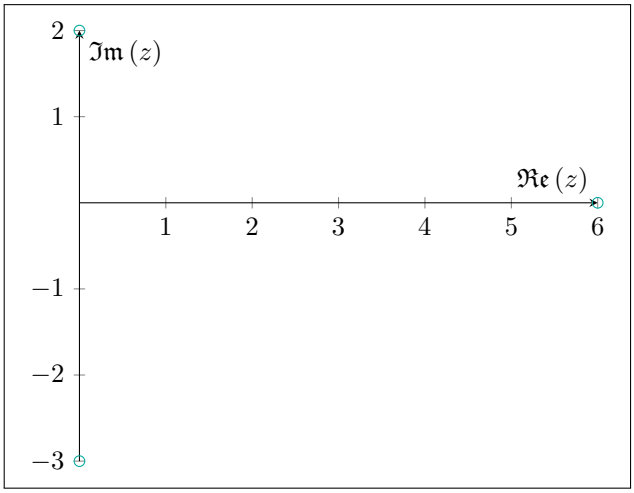
Analytic Proof:

$$\begin{aligned}(r\operatorname{cis}\theta)(t\operatorname{cis}\varphi) &= re^{i\theta}\cdot te^{i\varphi}\\ &= rte^{i\theta+i\varphi}\\ &= rte^{i(\theta+\varphi)}\\ &= rt\operatorname{cis}(\theta+\varphi).\end{aligned}$$

(b) The act of complex multiplication both scales the point (by a factor of the modulus) and rotates it around the origin (by the argument).

13. Let $u = 2\operatorname{cis}\frac{\pi}{2}$ and $v = 3cis\frac{3\pi}{2}$. Plot u, v, and uv on an Argand diagram.

$uv = 6\operatorname{cis}2\pi = 6.$



14. Prove de Moivre's Theorem: $(r\operatorname{cis}\theta)^n = (r^n)\operatorname{cis}(n\theta)$.

Trigonometric Proof: Induction on n using the result in 12.

Analytic Proof:

$$\begin{aligned}(r\operatorname{cis}\theta)^n &= \left(re^{i\theta}\right)^n \\ &= r^n\left(e^{i\theta}\right)^n \\ &= r^n e^{in\theta} \\ &= (r^n)\operatorname{cis}(n\theta).\end{aligned}$$

15. Show that if $u = r\operatorname{cis}\theta$ and $v = t\operatorname{cis}\varphi$ then $\frac{u}{v} = \frac{r}{t}\operatorname{cis}(\theta-\varphi)$.

Taking $(t\operatorname{cis}\varphi)^{-1}$, we obtain $\frac{1}{t}\operatorname{cis}(-\varphi)$ (using de Moivre's Theorem), and so

$$\frac{r\operatorname{cis}\theta}{t\operatorname{cis}\varphi} = \frac{r}{t}\operatorname{cis}(\theta-\varphi).$$

16. Using de Moirve's Theorem, prove that for complex numbers w and m and integers n and m,

a. $w^n w^m = w^{n+m}$

b. $(w^n)^m = w^{nm}$

Let $w = r\operatorname{cis}\theta$.

(a) $w^n w^m = r^n \operatorname{cis} n\theta r^m \operatorname{cis} m\theta = r^{n+m}\operatorname{cis}(n+m)\theta = w^{n+m}$

(b) $(w^n)^m = (r^n\operatorname{cis} n\theta)^m = (r^n)^m \operatorname{cis} nm\theta = r^{nm}\operatorname{cis} nm\theta = w^{nm}$.

17. Convert $w = 1+\sqrt{3}i$ into polar form, and calculate w^3.

$|w| = \sqrt{1^2+\sqrt{3}^2} = 2$, $\arg w = \arctan\frac{\sqrt{3}}{1} = \frac{\pi}{3}$.

Hence $w^3 = (2\operatorname{cis}\frac{\pi}{3})^3 = 2^3\operatorname{cis}\pi = -8$, using de Moivre's Theorem.

18. Show that for any complex number z, the product $z\bar{z}$ is both real and non-negative. Hence show that $(x-z)(x-\bar{z})$ has only real coeffients.

Let $z = a+bi$. Then $z\bar{z} = (a+bi)(a-bi) = a^2+b^2$, which is real and positive (or zero). This also provides an identity for the sum of two squares.

$(x-z)(x-\bar{z}) = x^2-(z+\bar{z})+z\bar{z} = x^2+2a+a^2+b^2$, and since $a, b \in \mathbb{R}$ the coefficients are real.

19. Let x be a real number. Show that, for all integers n, $\operatorname{cis}\frac{2x\pi}{n} = \operatorname{cis}\frac{2(x+n)\pi}{n}$.

We argue as follows:

$$\begin{aligned}
\operatorname{cis}\frac{2(x+n)\pi}{n} &= \cos\frac{2(x+n)\pi}{n} + i\sin\frac{2(x+n)\pi}{n} \\
&= \cos\frac{2x\pi}{n}\cos 2\pi - \sin\frac{2x\pi}{n}\sin 2\pi + i(\sin\frac{2x\pi}{n}\cos 2\pi + \cos\frac{2x\pi}{n}\sin 2\pi) \\
&= \cos\frac{2x\pi}{n}\cdot 1 - \sin\frac{2x\pi}{n}\cdot 0 + i(\sin\frac{2x\pi}{n}\cdot 1 + \cos\frac{2x\pi}{n}\cdot 0) \\
&= \cos\frac{2x\pi}{n} + i\sin\frac{2x\pi}{n} \\
&= \operatorname{cis}\frac{2x\pi}{n}.
\end{aligned}$$

20. For which complex numbers is z^2 real? What about z^3?

Let $z = x + yi$. Then $z^2 = x^2 + 2xyi - y^2$, which will be real if and only if $2xy = 0$; so at least one of x or y must be zero for z to be real. In other words, z must be either totally real or totally imaginary.

For the cube, we have $z^3 = x^3 + 3x^2yi - 3xy^2 - iy^3$. For z^3 to be real, we must have $3x^2y - y^3 = 0$. This will occur when $y = 0$; noting this, we suppose $y \neq 0$ and divide through by y, obtaining $3x^2 = y^2$. Solving this, we find $y = \pm\sqrt{3}x$. So z^3 will be real either if z is totally real, or if $\mathfrak{Im}(z) = \pm\sqrt{3}\mathfrak{Re}(z)$.

21. Transform $\frac{a+bi}{c+di}$ so that the only imaginary part is in the numerator.

Using the idea from question 18:

$\frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{(c+di)(c-di)} = \frac{ac+bd+(bc-ad)i}{c^2+d^2}$, where the denominator is real.

22. Find $(a+bi)^{-1}$.

$$\begin{aligned}
\frac{1}{a+bi} &= \frac{a-bi}{(a+bi)(a-bi)} \\
&= \frac{a-bi}{a^2+b^2} \\
&= \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i.
\end{aligned}$$

23. Write the complex number $\left(\frac{4i^7-i}{1+2i}\right)^2$ in the form $a+bi$, where a and b are real numbers.

$$\begin{aligned}\left(\frac{4i^7-i}{1+2i}\right)^2 &= \left(\frac{-4i-i}{1+2i}\right)^2\\ &= \left(\frac{-5i}{1+2i}\right)^2\\ &= \frac{25}{-3+4i}\\ &= \frac{25(-3-4i)}{(-3+4i)(-3-4i)}\\ &= \frac{25-3-4i}{25}\\ &= -3-4i.\end{aligned}$$

24. a. Prove that a number z is real if and only if $\bar{z}=z$.

b. Hence, or otherwise, show that $z\bar{w}+w\bar{z}$ is always real.

c. Show that $z\bar{w}+w\bar{z}\leq 2|w||z|$.

(a) Let $z=a+bi$. Suppose z is real. Then $b=0$, and $\bar{z}=\overline{a+0i}=a-0i=z$. Conversely, suppose $\bar{z}=z$. Then $a-bi=a+bi$, and $b=-b$; hence $b=0$ and z is real.

(b) By part (a), we need only check that the given expression is its own conjugate:

$$\overline{z\bar{w}+w\bar{z}}=\overline{z\bar{w}}+\overline{w\bar{z}}=\bar{z}\bar{\bar{w}}+\bar{w}\bar{\bar{z}}=\bar{z}w+\bar{w}z$$

(c) Let $z=r\operatorname{cis}\theta$ and $w=t\operatorname{cis}\phi$. Then we have:

$$\begin{aligned}z\bar{w}+w\bar{z} &= (r\operatorname{cis}\theta)(t\operatorname{cis}-\phi)+(t\operatorname{cis}\phi)(r\operatorname{cis}-\theta)\\ &= (rt)\operatorname{cis}(\theta-\phi)+(rt)\operatorname{cis}(\phi-\theta)\\ &= rt(\cos(\theta-\phi)+\cos(\phi-\theta)+i(\sin(\theta-\phi)+\sin(\phi-\theta)))\\ &= 2rt\cos(\theta-\phi)\\ &\leq 2rt \qquad (\text{since } \cos x\leq 1)\\ &= 2|z||w|\,.\end{aligned}$$

25. Show that if $z=a+ib$ then $\sqrt{z\bar{z}}=|z|$.

From question 18, we have $z\bar{z}=a^2+b^2$; hence $\sqrt{z\bar{z}}=\sqrt{a^2+b^2}=|z|$.

26. If $\zeta = \sqrt{\frac{1}{2}(a+\sqrt{a^2+b^2})} + i\sqrt{\frac{1}{2}(-a+\sqrt{a^2+b^2})}$ is a complex number, find ζ^2 in the form $p+iq$ (where a, b, p, and q are real).

$$\begin{aligned}
&\left(\sqrt{\frac{1}{2}(a+\sqrt{a^2+b^2})} + i\sqrt{\frac{1}{2}(-a+\sqrt{a^2+b^2})}\right)^2 \\
&= \frac{1}{2}(a+\sqrt{a^2+b^2}) + 2i\sqrt{\frac{1}{2}(a+\sqrt{a^2+b^2})}\sqrt{\frac{1}{2}(-a+\sqrt{a^2+b^2})} - \frac{1}{2}(-a+\sqrt{a^2+b^2}) \\
&= a + 2i\sqrt{\frac{1}{4}(\sqrt{a^2+b^2}+a)(\sqrt{a^2+b^2}-a)} \\
&= a + 2i\sqrt{\frac{1}{4}((a^2+b^2)-a^2)} \\
&= a + 2i\sqrt{\frac{b^2}{4}} \\
&= a + bi.
\end{aligned}$$

27. If $z = x+iy$, and $az^2+bz+c=0$, show that $a\bar{z}^2+b\bar{z}+c=0$ if a, b, and c are real. (This exercise is generalised in 9.32.)

See the exercise noted in the question for an easier way to prove this (which requires a bit less work).

Let the value of $a\bar{z}^2+b\bar{z}+c$ be K — our goal is to prove that $K=0$.

We have that

$$\begin{aligned}
a\bar{z}^2+b\bar{z}+c &= a(x-iy)^2+b(x-iy)+c \\
&= ax^2-2aixy-ay^2+bx-biy+c = K. \qquad (1)
\end{aligned}$$

And that

$$\begin{aligned}
az^2+bz+c &= a(x+iy)^2+b(x+iy)+c \\
&= ax^2+2aixy-ay^2+bx+biy+c = 0. \qquad (2)
\end{aligned}$$

Note that the real part of this equation is ax^2-ay^2+bx+c.

Since the second equation is equal to zero, we can add it to the first:

$$\begin{array}{rccccccc}
(& ax^2 & -2aixy & -ay^2 & +bx & -biy & +c & =K) \quad (1) \\
+(& ax^2 & +2aixy & -ay^2 & +bx & +biy & +c & =0) \quad (2) \\
= & 2ax^2 & & -2ay^2 & +2bx & & +2c & =K) \quad (3)
\end{array}$$

But we notice that the real part of (2) must be equal to zero — and equation (3) is simply twice the real part of (2), so $K=0$.

28. Use Euler's identity to find $\ln(-1)$, and hence $\ln(-x)$ for real x.

$$\begin{aligned} e^{i\pi} &= -1 \\ i\pi &= \ln(-1) \end{aligned}$$

Notice that $\operatorname{cis}\theta = e^{i\pi}$ is has a period of 2π, so $\ln(-1) = i(\pi + 2n\pi)$ for $n \in \mathbb{N}$.

$$\begin{aligned} \ln -x &= \ln(-1 \times x) \\ &= \ln(-1) + \ln x \\ &= \ln x + i\pi(1 + 2n). \end{aligned}$$

29. Prove that for every positive integer n, $(-1+\sqrt{3}i)^{3n}+(-1-\sqrt{3}i)^{3n} = 2^{3n+1}$.

If we convert $-1 + \sqrt{3}i$ to polar form, we obtain $2\operatorname{cis}\frac{5\pi}{6}$. Substituting:

$$\begin{aligned} (-1+\sqrt{3}i)^{3n} + (-1-\sqrt{3}i)^{3n} &= \left(2\operatorname{cis}\frac{2\pi}{3}\right)^{3n} + \left(2\operatorname{cis}\frac{-2\pi}{3}\right)^{3n} \\ &= 2^{3n}(\operatorname{cis} 2\pi n) + 2^{3n}\operatorname{cis}(-2\pi n) \\ &= 2^{3n} + 2^{3n} \\ &= 2^{3n+1}. \end{aligned}$$

30. Show that $y_1(x) = e^{ix} + e^{-ix}$ and $y_2(x) = 2\cos x$ are both solutions of the differential equation

$$\frac{\mathrm{d}^2y}{\mathrm{d}x^2} + y = 0$$

with initial conditions $y(0) = 2$ and $y'(0) = 0$. (Also see 32 below.)

Note that $y_1'(x) = ie^{ix} - ie^{-ix}$ and $y_1''(x) = -e^{ix} - e^{-ix} = -y_1$, so y_1 is a solution of the differential equation. We also have $y_2'(x) = -2\sin x$ and $y_2'' = -2\cos x = -y_2$, so y_2 is also a solution.

We check that the initial conditions hold: $y_1(0) = 1+1 = 2$ and $y_1'(0) = i - i = 0$, and $y_2(0) = 2$ and $y_2'(0) = 0$ as required. Hence y_1 and y_2 are both solutions of the differential equation that satisfy the initial conditions.

Note that in exercise 32 below, it is proved that in fact $y_1 = y_2$.

31. Find $\sqrt{i}$ in rectangular form.

Note that $i = \operatorname{cis}\frac{\pi}{2}$, so $\sqrt{i} = \operatorname{cis}(\frac{\pi}{4} + \frac{2n\pi}{2})$ for $n \in \{0, 1\}$. Hence the two square roots are $\operatorname{cis}\frac{\pi}{4} = \frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}}$ and $\operatorname{cis}\frac{5\pi}{4} = -\frac{1}{\sqrt{2}} - i\frac{1}{\sqrt{2}}$.

32. a. Show that $\cos\theta = \frac{e^{i\theta}+e^{-i\theta}}{2}$ and that $\sin\theta = \frac{e^{i\theta}-e^{-i\theta}}{2i}$.

b. If $x + x^{-1} = 2\cos\theta$, find $x^n + x^{-n}$ in terms of n and θ.

(a)

$$\begin{aligned} e^{i\theta} + e^{-i\theta} &= \operatorname{cis}\theta + \operatorname{cis} -\theta \\ &= \cos\theta + i\sin\theta + \cos -\theta + \sin -\theta \\ &= \cos\theta + i\sin\theta + \cos\theta - \sin\theta \\ &= 2\cos\theta. \\ e^{i\theta} - e^{-i\theta} &= \operatorname{cis}\theta - \operatorname{cis} -\theta \\ &= \cos\theta + i\sin\theta - \cos -\theta - \sin -\theta \\ &= \cos\theta + i\sin\theta - \cos\theta + \sin\theta \\ &= 2i\sin\theta. \end{aligned}$$

(b) From (a), $2\cos\theta = e^{i\theta} + e^{-i\theta} = e^{i\theta} + \left(e^{i\theta}\right)^{-1}$, and so $x = e^{i\theta}$. Hence $x^n = e^{ni\theta}$, and:

$$\begin{aligned} x^n + x^{-n} &= e^{ni\theta} + e^{-ni\theta} \\ &= \cos n\theta + i\sin n\theta + \cos n\theta - i\sin n\theta \\ &= 2\cos n\theta. \end{aligned}$$

33. **a. Show that $(2 \pm i)^3 = 2 \pm 11i$.**

b. Simplify fully $\sqrt[3]{2+\sqrt{-121}} + \sqrt[3]{2-\sqrt{-121}}$.

c. Show that (b) is a root of the cubic equation $t^3 - 15t - 4 = 0$, and hence find all three solutions.

Firstly, $(2+i)(2+i)(2+i) = (3+4i)(2+i) = 2+11i$; likewise, we have $(2-i)^3 = 2-11i$. Using this result, we can simplify the expression in (b):

$$\begin{aligned} \sqrt[3]{2+\sqrt{-121}} + \sqrt[3]{2-\sqrt{-121}} &= \sqrt[3]{2+11i} + \sqrt[3]{2-11i} \\ &= \sqrt[3]{(2+i)^3} + \sqrt[3]{(2-i)^3} \quad = (2+i) + (2-i) \\ &= 4. \end{aligned}$$

It is easy to show that 4 is a root of the cubic in (c): $4^3 - 15\cdot 4 - 4 = 0$, as expected.

We divide the cubic by $t-4$ to reduce it to a quadratic:

$$\begin{array}{r|l} & t^2 + 4t + 1 \\ \hline t-4 & t^3 - 15t - 4 \\ & \underline{-t^3 + 4t^2} \\ & 4t^2 - 15t \\ & \underline{-4t^2 + 16t} \\ & t - 4 \\ & \underline{-t + 4} \\ & 0 \end{array}$$

By the quadratic formula, the two solutions of the quadratic factor are $t = -2 \pm \sqrt{3}$, so the three solutions of the cubic must be $t \in \{-2 \pm \sqrt{3}, 4\}$.

34. You do not need the fundamental theorem of algebra for this exercise.

a. Prove that all cubic equations with real coefficients must have exactly three roots in the complex numbers.

b. Let $p(x)$ be a polynomial of degree n such that there exists some complex number ζ such that $p(\zeta) = 0$. Show that $p(x) = 0$ has exactly n solutions (counting repeated roots).

(a) A cubic with real coefficients must have at least one real root. There are two ways to see this; firstly, a cubic with real coefficients must cross the x-axis at at least one point; and secondly, all non-real roots of polynomials with real coefficients must come in conjugate pairs (in order for the imaginary parts to cancel in the coefficients) and so a real polynomial with an odd number of roots must have at least one real root.[3]

Call our real root p. Our cubic is $ax^3 + bx^2 + cx + d = 0$, and we can divide it out by $x - p$, which we know is a factor, to obtain a quadratic. We know that the coefficients of this quadratic factor must multiply with the real coefficients of the linear factor to give the real coefficients of the cubic, and so the coefficients of the quadratic must be real... and so we can apply the quadratic formula to show that the roots of the quadratic must be complex!

Hence all three roots of the general cubic are complex. *Note that all real roots are also complex.*

(b) We use induction on n. Firstly, note that if $n = 1$ then the result is trivial.

Now, suppose that the theorem holds for all polynomials of degree $n - 1$. It follows from $p(\zeta) = 0$ that $(x - \zeta)$ is a factor of $p(x)$, and so $p(x) = (x - \zeta)q(x)$ where $\partial q = n - 1$. But by the inductive hypothesis, $q(x)$ has exactly $n - 1$ roots; so $p(x)$ has n roots, and if the theorem holds for polynomials of degree $n - 1$ then it holds for polynomials of degree n.

Hence, by the axiom of induction, it follows that if a polynomial of degree n has at least one complex root then it has exactly n complex roots.

[3] A proof that roots of real polynomials come in conjugate pairs is exercise 9.32.

5 Geometry

1. Show that, if a and b are fixed complex numbers, then $|z-a| = |z-b|$ describes the line which cuts the midpoint of the segment between a and b at a right angle.

Suppose that the distance from z to a is equal to the distance from z to b.

The line joining a and b has direction $a-b$; the line joining z and $m(a,b) = \frac{a+b}{2}$ has direction $z - \frac{a+b}{2}$. I claim that the two complex numbers obtained are orthogonal. Indeed,

$$\begin{aligned}(z - \frac{a+b}{2}, a-b) &= (z,a) - (z,b) - (\frac{a+b}{2}, a) + (\frac{a+b}{2}, b) \\ &= (z,a) - (z,b) - \frac{1}{2}((a,a)+(b,a)) + \frac{1}{2}((a,b)+(b,b)) \\ &= (z,a) - (z,b) + \frac{1}{2}(b,b) - \frac{1}{2}(a,a).\end{aligned}$$

But $|z-a| = |z-b|$, so

$$(z-a, z-a) = (z-b, z-b) \implies (z,z) - 2(a,z) + (a,a) = (z,z) - 2(z,b) + (b,b)$$

and thus $(z,a) - (z,b) = \frac{1}{2}(a,a) - \frac{1}{2}(b,b)$; so $(z - \frac{a+b}{2}, a-b) = 0$, and the two vectors are orthogonal. So every such z lies on the perpendicular bisector of the segment $[ab]$; and clearly every z on that line is an equal distance from a and b.

2. Let $v = 1+i$ and $z = x+iy$ for any real numbers x and y.

a. Show that the equation $|z-v| = |vz|$ represents a circle, and find its centre and radius.

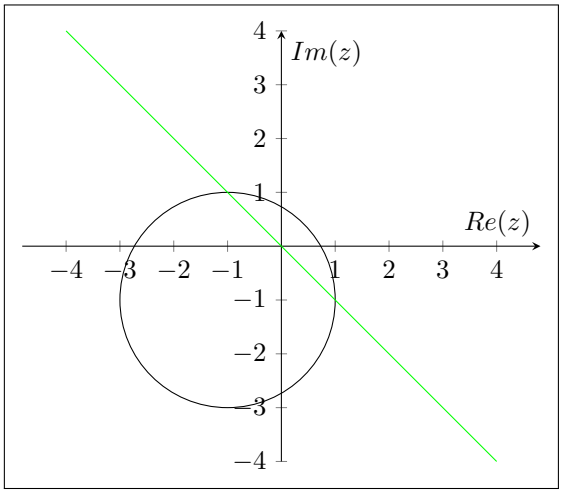
b. Find the point of intersection of the circle with the straight line $|z-v| = |z+v|$.

(a) Expanding using the distance formula, we have

$$\begin{aligned}|z-v| &= \sqrt{(x-1)^2 + (y-1)^2} \\ |vz| &= \big|(1+i)(x+iy)\big| \\ &= |x+iy+ix-y| \\ &= \sqrt{(x-y)^2 + (x+y)^2} \\ &= \sqrt{2x^2+2y^2} \\ &\Downarrow \\ (x-1)^2 + (y-1)^2 &= 2x^2 + 2y^2 \\ &\Downarrow \\ 0 &= x^2 + y^2 + 2x + 2y - 2 \\ &= (x+1)^2 + (y+1)^2 - 4 \text{ (completing the square).}\end{aligned}$$

Hence we have a circle centred on $(-1,-1)$ with a radius of 2.

(b)



Finding the equation of the line:

$$\begin{aligned}(x-1)^2+(y-1)^2 &= (x+1)^2+(y+1)^2\\ 0 &= 4x+4y\\ y &= -x.\end{aligned}$$

Substituting:

$$\begin{aligned}4 &= (x+1)^2+(1-x)^2\\ 1 &= x^2\\ x &= \pm 1\\ \implies y &= \mp 1\end{aligned}$$

So the line intersects the circle at $(-1,1)$ and $(1,-1)$.

3. Find the locus of all z such that for some fixed a, $z-a$ is perpendicular to $z+a$.

We have $(z-a, z+a) = 0$; so $(z,z) - (a,z) + (z,a) - (a,a) = 0$ and thus $(z,z) = (a,a)$. So $\sqrt{|z|} = \sqrt{|(|\, a)}$, and (since lengths are positive) $|z| = |a|$. In other words, we have a circle around zero of radius $|a|$.

4. Show that if u, v, and w are complex numbers, and if λ and μ are real numbers, then:

a. $(u,v) = (v,u)$

b. $(\lambda u + \mu v, w) = \lambda(u,w) + \mu(v,w)$

(a) $(u,v) = \mathfrak{Re}\,(u)\,\mathfrak{Re}\,(v) + \mathfrak{Im}\,(u)\,\mathfrak{Im}\,(v) = \mathfrak{Re}\,(v)\,\mathfrak{Re}\,(u) + \mathfrak{Im}\,(v)\,\mathfrak{Im}\,(u) = (v,u)$.

(b)

$$\begin{aligned}(\lambda u+\mu v,w) &= \mathfrak{Re}\,(\lambda u+\mu v)\,\mathfrak{Re}\,(w)+\mathfrak{Im}\,(\lambda u+\mu v)\,\mathfrak{Im}\,(w)\\ &= (\lambda\mathfrak{Re}\,(u)+\mu\mathfrak{Re}\,(v))\mathfrak{Re}\,(w)+(\lambda\mathfrak{Im}\,(u)+\mu\mathfrak{Im}\,(v))\mathfrak{Im}\,(w)\\ &= \lambda\mathfrak{Re}\,(u)\,\mathfrak{Re}\,(w)+\mu\mathfrak{Re}\,(v)\,\mathfrak{Re}\,(w)+\lambda\mathfrak{Im}\,(u)\,\mathfrak{Im}\,(w)+\mu\mathfrak{Im}\,(v)\,\mathfrak{Im}\,(w)\\ &= \lambda(\mathfrak{Re}\,(u)\,\mathfrak{Re}\,(w)+\mathfrak{Im}\,(u)\,\mathfrak{Im}\,(w))+\mu(\mathfrak{Re}\,(v)\,\mathfrak{Re}\,(w)+\mathfrak{Im}\,(v)\,\mathfrak{Im}\,(w))\\ &= \lambda(u,w)+\mu(v,w).\end{aligned}$$

5. Show that if b is a complex number and a and c are real numbers, then the locus of all complex numbers z satisfying $a(z,z)+(b,z)+c=0$ is a circle. (Hint: if z was real, you would complete the square.)

Indeed, we simply 'complete the square' but now with inner products instead of normal products:

$$\begin{aligned}0=a(z,z)+(b,z)+c=a(z+\frac{b}{2a},z+\frac{b}{2a})-\frac{(b,b)}{4a}+c\\ (z+\frac{b}{2a},z+\frac{b}{2a})=\frac{(b,b)-4ac}{4a^2}\\ \sqrt{(z+\frac{b}{2a},z+\frac{b}{2a})}=\sqrt{\frac{(b,b)-4ac}{4a^2}}\\ \left|z+\frac{b}{2a}\right|=\frac{\sqrt{(b,b)-4ac}}{2a}.\end{aligned}$$

So the locus is a circle of radius $\frac{\sqrt{(b,b)-4ac}}{2a}$ centred at $-\frac{b}{2a}$.

6. Let X be a set of complex numbers. If $\rho\neq 0$ and t are complex numbers, define $\rho X+t$ to be the set of all complex numbers of the form $\rho x+t$ for some x in the set X. Show that

a. if X is a line, then $\rho X+t$ is a line;

b. if X is a circle, then $\rho X+t$ is a circle.

Indeed, if X is a line then X is the set of all points of the form $\alpha z+c$ for some real number α and complex number c; so $\rho X+t$ is the set of all points of the form $\rho(\alpha z+c)+t=\rho\alpha z+\rho c$, which is the line in the direction ρz through the point ρc.

If X is a circle, then X is the locus of $|z-c|=r$ for some complex number c and some point r; then every point w in $\rho X+t$ satisfies $w=\rho z+t$ for some z in X, and so $z=\rho^{-1}(w-t)$; thus $\rho X+t$ is the locus of all w satisfying $\left|\rho^{-1}(w-t)-c\right|=r$. Applying properties of the modulus, we have that $\left|w-(t+\rho c)\right|=|\rho|\,r$, and so $\rho X+t$ is just the circle with centre $t+\rho c$ with radius $|\rho|\,r$.

7. Let p be a positive real number, and let Γ be the locus of points z satisfying $|z-p| = c\mathfrak{Re}(z)$. Show that Γ is:

a. an ellipse if $0 < c < 1$;

b. a parabola if $c = 1$;

c. a hyperbola if $c > 1$.

Let $z = x + yi$. Expanding, we have $(x-p)^2 + y^2 = c^2x^2$ and therefore $(1-c^2)x^2 - 2px + p^2 + y^2 = 0$. If $c = 1$, this is clearly the equation of the parabola $y^2 = 2px - p^2$; so assume $c \neq 1$. Dividing through by $1-c^2$ and completing the square, we have

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

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

where the coefficient of the $(x - p/(1-c^2))^2$ term is always positive and the coefficient of the y^2 term is positive when $c < 1$ and negative when $c > 1$, corresponding to an ellipse and a hyperbola respectively.

8. A set of complex numbers is called *convex* if for every pair of complex numbers in the set the line segment joining them is also in the set.

a. Show that the set of all z where $|z| < 1$ is convex.

b. Show that the set of all z where $0 < |z| < 1$ is not convex.

(a) Suppose w and v lie inside the disc $|z| < 1$. Then the segment joining them is given by $z = (1-t)w + tv$ (where $0 \leq t \leq 1$). Computing the modulus of this, we obtain

$$|z| = \big|(1-t)w + tv\big| \leq \big|(1-t)w\big| + |tv| = (1-t)|w| + t|v| < (1-t) + t = 1;$$

so every point in the segment also lies inside the disc.

(b) Consider the points $w = -1/2$ and $v = 1/2$. Then the segment between them is given by $z = (1-t)w + tv$, so the point $(1-(1/2))w + (1/2)v = (1/2)(-1/2) + (1/2)(1/2) = 0$ lies on the segment but not inside the given set.

9. A set of complex numbers is called *star shaped* if there is some point c in the set such that for every other point p in the set, the segment joining p to c lies in the set. Show that every convex set is star shaped.

If a set is convex, then pick any point c in the set; then the segment joining p to c lies inside the set (where p is any other point in the set) and so the set is star-shaped.

10. If S is a set of finitely many complex numbers $z_1, ..., z_n$, the *convex hull* of S is the smallest convex set containing every point of S. Show that a point w is in the convex hull of S precisely when there exist n non-negative real numbers, $\lambda_1, ..., \lambda_n$, such that $\lambda_1 + \cdots + \lambda_n = 1$, and

$$w = \lambda_1 z_1 + \cdots \lambda_n z_n.$$

The points w are called *convex combinations* of the z_i.

This is proved in two steps: we show that the given set is convex, and that it is contained in every other convex set containing S (so it is the smallest such set).

Suppose a and b lie inside the set; then $a = \lambda_1 z_1 + \cdots \lambda_n z_n$ and $b = \mu_1 z_1 + \cdots \mu_n z_n$ for some real numbers as restricted in the question. Consider the segment between them; any point z on the segment is of the form

$$\begin{aligned} z &= (1-t)(\lambda_1 z_1 + \cdots \lambda_n z_n) + t(\mu_1 z_1 + \cdots \mu_n z_n) \\ &= (\lambda_1 - t\lambda_1 + t\mu_1)z_1 + \cdots + (\lambda_n - t\lambda_n + t\mu_n)z_n. \end{aligned}$$

But the sum of the coefficients is

$$\begin{aligned} &(\lambda_1 - t\lambda_1 + t\mu_1) + \cdots + (\lambda_n - t\lambda_n + t\mu_n) \\ &\qquad = (\lambda_1 + \cdots + \lambda_n) - t(\lambda_1 + \cdots + \lambda_n) + t(\mu_1 + \cdots + \mu_1) \\ &\qquad\qquad = 1 - t + t = 1, \end{aligned}$$

and each coefficient is of the form $(1-t)\lambda_i + t\mu_i$ which lies on the segment of the real line joining λ_i to μ_i; since both of these are non-negative, the coefficient is non-negative. Thus z satisfies both criteria for its coefficients and lies inside the set; z is convex.

Now suppose we have any other convex set containing the n points. The claim is that any point $z = \lambda_1 z_1 + \cdots + \lambda_n z_n$ lies inside the convex set. Suppose every convex combination of this form where k coefficients are non-zero lies inside the set (the case $k = 2$ follows from convexity, because it is just a segment); consider convex combination $z = \lambda_1 z_1 + \cdots + \lambda_k z_k + \lambda_{k+1} z_{k+1}$ such that the first k coefficients are non-zero. Consider the point

$$\frac{\lambda_1 z_1 + \cdots + \lambda_k z_k}{\lambda_1 + \cdots + \lambda_k}$$

which has coefficient sum 1, so this point lies inside the convex set; and so the point

$$z = (\lambda_1 + \cdots + \lambda_k)\left(\frac{\lambda_1 z_1 + \cdots + \lambda_k z_k}{\lambda_1 + \cdots + \lambda_k}\right) + \lambda_{k+1} z_{k+1}$$

is a convex combination of two points in the set, and so lies inside the set. By induction, this holds for all k up to n; so the set of all convex combinations of $z_1, ..., z_n$ lies inside every other convex set containing the n points.

More generally, the convex hull of any set of points is the smallest convex set containing those points, and we have that the set of all points in the convex hull is the set of finite convex combinations of points in the set. However, it turns out that if we take our points in n-dimensional space then the convex

hull of a set can be described by the convex combinations of sets of $n+1$ points in the set. This theorem is due to Carathéodory (see [2], chapter 11).

11. The following inequality, which holds for all real numbers a_1, a_2, ..., a_n, b_1, ..., b_n, is known as the Cauchy-Schwarz inequality.

$$(a_1b_1+a_2b_2+\cdots+a_nb_n)^2 \leq (a_1^2+\cdots+a_n^2)(b_1^2+\cdots+b_n^2) \quad \text{(Cauchy-Schwarz)}$$

The inequality is a very useful result in analysis; there are several different elementary proofs of it.

a. Show that if $a > 0$, $ax^2 + bx + c \geq 0$ for all x if and only if $b^2 - 4ac \leq 0$.

b. Prove the Cauchy-Schwarz inequality by considering the expression $(a_1x + b_1)^2 + \cdots + (a_nx + b_n)^2$, collecting terms, and applying (a).

c. As a special case of the inequality, show that if w and z are complex numbers then $(w, z)^2 \leq |w|^2|z|^2$.

d. Hence show the *triangle inequality*: $|a + b| \leq |a| + |b|$ for complex numbers a and b.

(a) Use the quadratic formula.

(b) We rewrite in summation notation to make matters clearer; we simply write $\sum$ for $\sum_{i=1}^{n}$ to save space. Considering the suggested expression:

$$\sum(a_ix + b_i)^2 = \sum(a_i^2x^2 + 2a_ib_ix + b_i^2) = x^2\sum a_i^2 + 2x\sum a_ib_i + \sum b_i^2.$$

But $\sum a_i^2 \geq 0$ (since each a_i is real and so has non-negative square); by the same reasoning, $\sum(a_ix + b_i)^2$ is non-negative and hence so is the right-hand side of the above equality. Hence we can apply (a), and conclude that

$$\left(2\sum a_ib_i\right)^2 - 4\left(\sum a_i^2\right)\left(\sum b_i^2\right) \geq 0;$$

expanding and rearranging, we find the required result:

$$\left(\sum a_ib_i\right)^2 \geq \left(\sum a_i^2\right)\left(\sum b_i^2\right).$$

(c) We have

$$(w, z)^2 = (\mathfrak{Re}\,(w)\,\mathfrak{Re}\,(z)+\mathfrak{Im}\,(w)\,\mathfrak{Im}\,(z))^2 \leq (\mathfrak{Re}\,(w)^2+\mathfrak{Im}\,(w)^2)(\mathfrak{Re}\,(z)^2+\mathfrak{Im}\,(z)^2) = |w|^2|z|^2\,.$$

(d)

$$|a + b|^2 = (a+b, a+b) = (a, a)+2(a, b)+(b, b) = |a|^2+2(a, b)+|b|^2 \leq |a|^2+2|a||b|+|b|^2 = (|a|+|b|)^2;$$

the result follows by taking square roots.

12. Multiplication by i rotates a point by $\frac{\pi}{2}$ around the origin.

a. A generalisation of this allows us to rotate a point z around an arbitrary point a by that angle: $z' = a + i(z - a)$. Justify this formula.

b. Consider a treasure map with the following instructions:

> **From the statue of Richard Seddon, go to the kauri tree (counting your steps), and then turn exactly 90°left and walk the same number of steps to the point g'. Returning to the statue, walk to the beech tree (again counting your steps). Turn right by 90°, and walk the same number of steps to point g''. The treasure is buried exactly at the midpoint of the line joining g' and g''.**

Given that the kauri tree is at $(0, 0)$, the beech tree is at $(10, 0)$, and the statue is somewhere on the line $y = 2009$, find the location of the treasure.

(a) We shift our coordinate system so that a becomes the origin, rotate the plane by multiplying by i, and shift the origin back to a.

(b) We will call the x-coordinate of the statue x_0.

Our technique for solving this problem is simply to rotate the point representing the statue around the given points for the trees by 90°using the formula given in the question — then finding the midpoint is simple.

First, we rotate $x_0 + 2009i$ around the point $0 + 0i$, obtaining $g' = -2009 + ix_0$. We next rotate the statue around $10 + 0i$ three times (as we are turning right — draw a diagram!) using the formula:

$$\begin{aligned} 10 + i(x_0 + 2009i - 10) &= -1999 + i(x_0 - 10) \\ 10 + i(-1999 + i(x_0 - 10) - 10) &= 20 - x_0 - 2009i \\ 10 + i(20 - x_0 - 2009i - 10) &= 2019 + i(10 - x_0) \end{aligned}$$

The midpoint is therefore $\left(\frac{-2009+2019}{2}, \frac{x_0+10-x_0}{2}\right) = (5, 5)$. Interestingly, the position of the treasure does not depend on the x-coordinate of the statue!

13. A *Gaussian integer* is a complex number of the form $m+ni$, for integers m and n. Show that there is no equilaterial triangle on the complex plane with Gaussian integer vertices.

Suppose we have such an equilateral triangle; without loss of generality, we can take one of the vertices to be the origin. Let the other two vertices be $a+bi$ and $c+di$. Since the triangle is equilateral, $|a+bi| = |c+di|$. Further, the angle between the two points at the origin is $\frac{\pi}{3}$. Then, by the rotation property of complex multiplication,

$$a+bi = \operatorname{cis}\frac{\pi}{3}(c+di) = \frac{1}{2}c + \frac{\sqrt{3}}{2}di;$$

hence $b = d\sqrt{3}/2$, which is irrational if d is an integer (contradiction).

14. A line in $\mathbb{C}^2$ (the plane with complex coordinates) is defined to be the locus of a linear $ax + by + c = 0$ where a, b, and c are complex constants. Prove that, given two distinct points (x_0, y_0) and (x_1, y_1) in $\mathbb{C}^2$, there is a unique line through those two points. *Hint: it is certainly not true that there is a unique linear equation whose graph includes both points.*

Let $\mathcal{L}$ and $\mathcal{M}$ be two lines passing through both points. (Our goal is to show that $(x, y) \in \mathcal{L} \iff (x, y) \in \mathcal{M}$.) Then $\mathcal{L}$ is the locus of some linear equation $ax + by + c = 0$, and $\mathcal{M}$ is the locus of some other linear equation $dx + ey + f = 0$.

Consider first $\mathcal{L}$. We know that $(x_0, y_0) \in \mathcal{L} \wedge (x_1, y_1) \in \mathcal{L}$. Hence we have the following system of simultaneous equations:

$$\begin{aligned} ax_0 + by_0 + c &= 0 \\ ax_1 + by_1 + c &= 0. \end{aligned}$$

Since we have a system of rank two with three variables, one variable must be free (a parameter); we chose it to be c as this simplifies the whole process. Our goal, therefore, is to rewrite $ax + by + c = 0$ in terms of c only (the purpose of this goal may not be clear at this point, but trust us). This can be done using any appropriate method (e.g. substitution); we chose to use linear algebra because it minimises the amount of tedious work required.

Readers who do not know linear algebra should feel free to skip this portion of the solution, and are encouraged to find another way to derive the same result.

We have

$$\begin{bmatrix} x_0 & y_0 \\ x_1 & y_1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} -c \\ -c \end{bmatrix}.$$

Inverting the coefficient matrix and solving for $(a\ b)^t$ gives

$$\begin{bmatrix} a \\ b \end{bmatrix} = \frac{1}{x_0y_1 - x_1y_0} \begin{bmatrix} y_1 & -y_0 \\ -x_1 & x_0 \end{bmatrix} \begin{bmatrix} -c \\ -c \end{bmatrix};$$

We therefore conclude that

$$\begin{aligned} a &= -\frac{c}{x_0y_1 - x_1y_0}(y_1 - y_0) \\ b &= -\frac{c}{x_0y_1 - x_1y_0}(x_0 - x_1) \end{aligned}$$

and (substituting) $\mathcal{L}$ is the locus of

$$c\left(1 - \frac{y_1 - y_0}{x_0y_1 - x_1y_0}x - \frac{x_0 - x_1}{x_0y_1 - x_1y_0}y\right) = 0.$$

Similarly, $\mathcal{M}$ is the locus of

$$f\left(1 - \frac{y_1 - y_0}{x_0y_1 - x_1y_0}x - \frac{x_0 - x_1}{x_0y_1 - x_1y_0}y\right) = 0.$$

Now, we must show that if a point $(x_\star, y_\star)$ is in $\mathcal{L}$ then it is in $\mathcal{M}$ (and vice versa). To this end, consider the following:

$$(x_\star, y_\star) \in \mathcal{L} \iff c\left(1 - \frac{y_1 - y_0}{x_0 y_1 - x_1 y_0} x_\star - \frac{x_0 - x_1}{x_0 y_1 - x_1 y_0} y_\star\right) = 0$$

So one of $c = 0$ and $\left(1 - \frac{y_1 - y_0}{x_0 y_1 - x_1 y_0} x_\star - \frac{x_0 - x_1}{x_0 y_1 - x_1 y_0} y_\star\right) = 0$ is true.

Case I: $\left(1 - \frac{y_1 - y_0}{x_0 y_1 - x_1 y_0} x_\star - \frac{x_0 - x_1}{x_0 y_1 - x_1 y_0} y_\star\right) = 0$
Evidently

$$f\left(1 - \frac{y_1 - y_0}{x_0 y_1 - x_1 y_0} x_\star - \frac{x_0 - x_1}{x_0 y_1 - x_1 y_0} y_\star\right) = 0$$

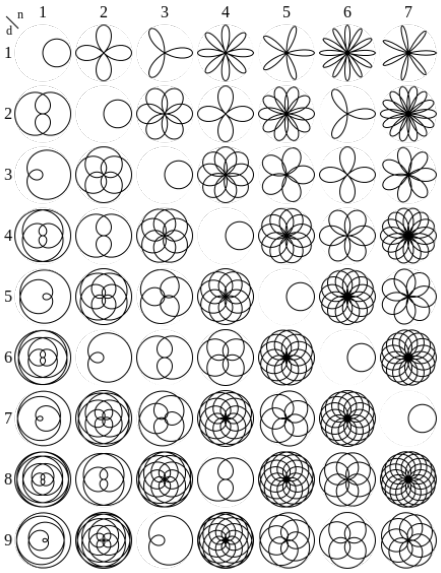
and so $(x_\star, y_\star) \in \mathcal{M}$. (The same argument works with $\mathcal{M}$ and $\mathcal{L}$ swapped.)

Case II: $c = 0$ **and** $\left(1 - \frac{y_1 - y_0}{x_0 y_1 - x_1 y_0} x_\star - \frac{x_0 - x_1}{x_0 y_1 - x_1 y_0} y_\star\right) \neq 0$
In both cases,

$$f\left(1 - \frac{y_1 - y_0}{x_0 y_1 - x_1 y_0} x_\star - \frac{x_0 - x_1}{x_0 y_1 - x_1 y_0} y_\star\right) = 0$$

and so $(x_\star, y_\star) \in \mathcal{M}$. The above arguments also show that $(x_\star, y_\star) \in \mathcal{M} \implies (x_\star, y_\star) \in \mathcal{L}$, so $\mathcal{M} = \mathcal{L}$.

15. Investigate the locus of $\left\{z = r \operatorname{cis}\theta : r = \cos\left(\frac{n}{d}\theta\right)\right\}$ for different values of n and d.



(Image: Jason Davies [CC BY-SA 3.0 (https://creativecommons.org/licenses/by-sa/3.0)], from Wikimedia Commons)

6 Roots of Unity

Many of the results here follow from basic results in number theory. The interested reader is directed towards 'Elementary Number Theory' by Underwood Dudley [5]. More generally, the material in this chapter develops the theory of finite cyclic groups (the nth roots of unity under multiplication form a group isomorphic to the finite cyclic group of order n).

1. Let $p(z) = z^5 - 1$.

a. Find exactly each of the roots of $p(z)$.

b. Let α be the root of p with the smallest non-zero positive argument. Show explicitly that the roots can be written as 1, α, α^2, α^3, and α^4.

(a) The five roots will be symmetrical around the x-axis with angles of $\frac{2\pi}{5}$ separating them:

Root	**Polar form**
z_0	$\operatorname{cis} 0$
z_1	$\operatorname{cis} \frac{2\pi}{5}$
z_2	$\operatorname{cis} \frac{-2\pi}{5}$
z_3	$\operatorname{cis} \frac{4\pi}{5}$
z_4	$\operatorname{cis} \frac{-4\pi}{5}$

(b) In this case, we use de Moivre's Theorem:
$z_0 = \alpha^0 = \operatorname{cis} 0 \times \frac{2\pi}{5} = 1$;
$z_1 = \alpha^1 = \operatorname{cis} 1 \times \frac{2\pi}{5} = \operatorname{cis} \frac{2\pi}{5}$;
$z_2 = \alpha^4 = \operatorname{cis} 4 \times \frac{2\pi}{5} = \operatorname{cis} \frac{8\pi}{5} = \operatorname{cis} \frac{-2\pi}{5}$;
$z_3 = \alpha^2 = \operatorname{cis} 2 \times \frac{2\pi}{5} = \operatorname{cis} \frac{4\pi}{5} = \operatorname{cis} \frac{4\pi}{5}$; and
$z_4 = \alpha^3 = \operatorname{cis} 3 \times \frac{2\pi}{5} = \operatorname{cis} \frac{6\pi}{5} = \operatorname{cis} \frac{-4\pi}{5}$.

We could also use the result in exercise 14 (since $z_1 = \alpha$ is the 5th root of unity with smallest positive argument, it is primitive and so generates all the 5th roots of unity).

2. Find all solutions of $z^3 + n = 0$, where n is a positive real number, in exact form in terms of n.

Note that $n = n \operatorname{cis} 0$ and so $-n = n \operatorname{cis} \pi$.

$$\begin{aligned} z^3 &= -n \\ z &= n^{\frac{1}{3}} \operatorname{cis}\left(\pi + \frac{2n\pi}{3}\right) \\ &= \sqrt[3]{n} \operatorname{cis}\left(\pi + \frac{2n\pi}{3}\right) \qquad (0 \leq n < 3) \end{aligned}$$

So $z_0 = \sqrt[3]{n} \operatorname{cis} \pi$, $z_1 = \sqrt[3]{n} \operatorname{cis} \frac{5\pi}{3}$, $z_2 = \sqrt[3]{n} \operatorname{cis} \frac{\pi}{3}$ are the three roots.

3. Solve for z if $(z-3)^7 = 1$.

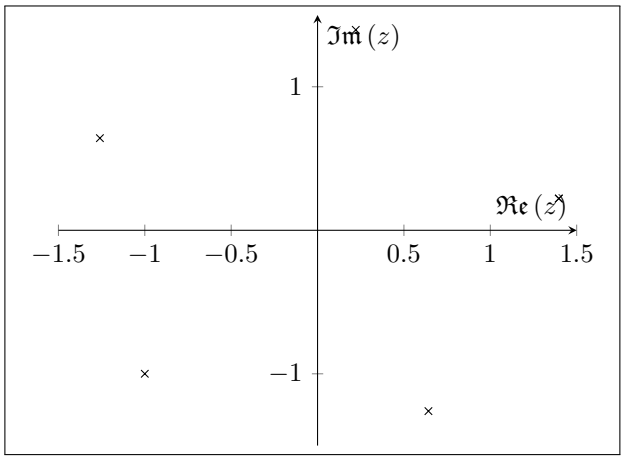
Root	Polar form
$z_0 - 3$	$\operatorname{cis} 0$
$z_1 - 3$	$\operatorname{cis} \frac{2\pi}{7}$
$z_2 - 3$	$\operatorname{cis} \frac{-2\pi}{7}$
$z_3 - 3$	$\operatorname{cis} \frac{4\pi}{7}$
$z_4 - 3$	$\operatorname{cis} \frac{-4\pi}{7}$
$z_5 - 3$	$\operatorname{cis} \frac{6\pi}{7}$
$z_6 - 3$	$\operatorname{cis} \frac{-6\pi}{7}$

Then simply convert each root to rectangular form and add 3.

4. Find the fifth roots of $4+4i$ in polar form, and draw them on an Argand diagram. Hence find integers p and q such that $(p+qi)^5 = (4+4i)$.

Note that $4+4i = 4\sqrt{2}\operatorname{cis}\frac{\pi}{4}$. We therefore compute $\sqrt[5]{4\sqrt{2}\operatorname{cis}\frac{\pi}{4}} = \sqrt[10]{32}\operatorname{cis}\left(\frac{\pi}{20} + \frac{2n\pi}{5}\right)$ for $0 \le n < 5$:

Root	Polar form
z_1	$\sqrt{2}\operatorname{cis}\frac{\pi}{20}$
z_2	$\sqrt{2}\operatorname{cis}\frac{9\pi}{20}$
z_3	$\sqrt{2}\operatorname{cis}\frac{17\pi}{20}$
z_4	$\sqrt{2}\operatorname{cis}\frac{5\pi}{4}$
z_5	$\sqrt{2}\operatorname{cis}\frac{33\pi}{20}$



Hence the required integer values are $p = q = -1$.

5. Write down all of the primitive sixth roots of unity. What about the primitive fifth roots of unity?

Let $\alpha = \operatorname{cis} \frac{2\pi}{6}$. Then the sixth roots of unity are:

Root	Polar form
z_0	$\operatorname{cis} 0$
z_1	$\operatorname{cis} \frac{2\pi}{6} = \operatorname{cis} \frac{\pi}{3}$
z_2	$\operatorname{cis} \frac{4\pi}{6} = \operatorname{cis} \frac{2\pi}{3}$
z_3	$\operatorname{cis} \frac{6\pi}{6} = \operatorname{cis} \frac{2\pi}{2}$
z_4	$\operatorname{cis} \frac{8\pi}{6} = \operatorname{cis} \frac{4\pi}{3}$
z_5	$\operatorname{cis} \frac{10\pi}{6} = \operatorname{cis} \frac{5\pi}{3}$

It is clear that z_2 and z_4 are third roots of unity, and that z_3 is a square root of unity. This just leaves z_1 and z_5 as primitive sixth roots of unity.

The primitive fifth roots of unity are all the fifth roots of unity (except 1 itself); more generally, the primitive pth roots of unity (p prime) are all the pth roots of unity (again, excluding 1).

6. a. Let α be a complex root of $x^3 = 1$. Show by computation that $\alpha^2 + \alpha + 1 = 0$.

b. In general, prove that the sum of all n nth roots of unity is zero (for $n > 1$).

(a) We have that $(x-1)$ is a root of the polynomial; by long division, x^2+x+1 is the quadratic factor. Since $\alpha \neq 1$, it must be a root of this quadratic; and so $\alpha^2 + \alpha + 1 = 0$.

$$
\begin{array}{r|l}
x-1 & \begin{array}{r} x^2 + x + 1 \\ \hline x^3 \qquad\quad -1 \\ -x^3 + x^2 \\ \hline x^2 \\ -x^2 + x \\ \hline x - 1 \\ -x + 1 \\ \hline 0 \end{array}
\end{array}
$$

This demonstrates that the sum of all three third roots of unity is zero, and the same technique can be used for (b).

(b) Let ω be a primitive nth root of unity. Then all the nth roots of unity are given by $\omega^0, \omega^1, \ldots, \omega^{n-1}$. Also note that $0 = \omega^n - 1 = (\omega - 1)(1 + \omega + \cdots + \omega^{n-1})$. But ω is primitive, and so in particular is not equal to one. So we can divide through by $(\omega - 1)$ to obtain the required result.

Geometrically, this result can also be seen by drawing a diagram and taking vector sums.

7. Find the product of all n nth roots of unity.

Suppose $\{\omega_0, \omega_1, \ldots, \omega_{n-1}\}$ are the nth roots of unity, where $\omega_k = \operatorname{cis}\left(\frac{2k\pi}{n}\right)$. Then:

$$\begin{aligned}\prod_{k=0}^{k<n} \operatorname{cis}\left(\frac{2k\pi}{n}\right) &= \operatorname{cis}\left(\sum_{k=0}^{k<n} \frac{2k\pi}{n}\right) \\ &= \operatorname{cis}\left(\frac{2\pi}{n} \cdot \frac{(n-1)n}{2}\right) \\ &= \operatorname{cis}\big((n-1)\pi\big) \\ &= \cos\big((n-1)\pi\big) \\ &= (-1)^{n-1}.\end{aligned}$$

8. Solve $(z+1)^3 = 8$ for z and show that the sum of the solutions is -3.

Rearranging, we find that $(z+1)^3 - 8 = z^3 + 3z^2 + 3z - 7$. Since 1 is a solution ($2^3 = 8$), we divide through.

$$\begin{array}{r|l} & z^2 + 4z + 7 \\ \hline z-1 & z^3 + 3z^2 + 3z - 7 \\ & \underline{-z^3 + z^2} \\ & 4z^2 + 3z \\ & \underline{-4z^2 + 4z} \\ & 7z - 7 \\ & \underline{-7z + 7} \\ & 0 \end{array}$$

We do not have to solve this quadratic if we recall that $(x-\alpha)(x-\beta) = x^2 - (\alpha+\beta) + \alpha\beta$, and so the sum of the two solutions will be the negative of the coefficient of the x term - namely -4. Hence the sum of all three solutions will be $-4 + 1 = -3$.

9. Given that $a = b + kn$ for some integer k, show that $z^a = z^b$ where z is a primitive nth root of unity.

$$\begin{aligned}z^a &= z^{b+kn} \\ &= z^b z^{kn} \\ &= z^b \left(z^n\right)^k \\ &= z^b (1)^k = z^b.\end{aligned}$$

10. Prove that the product of an ath root of unity by a bth root of unity is an abth root of unity.

Suppose that $\omega^a = 1$ and $\zeta^b = 1$. Then $(\omega\zeta)^{ab} = (\omega^{ab})(\zeta^{ab}) = 1^b 1^a = 1$.

11. Prove the following: Let a and b be coprime integers. Then all the abth roots of unity can be obtained as products of ath roots of unity and bth roots of unity. *Hint: for all integers a and b there exist integers m and n such that $am + bn = \gcd(a, b)$.*

Suppose a and b are coprime integers. Then there exist integers m and n such that

$$k(am + bn) = k \gcd(a, b) = k,$$

for all natural numbers k.

Now, suppose $\operatorname{cis} \frac{2\pi k}{ab}$ is an abth root of unity, where $0 \leq k < ab$. It is obvious that every abth root of unity can be written in this form.

Consider, then, the following:

$$\begin{aligned} \operatorname{cis} \frac{2\pi k}{ab} &= \operatorname{cis} \left(\frac{2\pi am + 2\pi bn}{ab} \right) \\ &= \operatorname{cis} \left(\frac{2\pi m}{b} + \frac{2\pi n}{a} \right) \\ &= \operatorname{cis} \frac{2\pi m}{b} \times \operatorname{cis} \frac{2\pi n}{a}, \end{aligned}$$

where the right hand side is clearly the product of a bth root of unity by an ath root of unity.

12. The theorem stated in this section requires ω to be a primitive nth root of unity in order for all the nth roots of unity to be powers of ω. Why do we need this restriction?

For convenience, the theorem is restated here:

Theorem. *Given the polynomial $z^n = 1$, with primitive root ω, all solutions are given by ω^k for $0 \leq k \leq (n-1)$. In other words, the integer powers of a primitive nth root of unity must be* all *the nth roots of unity.*

The theorem is false without this restriction. For example, the fourth roots of unity include the second roots of unity, and therefore the principal second root of unity (-1). However, the primitive second root of unity will not produce the primitive fourth roots of unity when raised to a natural power (otherwise the primitive fourth roots of unity would also be second roots of unity by the theorem, which is obviously false).

Assume that we don't include the restriction; we show that a contradiction results. In general, the nth principal roots of unity will be contained within the mnth roots of unity for $m \in \mathbb{N}$. Hence, without the restriction, we would be claiming that the nth principal roots of unity (which are also mnth roots of unity) would generate the mnth principal roots of unity. Say that we take ω to be an nth principal root of unity, and take ξ to be an mnth principal root of unity. Then, without the restriction, $\omega^k = \xi$ for some natural number k, and so (by the theorem in the text) ξ is also an nth root of unity. But by definition, principal roots of unity cannot also be roots of unity for lower powers — and n is obviously a lower power than mn. Hence the restriction must be included for the theorem to hold.

Note that this reasoning also implies that the nth powers of unity for prime n are all principal (apart from the trivial root $z = 1$), since they do not include lower powers!

13. Prove the following: Let a and b be relatively prime integers. Then $x^a - 1 = 0$ and $x^b - 1 = 0$ have only the trivial root $x = 1$ in common.

Suppose $x^a - 1 = 0$ and $x^b - 1 = 0$. So $x = \operatorname{cis} \frac{2\pi m}{a} = \frac{2\pi n}{b}$ for some integers m and n. This implies that $(\operatorname{cis} \frac{2\pi n}{b})^a = 1$, and so $\operatorname{cis} \frac{2\pi an}{b} = 1$. Hence $\frac{an}{b}$ is an integer, and therefore b divides an. Likewise, a divides bm. Since a and b are coprime, we must have a divides m and b divides n. Hence $m = ap$ and $n = bq$ for some integers p and q. Therefore we have

$$x = \operatorname{cis} \frac{2\pi n}{b} = \operatorname{cis} 2\pi q = 1.$$

14. a. Prove the converse of the theorem in the text: i.e. show that if ζ generates all the kth roots of unity then it is a primitive kth root of unity.

b. Let ζ be the root of $p(x) = x^k - 1$ with smallest positive argument. Show that ζ is a primitive kth root of unity.

(a) Suppose (in order to obtain a contradiction) that ζ generates all the kth roots of unity but is *not* a primitive kth root of unity. Then there exists some n $(0 < n < k)$ such that $\zeta^n = 1$. Let α be an arbitrary kth root of unity. By the definition of ζ, there is some j such that $\alpha = \zeta^j$. Then $\alpha^n = (\zeta^j)^n = \zeta^{jn} = (\zeta^n)^j = 1^j = 1$. But this shows that every kth root of unity is also an nth root of unity for some $n < k$, which is plainly false; so our assumption that $\zeta^n = 1$ must be false, and ζ must be a primitive root of unity.

(b) We must show that $\zeta^n \neq 1$ for all $0 < n < k$. Recall that the kth roots of unity are given by $z_j = \operatorname{cis} \frac{2\pi j}{k}$ for integral j; we have the smallest possible positive argument, so $\zeta = z_1 = \operatorname{cis} \frac{2\pi}{k}$. But this obviously generates all the kth roots of unity ($z_j = \operatorname{cis} \frac{2\pi j}{k} = \zeta^j$), and so by part (a) it is primitive.

15. Let α be the kth root of unity with smallest positive argument. Show that the primitive kth roots of unity are precisely α^a where $0 < a < k$ and $\gcd(a, k) = 1$. *Hint: for all integers a and b there exist integers m and n such that $am + bn = \gcd(a, b)$.*

Suppose that α^a is such that $0 < a < k$ and $\gcd(a, k) = 1$. Let α^b be a kth root of unity (we know that all the roots of unity are of this form by exercise 14). Then by Bézout's identity we have that there exist m and n such that $am + kn = 1$ and therefore $bam + bkn = b$. Hence

$$\alpha^b = \alpha^{bam+bkn} = (\alpha^a)^{bm}(\alpha^k)^{bn} = (\alpha^a)^{bm}.$$

Hence every power of α is a power of α^a, and so every kth root of unity is a power of α^a, implying (by exercise 14) that α^a is a primitive root of unity.

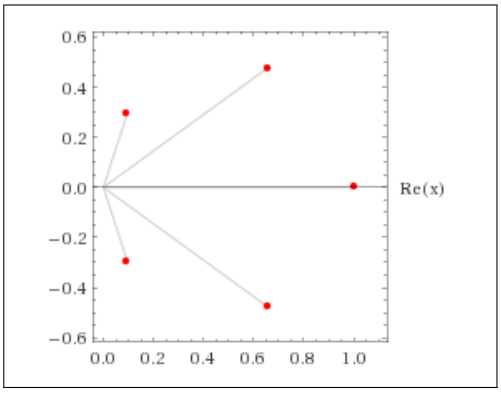
On the other hand, suppose that $\gcd(a, k) = d \neq 1$. Then $k/d < k$ is an integer and $a/d < k$ is an integer. Hence $(\alpha^a)^{k/d} = (\alpha^k)^{a/d} = 1$, so α^a has is a (k/d)th root of unity — but $k/d < k$, so α^a cannot be a primitive kth root of unity.

16. The fifth-degree polynomial $p(x)$, where $p(k) = 0$, has as its roots the vertices of a regular pentagon centred around $(\frac{1}{2}k, 0)$. Give $p(x)$ such that all coefficients are real.

There are two ways to solve this problem. One method is to geometrically find each root and then form $p(x) = (x - k)(x - \alpha_2)...(x - \alpha_5)$, but this method is tedious.

The second method is to simply notice that this is a transformed root of unity question, and so $p(x)$ will be of the form $a^5 - b$ for some a and b. We first make the problem easier, by shifting the pentagon back to the origin. Call this polynomial $q(x)$. We know that $q(x) = x^5 - c$ for some constant c, and that $q(\frac{k}{2}) = 0$ (since we shift k left by $\frac{k}{2}$ to get from the roots of p to the roots of q) — hence $c = \frac{k^5}{32}$.

In order to shift the roots to the right, we simply shift $q(x)$ to the right by $\frac{k}{2}$ by subtracting $\frac{1}{2}k$ from x when it occurs. Hence $p(x) = (x - \frac{k}{2}k)^5 - \frac{k^5}{32}$. Graphing this when $k = 1$, we obtain the following Argand diagram of the roots, which is a pentagon centred around $x = 0.5$ with radius 1 as expected.



17. Show that all solutions to $(z+1)^n = z^n$ lie on the line $\mathfrak{Re}(z) = -\frac{1}{2}$.

$$\begin{aligned} 1 &= \left(\frac{z+1}{z}\right)^n \\ &= \left(1+\frac{1}{z}\right)^n. \end{aligned}$$

Now, let $1 + \frac{1}{z} = r\,\mathrm{cis}\,\theta$. This implies that $r = 1$ and $\theta = \frac{2\pi k}{n}$, for some integer k:

$$\begin{aligned} 1+\frac{1}{z} &= \mathrm{cis}\,\frac{2\pi k}{n} \\ &= \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n} \\ &= 1 - 2\sin^2\frac{\pi k}{n} + 2i\sin\frac{\pi k}{n}\cos\frac{\pi k}{n} \\ \frac{1}{z} &= 2i\sin\frac{\pi k}{n}\left(\cos\frac{\pi k}{n} + i\sin\frac{\pi k}{n}\right) \\ z &= \frac{1}{2i\sin\frac{\pi k}{n}\left(\cos\frac{\pi k}{n} + i\sin\frac{\pi k}{n}\right)} \\ &= \frac{1}{2i\sin\frac{\pi k}{n}\,\mathrm{cis}\,\frac{\pi k}{n}} \\ &= \frac{\mathrm{cis}\,\frac{-\pi k}{n}}{2i\sin\frac{\pi k}{n}} \\ &= \frac{\cos\frac{\pi k}{n} - \sin\frac{-\pi k}{n}}{2i\sin\frac{\pi k}{n}} \\ &= \frac{\cos\frac{\pi k}{n}}{2i\sin\frac{\pi k}{n}} - \frac{i\sin\frac{\pi k}{n}}{2i\sin\frac{\pi k}{n}} \\ &= \frac{\cos\frac{\pi k}{n}}{2i\sin\frac{\pi k}{n}} - \frac{1}{2} \end{aligned}$$

so $\mathfrak{Re}(z) = -\frac{1}{2}$, as required.

18. Find all the third roots of 2.

We have that $\sqrt[3]{2} = 1.259992...$ is one third root of 2. The other two will be $\alpha\sqrt[3]{2} = \sqrt[3]{2}\,\mathrm{cis}\,\frac{2\pi}{3}$ and $\alpha^2\sqrt[3]{2} = \sqrt[3]{2}\,\mathrm{cis}\,\frac{4\pi}{3}$.

19. A *group* is a set G together with some operation $\cdot$ satisfying the following:

(a) For all a, b in G, $a \cdot b$ is in G.

(b) For all a, b, c in G, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

(c) There is some element e in G such that for all a in G, $a \cdot e = a$.

(d) For every element a in G there is some b in G such that $a \cdot b = e$.

Show that the set of all nth roots of unity form a group under multiplication.

(a) Suppose a and b are nth roots of unity. Then $(ab)^n = a^n b^n = 1$, so ab is also an nth root of unity.

(b) This follows from the associativity of multiplication of complex numbers in general (which in turn follows from associativity of multiplication of reals).

(c) Obviously $e = 1$.

(d) Suppose a is an nth root of unity. Then a^{-1} is also an nth root of unity ($(a^{-1})^n = (a^n)^{-1} = 1$), and $aa^{-1} = 1$. Hence a^{-1} is the required b.

20. Suppose $\sigma(n)$ is the function that sends n to the sum of its divisors. For example, the divisors of 4 are 1, 2, and 4; so $\sigma(4) = 1 + 2 + 4 = 7$. Prove that if p is prime then $\sigma(p^n) = \frac{p^{n+1}-1}{p-1}$.

The divisors of p^n are simply $1,\ p,\ p^2, \ldots,\ p^n$. Hence $\sigma(n) = 1 + p + \cdots + p^n = \frac{p^{n+1}-1}{p-1}$. Note here that we are viewing this sum as a polynomial in a known number p rather than an indeterminant x.

7 The Double-Triangle Problem

There are no exercises for this section that require worked answers.

8 Solving the Cubic

1. Check the author's algebra.

If the reader is expecting a solution to this problem, she is missing the point.

2. Solve $t^3 + t^2 - 89t + 231 = 0$.

We have $\sigma_1 = -1$, $\sigma_2 = -89$, and $\sigma_3 = -231$. Hence, following the method, we have $uv = ((-1)^2 - 3(-89))^3 = 19248832$ and $u + v = 2(-1)^3 - 9(-1)(-89) + 27(-231) = -7041$. Hence, we have

$$u, v = \frac{-7041 \pm \sqrt{(-7041)^2 - 4(19248832)}}{2}$$

and, plugging these values directly in, we have

$$x = \frac{1}{3}\left(-1 + \sqrt[3]{\frac{-7041 + \sqrt{(-7041)^2 - 4(19248832)}}{2}} + \sqrt[3]{\frac{-7041 - \sqrt{(-7041)^2 - 4(19248832)}}{2}}\right)$$

$$y = \frac{1}{3}\left(-1 + \alpha\sqrt[3]{\frac{-7041 + \sqrt{(-7041)^2 - 4(19248832)}}{2}} + \alpha^2\sqrt[3]{\frac{-7041 - \sqrt{(-7041)^2 - 4(19248832)}}{2}}\right)$$

$$z = \frac{1}{3}\left(-1 + \alpha^2\sqrt[3]{\frac{-7041 + \sqrt{(-7041)^2 - 4(19248832)}}{2}} + \alpha\sqrt[3]{\frac{-7041 - \sqrt{(-7041)^2 - 4(19248832)}}{2}}\right)$$

So (the author confidently exclaims, after wrestling with his calculator for several minutes) $x = 7$, $y = -11$, and $z = 3$. It is up to the reader to verify that these are indeed solutions of the original polynomial.

3. Solve $t^3 + 21t^2 - 32t + 3510 = 0$.

We have $\sigma_1 = -21$, $\sigma_2 = -32$, $\sigma_3 = -3510$. So $u + v = -119340$ and $uv = 154854153$. The engineers and physicists among the readers may be tempted to round off, but this feeling must be controlled.

After plugging everything into the quadratic formula, followed by the cubic formula, we obtain the three roots $t \in \{-27, 3 + 11i, 3 - 11i\}$.

4. Solve $2t^3 + 4it^2 + 58t - 84i$.

We have $\sigma_1 = -2i$, $\sigma_2 = 29$, and $\sigma_3 = 42i$. Hence $u + v = 1672i$ and $uv = -753571$.

We calculate the roots as $t \in \{-7i, 2i, 3i\}$, noting that we need to take all nine possible combinations of roots, checking to see which three actually work in the original equation.

5. In 1225, Leonardo of Pisa (Fibonacci) was asked by Holy Roman Emperor Frederick II to solve the cubic equation $x^3+2x^2+10x=20$. His solution was

$$x = 1 + \frac{22}{60} + \frac{7}{60^2} + \frac{42}{60^3} + \frac{33}{60^4} + \frac{4}{60^5} + \frac{40}{60^6}.$$

a. Show that the equation has exactly one real root.

b. Use the method outlined in this section to find numerical approximations to the three roots of the polynomial.

(a) We wish to show that the graph of $y = x^3 + 2x^2 + 10x - 20$ crosses the x-axis exactly one time. We find that $\frac{dy}{dx} = 3x^2 + 4x + 10$ has no real roots, and so the graph of y has no turning points. Since y is continuous, it must be strictly increasing and therefore crosses the x-axis exactly once.

(b) This question is nasty.

$\sigma_1 = -2$, $\sigma_2 = 10$, $\sigma_3 = 20$.

$$\begin{aligned} u + v &= 704 \\ uv &= -17576 \end{aligned}$$

$$\begin{aligned} u &\approx 728.1383 \\ v &\approx -24.13827 \end{aligned}$$

Possible roots:

	1	ω	ω^2
1	1.368808	$2.813822 - 0.8342792i$	$2.813822 + 0.8342792i$
ω	$-3.129418 + 2.597052i$	$-1.68404 + 1.762773i$	$-1.68404 + 3.431332i$
ω^2	$-3.129418 - 2.597052i$	$-1.68404 - 3.431332i$	$-1.68404 + -.762773i$

6. Solve $t^3 - 15t - 4 = 0$ using the methods outlined in this section. See exercise 33 from the section on complex numbers.

$\sigma_1 = -2$, $\sigma_2 = 10$, $\sigma_3 = 20$.

$$\begin{aligned} u + v &= 108 \\ uv &= 91125 \end{aligned}$$

The working roots are $t \in \{4, -2 + \sqrt{3}, -2 - \sqrt{3}\}$.

7. Verify that uv and $u+v$ are symmetric in x, y, and z.

This can be done by expanding both expressions out in terms of x, y, and z (the expressions themselves are given in the text, σ_k terms can be substituted out) and checking that for each type of term, all possible combinations of the three variables occur. For example, if xy occurs then xz and yz must also appear.

8. Read the historical introduction of Ian Stewart's *Galois Theory*.

For bonus marks, read the book and list all the typoes[4].

9. The discriminant of the general quartic equation $q(x) = A(x-\alpha)(x-\beta)(x-\gamma)(x-\delta)$ is given by the formula

$$\Delta_4[q(x)] = (\alpha-\beta)^2(\alpha-\gamma)^2(\alpha-\delta)^2(\beta-\gamma)^2(\beta-\delta)^2(\gamma-\delta)^2.$$

Suppose that for a particular quartic $Q(x)$ with real coefficients, $\Delta_4[Q(x)] > 0$. What can you say about the number of real roots?

Firstly, there must be no repeated roots (or the discriminant would be zero).

Obviously if all four roots are real, the discriminant is positive (since it is a square); so suppose that there is at least one complex root. We know that any non-real roots must appear in conjugate pairs. Let the four roots be $a \pm bi$ and $c \pm di$, so (after simplifying)

$$\begin{aligned}\Delta_4[q(x)] &= (a+bi-a+bi)^2(a+bi-c-di)^2(a+bi-c+di)^2 \\ &\qquad (a-bi-c-di)^2(a-bi-c+di)^2(c+di-c+di)^2 \\ &= 16b^2d^2(a^4-4a^3c+2a^2b^2+6a^2c^2+2a^2d^2-4ab^2c-4ac^3 \\ &\qquad -4acd^2+b^4+2b^2c^2-2b^2d^2+c^4+2c^2d^2+d^4)^2\end{aligned}$$

But $\Delta_4[q(x)] \neq 0$, so neither b nor d is zero. Hence all four roots are complex.

Therefore if the discriminant is positive, either all four roots are real or all four roots are complex.

[4] An intentional mispelling.

9 Final Exercises

1. Is $(x-15)$ a factor of $(x^3-19x-30)$? Is (x^2+5x+6) a factor?

By the remainder theorem, $(x-15)$ is not a factor $(15^3-19(15)-30=3060\neq 0)$. We check each factor of (x^2+5x+6) individually:

$$(-2)^3-19(-2)-30=0$$
$$(-3)^3-19(-3)-30=0$$

So the quadratic is a factor.

2. Factor completely $9x^4-13x^2+4$.

Using the quadratic formula, $x^2\in\{\frac{4}{9},1\}$ and so $x\in\{-1,-\frac{2}{3},\frac{2}{3},1\}$. Hence the full factorisation is $(x+1)(x-1)(x+\frac{2}{3})(x-\frac{2}{3})$.

3. Solve $x^3+9x^2=60-8x$.

After trying a few simple solutions, we find that $x=2$ is a solution.

$$\begin{array}{r|l} & x^2+11x+30 \\ \hline x-2 & x^3+9x^2+8x-60 \\ & -x^3+2x^2 \\ \hline & \quad 11x^2+8x \\ & \quad -11x^2+22x \\ \hline & \qquad 30x-60 \\ & \qquad -30x+60 \\ \hline & \qquad\quad 0 \end{array}$$

We factor the quadratic as $(x+5)(x+6)$, so the three solutions of the cubic are $x\in\{-6,-5,2\}$.

4. Find k such that $(x-4)$ is a factor of $x^3+7x^2-14x+k$.

By the remainder theorem, we want $4^3+7(4)^2-14(4)+k=0$. Hence $k=-120$.

5. Find a value of $k\neq 0$ such that $kx^2-6x+1=0$ will have just one root.

We set $\Delta_2=(-6)^2-4k=0$, so $k=9$.

6. Find all sixth roots of i.

We convert to polar form, so $i=\operatorname{cis}\frac{\pi}{2}$. Then, by de Moivre's Theorem, we have:

Root	Polar form
z_1	$\operatorname{cis}\frac{\pi}{12}$
z_2	$\operatorname{cis}\frac{5\pi}{12}$
z_3	$\operatorname{cis}\frac{3\pi}{4}$
z_4	$\operatorname{cis}\frac{13\pi}{12}$
z_5	$\operatorname{cis}\frac{17\pi}{12}$
z_6	$\operatorname{cis}\frac{7\pi}{4}$

7. Find k such that $8 - x + 2\sqrt{2x+k} = 0$ has exactly one real root.

Rearrange as follows:

$$\begin{aligned} 2\sqrt{2x+k} &= x - 8 \\ 8x + 4k &= x^2 - 16x + 64 \\ 0 &= x^2 - 24x + (64 - 4k) \end{aligned}$$

But $\Delta_2 = 0$, so $24^2 = 4(64 - 4k)$ and $k = -20$.

8. Solve $(\alpha^2 + 2\alpha - 4)(\alpha^7 + 1) = 0$.

The roots of the first factor are $\alpha = -1 \pm \sqrt{5}$. The roots of the second are simply all the seventh roots of unity, so all nine roots of the equation are:

Root	Polar form	Rectangular form
z_8		$-1+\sqrt{5}$
z_9		$-1-\sqrt{5}$
z_1	$\operatorname{cis} 0$	1
z_2	$\operatorname{cis} \frac{2\pi}{7}$	
z_3	$\operatorname{cis} \frac{-2\pi}{7}$	
z_4	$\operatorname{cis} \frac{4\pi}{7}$	
z_5	$\operatorname{cis} \frac{-4\pi}{7}$	
z_6	$\operatorname{cis} \frac{6\pi}{7}$	
z_7	$\operatorname{cis} \frac{-6\pi}{7}$	

9. Solve $x^4 + x^2 + 1 = 0$ for x.

$x^2 = \frac{-1 \pm \sqrt{3}i}{2}$, so $x = \pm\frac{1 \pm \sqrt{3}i}{2}$.

10. Solve $\beta^2 + \beta + 1 = 0$ for x if $\beta = x^2 + x + 1$.

We have $\beta = \frac{-1}{2} \pm \frac{\sqrt{3}i}{2}$. Now, $x^2 + x + 1.5 \mp \frac{\sqrt{3}i}{2} = 0$.

Using the quadratic formula (twice!), we obtain the following four roots:

Root	Rectangular form
x_1	$\frac{-1+\sqrt{-5-2\sqrt{3}i}}{2}$
x_2	$\frac{-1-\sqrt{-5-2\sqrt{3}i}}{2}$
x_3	$\frac{-1+\sqrt{-5+2\sqrt{3}i}}{2}$
x_4	$\frac{-1-\sqrt{-5+2\sqrt{3}i}}{2}$

11. Let α, β, and γ be the three roots of $ax^3 + bx^2 + cx + d = 0$. Prove that: a. $\alpha + \beta + \gamma = \frac{-b}{a}$, b. $\alpha\beta + \beta\gamma + \alpha\gamma = \frac{c}{a}$, and c. $\alpha\beta\gamma = \frac{-d}{a}$. Hence show that $\alpha^2\beta\gamma + \alpha\beta^2\gamma + \alpha\beta\gamma^2 = \frac{bd}{a^2}$.

We have that $ax^3 + bx^2 + cx + d = a(x-\alpha)(x-\beta)(x-\gamma) = ax^3 - a(\alpha+\beta+\gamma)x^2 + a(\alpha\beta+\alpha\gamma+\beta\gamma)x - a\alpha\beta\gamma$, and so $b = -a(\alpha+\beta+\gamma)$, $c = a(\alpha\beta+\alpha\gamma+\beta\gamma)$, and $d = -a\alpha\beta\gamma$.

Hence, $\frac{-b}{a} = \frac{a(\alpha+\beta+\gamma)}{a} = \alpha+\beta+\gamma$, $\frac{c}{a} = \frac{a(\alpha\beta+\alpha\gamma+\beta\gamma)}{a} = \alpha\beta+\alpha\gamma+\beta\gamma$, and $\frac{-d}{a} = \frac{a\alpha\beta\gamma}{a} = \alpha\beta\gamma$ as expected.

We also have that $\frac{bd}{a^2} = \frac{-b}{a} \times \frac{-d}{a} = (\alpha+\beta+\gamma)\alpha\beta\gamma = \alpha^2\beta\gamma + \alpha\beta^2\gamma + \alpha\beta\gamma^2$.

12. Solve $(z+1)^3 = 8(z-1)^3$ for z. Give exact answers in the form $a+ib$.

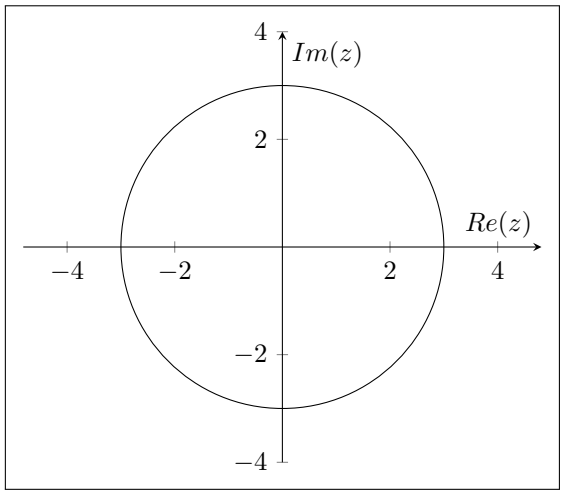
Expanding, $z^3 + 3z^2 + 3z + 1 = 8z^3 - 24z^2 + 24z - 8$ and so we need to solve $7z^3 - 27z^2 + 21z - 9 = 0$. Using magic, we notice that one solution is $z = 3$ — a useful trick is to realise that there must be at least one real root (as we have an odd polynomial with real coefficients), and that that root must divide the constant term: this means we only need to try $z = 1$, $z = 3$, and $z = 9$ (and the negatives of those values).

Dividing:

$$
\begin{array}{r|l}
z-3 & 7z^2 - 6z + 3 \\
\hline
 & 7z^3 - 27z^2 + 21z - 9 \\
 & -7z^3 + 21z^2 \\
\hline
 & -6z^2 + 21z \\
 & 6z^2 - 18z \\
\hline
 & 3z - 9 \\
 & -3z + 9 \\
\hline
 & 0
\end{array}
$$

Using the quadratic formula, we find the roots of the quadratic factor to be $z = \frac{3}{7} \pm \frac{2}{7}\sqrt{3}i$.

13. Graph the equation $|z| = 3$ in the complex plane.



14. If $z = 1 + i$ and $w = \frac{1}{z} + i$, find the argument of w.

$$\begin{aligned} w &= \frac{1}{1+i} + i \\ &= \frac{1-i}{(1+i)(1-i)} + i \\ &= \frac{1-i}{2} + i \\ &= \frac{1}{2} + \frac{1}{2}i \\ \Rightarrow \arg w &= \frac{\pi}{4}. \end{aligned}$$

15. If $\frac{z+2i}{z-2i}$ is purely imaginary, describe the possible values of z.

Let $z = x + yi$.

$$\begin{aligned} \frac{x+(y+2)i}{x+(y-2)i} &= \frac{(x+(y+2)i)(x-(y-2)i)}{(x+(y-2)i)(x-(y-2)i)} \\ &= \frac{x^2 + x(y+2)i - x(y-2)i + (y+2)(y-2))}{x^2 + (y-2)^2} \\ &= \frac{x^2 + 4ix + y^2 - 4}{x^2 + (y-2)^2} \end{aligned}$$

So in order for the fraction to be purely imaginary, $x^2 + y^2 = 4$ and so z must lie on the circle of radius two centred on the origin.

16. If $|z - 1 + 2i| = |z + 1|$ and $z = x + yi$, find an expression for y in terms of x (i.e. find the locus of z).

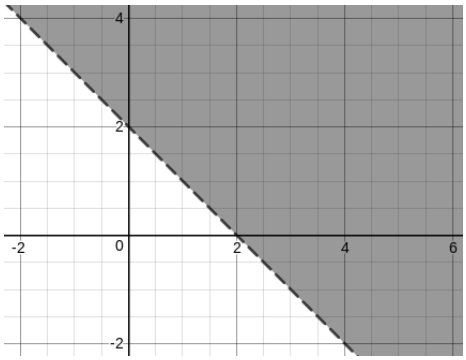
$$\begin{aligned} \big|(x-1)+(y+2)i\big| &= \big|(x+1)+yi\big| \\ \sqrt{(x-1)^2 + (y+2)^2} &= \sqrt{(x+1)^2 + y^2} \\ x^2 - 2x + 1 + y^2 + 4y + 4 &= x^2 + 2x + 1 + y^2 \\ 4y &= 4x - 4 \\ y &= x - 1. \end{aligned}$$

17. Sketch the region satisfied by $\mathfrak{Re}\,(z - i\bar{z}) > 2$.

Let $z = x + yi$.

$$z - i\bar{z} = x + yi - xi + y$$
$$\mathfrak{Re}\,(z - i\bar{z}) = x + y$$

So the region is $x + y > 2$:



18. If $x = 2$ and $x = 6$ are solutions of $p(x) = Ax^2 + Bx + C$ and $p(0) = -4$, find A, B, and C.

A quadratic equation with the roots $x = 2$ and $x = 6$ must have the form $A(x-2)(x-6) = Ax^2 - 8Ax + 12A$, and the constant term $p(0) = C = 12A = -4$.

Hence $A = \frac{-4}{12} = -\frac{1}{3}$, and so $p(x) = \frac{-x^2}{3} + \frac{8x}{3} - 4$.

19. If $w = 2 - 3i$ is a zero of $3w^3 - 14w^2 + Aw - 26$ (where A is real), find A and the remaining two roots.

Given that the polynomial has real coefficients, $\bar{w} = 2 + 3i$ must also be a root. Call α the third (and only real) root.

We can expand the factored form and equate the coefficients:

$$\begin{aligned}(x - 2 + 3i)(x - 2 - 3i)(x - \alpha) &= (x^2 - 4x + 13)(x - \alpha) \\ &= x^3 - x^2(4 + \alpha) + x(14 + 4\alpha) - 13\alpha\end{aligned}$$

So $\alpha = 2$ and $A = 13 + 4 \times 2 = 21$.

20. Use de Moivre's Theorem to show that

a. $\sin 2\theta = 2\sin\theta\cos\theta$ **and** $\cos 2\theta = \cos^2\theta - \sin^2\theta$**; and**

b. $\sin 3\theta = 3\sin\theta - 4\sin^3\theta$ **and** $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$**.**

(a) The key idea is to note that we can expand $\operatorname{cis}^n\theta$ in two different ways: by the binomial theorem, and by de Moivre's theorem.

$$\begin{aligned}\operatorname{cis} 2\theta &= (\operatorname{cis}\theta)^2 \\ &= (\cos\theta + i\sin\theta)^2 \\ &= \cos^2\theta + 2i\cos\theta\sin\theta - \sin^2\theta\end{aligned}$$

Taking just the real parts, we obtain $\cos 2\theta = \cos^2\theta - \sin^2\theta$, and taking just the non-real parts, we obtain $\sin 2\theta = 2\cos\theta\sin\theta$ as expected.

(b) Likewise for the third power (although we use identities to simplify further):

$$\begin{aligned}\operatorname{cis} 3\theta &= (\operatorname{cis}\theta)^3 \\ &= (\cos\theta + i\sin\theta)^3 \\ &= \cos^3\theta + 3i\cos^2\theta\sin\theta - 3\cos\theta\sin^2\theta - i\sin^3\theta \\ &= \cos^3\theta + 3i(1-\sin^2\theta)\sin\theta - 3\cos\theta(1-\cos^2\theta) - i\sin^3\theta \\ &= 4\cos^3\theta + 3i\sin\theta - 3\cos\theta - 4i\sin^3\theta\end{aligned}$$

Hence $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$ and $\sin 3\theta = 3\sin\theta - 4\sin^3\theta$.

21. Use Euler's formula to prove that $\cos(\alpha+\beta) = \cos\alpha\cos\beta - \sin\alpha\sin\beta$**, and that** $\sin(\alpha+\beta) = \sin\alpha\cos\beta + \cos\alpha\sin\beta$**.**

$$\begin{aligned}\cos(\alpha+\beta) + i\sin(\alpha+\beta) = e^{i(\alpha+\beta)} &= e^{i\alpha}e^{i\beta} \\ &= (\cos\alpha + i\sin\alpha)(\cos\beta + i\sin\beta) \\ &= \cos\alpha\cos\beta + i\sin\alpha\cos\beta + i\cos\alpha\sin\beta - \sin\alpha\sin\beta \\ &= (\cos\alpha\cos\beta - \sin\alpha\sin\beta) + i(\sin\alpha\cos\beta + \sin\beta\cos\alpha).\end{aligned}$$

The identities immediately follow from equating real and imaginary components.

22. Show that $\arctan a + \arctan b = \arctan \frac{a+b}{1-ab}$.

Recall that $\arg(x + yi) = \arctan \frac{y}{x}$. Specifically, $\arg(1 + yi) = \arctan y$. Hence, we argue as follows:

$$\begin{aligned}\arctan a + \arctan b &= \arg(1 + ai) + \arg(1 + bi)\\ &= \arg((1 + ai)(1 + bi))\\ &= \arg((1 - ab) + (a + b)i)\\ &= \arctan \frac{a + b}{a - ab}.\end{aligned}$$

Aside: Note that arg here behaves like a logarithm in that it converts a sum to a product. This is because if $z = \operatorname{cis}\theta$ then $z = e^{i\theta}$ and so $\arg z = \theta = \frac{1}{i}\ln z$; hence we take $\arg w + \arg z = \frac{1}{i}\ln w + \ln z = \frac{1}{i}\ln(wz) = \arg wz$.

23. If $3z^3 + (2 - 3ai)z^2 + (6 + 2bi)z + 4$ has exactly one real root, what value must the quotient b/a take if both a and b are real? Find the real root.

For a real root to occur, the imaginary part of the polynomial must become zero (assuming $z \in \mathbb{R}$). Hence we first solve $-3aiz^2 + 2biz = 0$, finding the two solutions to be $z = 0$ and $z = \frac{2b}{3a}$.

Looking at the real part, we need to solve $3z^3 + 2z^2 + 6z + 4 = 0$; $z = 0$ is not a solution here, so that means that in order to find the single remaining possible real root we must find $\frac{2b}{3a}$. Luckily this cubic does not have coefficients depending on a or b (so we can find exact answers), and so we solve it to find that it has a single real solution of $z = -\frac{2}{3}$; so the single real root is $z = -\frac{2}{3}$ and $\frac{b}{a} = -1$.

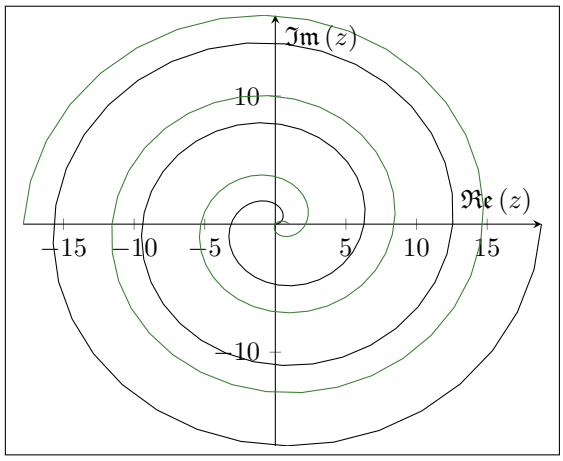
24. Find all possible values for θ if $\operatorname{cis}^2\theta + \operatorname{cis}\theta + 1 = 0$.

We have a quadratic in $\operatorname{cis}\theta$, so $\operatorname{cis}\theta = \frac{-1 \pm \sqrt{3}i}{2}$.

Hence $\cos\theta = \frac{-1}{2}$ and $\sin\theta = \frac{\sqrt{3}}{2}$, so $\theta = \frac{2\pi}{3} + 2n\pi$ for $n \in \mathbb{N}$.

25. Graph the locus of $\arg w = |w|$. What about $\arg w + |w| = 1$?

The first equation (in black) is an equiangular spiral; the second (in green) is congruent to the first spiral but transformed.



26. Given a quadratic equation x^2+px+q and a root α, show that the other root β is given by $\beta = -p - \alpha$ and find a similar expression for finding two roots of a cubic given the third.

The first fact is easily shown by writing out the quadratic in factored form and matching coefficients:

$$(x-\alpha)(x-\beta) = x^2 - (\alpha+\beta)x + \alpha\beta$$

So $p = -\alpha - \beta \Rightarrow \beta = -p - \alpha$. Note we have two equations ($p = -\alpha - \beta$ and $q = \alpha\beta$) in *one* unknown (namely β), so the system is easily solvable.

Attempting the same thing for the cubic $x^3 + px^2 + qx + r$, with the known root being γ:

$$(x-\alpha)(x-\beta)(x-\gamma) = x^3 - (\alpha+\beta+\gamma)x^2 + (\alpha\beta+\alpha\gamma+\beta\gamma)x - \alpha\beta\gamma$$

So we have three equations in two unknowns:

$$\begin{aligned} p &= -\alpha - \beta - \gamma \\ q &= \alpha\beta + \alpha\gamma + \beta\gamma \\ r &= -\alpha\beta\gamma \end{aligned}$$

We rearrange and solve the first and third equations to find an expression for α in terms of γ:

$$\begin{aligned} \beta = -p - \alpha - \gamma &= \frac{-r}{\alpha\gamma} \\ p + \alpha + \gamma &= \frac{r}{\alpha\gamma} \\ p\alpha\gamma + \alpha^2\gamma + \alpha\gamma^2 - r &= 0 \\ \gamma\alpha^2 + (p\gamma + \gamma^2)\alpha - r &= 0 \end{aligned}$$

Using the quadratic formula:

$$\alpha = \frac{-p\gamma - \gamma^2 \pm \sqrt{(p\gamma+\gamma^2)^2 + 4r\gamma}}{2\gamma}$$

Interestingly, this single formula will give us both α *and* β due to the square root! This is because the three equations within the coefficients are symmetrical, and so we could also write β in place of α (and vice versa) everywhere above — giving us the same formula but this time equal to β. The distinction between roots by letter is purely a notational construct! Whichever way we permute the roots, the formula we have found here will always find the two other roots given one.

27. Suppose p is a quadratic (i.e. $p(x) = ax^2 + bx + c$ for some a, b, and c). Suppose further that $p(0) = 9$, and $p(3) = 0$. How many distinct roots does p have?

We have $9 = p(0) = a \cdot 0^2 + b \cdot 0 + c = c$, and that one of the roots of the quadratic is 3. But recall that the constant term of a quadratic is simply the product of the roots; hence the second root is $9 \div 3 = 3$. Hence the quadratic has a single repeated root, $x = 3$.

28. Use the identity $x^2 + y^2 = (x - iy)(x + iy)$ to prove that if m and n are integers that can be written as the sum of two squares, then their product mn can also be written as a sum of two squares.

Suppose $m = a^2 + b^2$ and $n = c^2 + d^2$. Then $m = (a + ib)(a - ib)$ and $n = (c + id)(c - id)$. We therefore have the following:

$$\begin{aligned} mn &= (a + ib)(a - ib)(c + id)(c - id) \\ &= (a + ib)(c - id)(a - ib)(c + id) \\ &= (ac - iad + ibc + bd)(ac + iad - ibc + bd) \\ &= (ac + bd + i(bc - ad))(ac + bd + i(ad - bc)) \\ &= (ac + bd + i(bc - ad))(ac + bd - i(bc - ad)) \\ &= (ac + bd)^2 + (bd - ad)^2, \end{aligned}$$

where $(ac + bd)$ and $(bd - ad)$ are integers.

29. Solve the following system of equations:

$$\begin{aligned} x^2 + 4xy + y^2 &= 2 \\ x^2 - 2xy + y^2 &= -4 \end{aligned}$$

From the second equation, we have that $(x-y)^2 = -4$ and hence that $x-y = \pm 2i$. From the first, we have $(x - y)^2 + 6xy = 2$ and therefore $-4 + 6xy = 2$ and $xy = 1$.

Consider the first case, $x-y = 2i$. Then $x - \frac{1}{x} = 2i$, and therefore $x^2 - 2xi - 1 = 0$. But this can be factorised as $(x - i)^2 = 0$, or $x = i$ (and so $y = 1/i = -i$). Hence one solution is $(x, y) = (i, -i)$.

Similarly, if $x - y = -2i$ then $x^2 + 2xi - 1 = 0$ and so $(x + i)^2 = 0$; hence $x = -i$, and so $y = i$. Hence a second solution is $(x, y) = (-i, i)$.

It is left to the reader to check that both these solutions are in fact solutions of the original system.

30. Suppose ω is a primitive cube root of unity. Show that $y_2 = \omega\sqrt[3]{\frac{1}{2}(-1+\sqrt{5})}+\omega^2\sqrt[3]{\frac{1}{2}(-1-\sqrt{5})}$ and $y_3 = \omega^2\sqrt[3]{\frac{1}{2}(-1+\sqrt{5})}+\omega\sqrt[3]{\frac{1}{2}(-1-\sqrt{5})}$ are complex conjugates.

We proceed to show that $\arg y_2 = -\arg y_3$, and $|y_2| = |y_1|$.

When we multiply the two, we obtain

$$\begin{aligned} y_2y_3 = &\left(\sqrt[3]{\frac{1}{2}(-1+\sqrt{5})}\right)^2 && + \omega^2\sqrt[3]{\frac{1}{2}(-1+\sqrt{5})}\sqrt[3]{\frac{1}{2}(-1-\sqrt{5})} \\ & && + \omega\sqrt[3]{\frac{1}{2}(-1+\sqrt{5})}\sqrt[3]{\frac{1}{2}(-1-\sqrt{5})} \\ & && + \left(\sqrt[3]{\frac{1}{2}(-1-\sqrt{5})}\right)^2 \\ = &\left(\sqrt[3]{\frac{1}{2}(-1+\sqrt{5})}\right)^2 && - \sqrt[3]{\frac{1}{2}(-1+\sqrt{5})}\sqrt[3]{\frac{1}{2}(-1-\sqrt{5})} \\ & && + \left(\sqrt[3]{\frac{1}{2}(-1-\sqrt{5})}\right)^2, \end{aligned}$$

which is real (remembering that $\omega + \omega^2 = -1$). Hence, we must have $\arg y_2 = -\arg y_3$ (since the arguments must add to give zero).

The fact that $|y_2| = |y_3|$ is easily shown by drawing a diagram (remembering that $\arg\omega = \frac{2\pi}{3}$ and $|\omega| = 1$) and noticing the symmetry.

31. Find all solutions to $x^{n-1}+x^{n-2}+\cdots+1 = 0$, where n is a natural number.

Simply note that $(x^{n-1}+x^{n-2}+\cdots+1)(x-1) = x^n - 1$, and so the solutions will simply be all nth roots of unity except 1 itself.

32. **a. Let $p(x) = \sum_{r=0}^{n} p_r x^r$ be a polynomial with real coefficients. If $p(z) = 0$, then $p(\overline{z}) = 0$. (This is a generalisation of 5.27 to arbitrary degree polynomials.)**

b. Let $p(x) = \sum_{r=0}^{n} p_r x^{2r}$ be a polynomial with real coefficients and only even powers of x. If $p(a+bi) = 0$, then $p(\pm a \pm bi) = 0$ for all possible combinations of $\pm$.

(a) Recall that we have already shown in section 5 that $\overline{w} + \overline{z} = \overline{w+z}$ and that $\overline{w} \cdot \overline{z} = \overline{wz}$. It follows by induction that these hold for arbitrary long strings of addition and multiplication. Hence if $p(z) = 0$ then:

$$\begin{aligned}
p(\overline{z}) &= \sum_{r=0}^{n} p_r (\overline{z})^r \\
&= \sum_{r=0}^{n} p_r \overline{z^r} \\
&= \sum_{r=0}^{n} \overline{p_r} \overline{z^r} \text{ (since } p_r \text{ is real)} \\
&= \sum_{r=0}^{n} \overline{p_r z^r} \\
&= \overline{\sum_{r=0}^{n} p_r z^r} \\
&= \overline{p(z)} = \overline{0} = 0.
\end{aligned}$$

(b) Note that the statement to be proved in the question is equivalent to $p(a+bi) = 0 \implies p((-1)^p a + (-1)^q bi) = 0$ for all integers p and q. Then:

$$\begin{aligned}
p((-1)^p a + (-1)^q bi) &= \sum_{r=0}^{n} p_r ((-1)^p a + (-1)^q bi)^{2r} \\
&= \sum_{r=0}^{n} p_r \left(((-1)^p a)^2 + 2(-1)^p (-1)^q abi + ((-1)^q bi)^2 \right)^r \\
&= \sum_{r=0}^{n} p_r \left(a^2 + 2(-1)^{p+q} abi + (bi)^2 \right)^r
\end{aligned}$$

We have two cases: $p+q$ is even, or $p+q$ is odd.

Case I: $p+q$ **even** So $(-1)^{p+q}=1$ and

$$\begin{aligned} p((-1)^p a+(-1)^q bi) &= \sum_{r=0}^{n} p_r\left(a^2+2abi+(bi)^2\right)^r \\ &= \sum_{r=0}^{n} p_r(a+bi)^{2r} \\ &= p(a+bi)=0. \end{aligned}$$

Case II: $p+q$ **odd** So $(-1)^{p+q}=-1$ and

$$\begin{aligned} p((-1)^p a+(-1)^q bi) &= \sum_{r=0}^{n} p_r\left(a^2-2abi+(bi)^2\right)^r \\ &= \sum_{r=0}^{n} p_r(a-bi)^{2r} \\ &= p(a-bi) \\ &= p(\overline{a+bi})=0 \text{ (from (a) above).} \end{aligned}$$

Alternatively for (b), one could notice that all we are claiming is that if z is a root, then $\overline{z}$, $-z$, and $-\overline{z}$ are also roots; the first follows from part (a), and since all powers of x are even the negative signs on the second two vanish and they reduce to z and $\overline{z}$.

33. Under which conditions will the equation $x^2+a(1+i)x+b(1+i)=0$ have one or more real solutions if both a and b are real?

The possible real root must satisfy $ax+b=0$ in order for the imaginary part of the polynomial to be zero. Hence $x=-\frac{b}{a}$.

For this value to be a solution, it must also satisfy the real part:

$$\begin{aligned} x^2+ax+b &= 0 \\ \left(\frac{-b}{a}\right)^2+a\left(\frac{-b}{a}\right)+b &= 0 \\ \left(\frac{-b}{a}\right)^2 &= 0 \\ b &= 0. \end{aligned}$$

So the equation will only have real solutions when $b=0$, in which case the only real solution will be $x=-\frac{0}{a}=0$.

34. Find the complex number z which satisfies $\arg(z-1-i) = -\frac{\pi}{6}$ and $\arg(z-1+i) = \frac{\pi}{6}$.

Suppose $z = x + yi$. So:

$$\arg((x-1)+(y-1)i) = \arctan\left(\frac{y-1}{x-1}\right) = -\frac{\pi}{6}$$
$$\arg((x-1)+(y+1)i) = \arctan\left(\frac{y+1}{x-1}\right) = \frac{\pi}{6}.$$

Simplifying, we have $\frac{y+1}{x-1} = \frac{\sqrt{3}}{3}$ and $\frac{y-1}{x-1} = -\frac{\sqrt{3}}{3}$. Then $\frac{3y+3}{\sqrt{3}} = x-1 = \frac{3-3y}{\sqrt{3}} \implies y = 0$, $x = \sqrt{3}+1$. So $z = \sqrt{3}+1$.

35. Find all integer values of a and b such that $\frac{a^2+b^2}{ab}$ is an integer.

We will call the integer pairs (a, b) such that the fraction is an integer *solutions* of the fraction. We prove that all solutions are of the form (n, n) or $(n, -n)$ for $n \in \mathbb{Z}$ and $n \neq 0$ — i.e. the fraction is an integer if and only if $a = b$ or $a = -b$.

We first show that both (n, n) and $(n, -n)$ are solutions (with the restrictions that $n \in \mathbb{Z}$ and $n \neq 0$). Firstly, $\frac{n^2+n^2}{nn} = 2$ and so (n, n) is a solution. Secondly, $\frac{n^2+(-n)^2}{-nn} = -2$ and so $(n, -n)$ is a solution.

To show that these are the only solutions, we rewrite the fraction as follows:

$$\begin{aligned}\frac{a^2+b^2}{ab} &= \frac{a^2}{ab} + \frac{b^2}{ab} \\ &= \frac{a}{b} + \frac{b}{a}.\end{aligned}$$

Let $p = \frac{a}{b}$. Then we must therefore find all values of p such that $p + \frac{1}{p}$ is an integer. Call that integer n.

We have the following equation to solve for p: $p + \frac{1}{p} = n$. This is a quadratic in p (it rearranges to $p^2 - np + 1 = 0$), and so we use the quadratic formula:

$$p = \frac{-n \pm \sqrt{n^2 - 4}}{2}$$

We know that p must be rational as it is (by definition) the ratio between a and b, which are both integers. This implies that $\sqrt{n^2 - 4}$ must be rational, and therefore that $n^2 - 4$ is a perfect square (as n is an integer, $n^2 - 4$ must be an integer and its square root will be rational only if it is a perfect square).

Hence we have two squares with a difference of 4: $n^2 - 4$ and n^2 are both perfect squares. However, there are only two pairs of perfect squares that satisfy this requirement: $(-2)^2 - 4 = 0^2$, and $(2)^2 - 4 = 0^2$. Hence $n = \pm 2$ are the only possible integers that the fraction $\frac{a^2+b^2}{ab}$ will evaluate to.

Take the case where $n = 2$. We therefore have that:

$$\begin{aligned}\frac{a^2+b^2}{ab} &= 2 \\ a^2 + b^2 &= 2ab \\ a^2 - 2ab + b^2 &= 0 \\ a &= \frac{2b \pm \sqrt{4b^2 - 4b^2}}{2} \\ &= b\end{aligned}$$

Likewise, when $n = -2$, $a = -b$. Hence these are the only solutions.

This exercise was inspired by an incredibly melodramatic video which can be found at `https://www.youtube.com/watch?v=Y30VF3cSIYQ`.

36. Let w and z be complex numbers, and let $u = w+z$ and $v = w^2+z^2$. Prove that w and z are real if and only if u and v are real and $u^2 \leq 2v$.

First we prove the "only if" direction - obviously, if w and z are real, u and v are real. Additionally, we must prove that $u^2 \leq 2v$:

$$\begin{aligned} u^2 \leq 2v &\iff w^2 + 2wz + z^2 \leq 2w^2 + 2z^2 \\ &\iff 2wz \leq w^2 + z^2 \\ &\iff 0 \leq w^2 - 2x^2 + z^2 = (w-z)^2, \end{aligned}$$

the last inequality being obviously true as a square is always positive.

Now we prove that given the three conditions (those on u and v), w and z must be real. We do this by assuming that w and z are non-real, and show that a contradiction results.

Let $w = a + bi$ and $z = c + di$. Assume that b and d are non-zero: i.e. that w and z are non-real.

We have that u is real. Since $u = w + z = a + bi + c + di$, we must have that $bi + di = 0$ and therefore $b = -d$. So $z = c - bi$.

We also have that v is real. We compute as follows:

$$\begin{aligned} v = w^2 + z^2 &= (a + bi)^2 + (c - bi)^2 \\ &= a^2 + 2abi - b^2 + c^2 - 2cbi - b^2. \end{aligned}$$

Since v is real, $2abi - 2cbi = 0$ and therefore (since we assumed that $b \neq 0$ and so we can divide by it) $a = c$. Hence $w = a + bi$ and $z = a - bi$.

Our final assumption was that $u^2 \leq 2v$; however, $u^2 = (a + c)^2 = (2a)^2 = 4a^2$, and $2v = a^2 + c^2 - b^2 - b^2 = 2a^2 - 2b^2$. Hence, if we assume that $b \neq 0$ we have that $4a^2 \leq 2a^2 - 2b^2$ which is obviously false as a and b are real and so their squares are non-negative — the right hand side must be less than the left! And so we have our contradiction. □

37. Suppose $x + \frac{1}{x} = 1$.

a. Show, without calculating x, that we must necessarily have $x^7 + \frac{1}{x^7} = 1$.

b. Calculate the possible values of x and verify this fact.

(a) We have the following:

$$\begin{aligned} x + \frac{1}{x} &= 1 \\ x^2 &= x - 1 \\ x^3 &= x^2 - x \\ x^3 &= (x-1) - x = -1 \\ x^6 &= (-1)^2 = 1 \\ x^7 &= x. \end{aligned}$$

Hence $x + \frac{1}{x} = x^7 + \frac{1}{x^7} = 1$.

(b) We have that $x = \frac{1 \pm \sqrt{1-4}}{2} = \frac{1}{2} \pm \frac{\sqrt{3}}{2}i$. In polar form, this becomes $x = \operatorname{cis}\left(\pm\frac{\pi}{3}\right)$. It is easy to show that $\operatorname{cis}\left(\pm\frac{7\pi}{3}\right) + \operatorname{cis}\left(\mp\frac{7\pi}{3}\right) = 1$, by converting both terms back to rectangular form.

38. Calculate i^i.

We use Euler's formula. Note first that

$$e^{i\frac{\pi}{2}} = i$$

so $\ln i = i\frac{\pi}{2}$. Then:

$$i^i = e^{\ln(i^i)} = e^{i \ln i} = e^{ii\frac{\pi}{2}} = e^{-\frac{\pi}{2}} \approx 0.208.$$

Note that ln has multiple branches since $i = e^{i\frac{\pi}{2}} = e^{i(\frac{\pi}{2}+2n\pi)} = e^{i\frac{(4n+1)\pi}{2}}$, and so $\ln i = i\frac{(4n+1)\pi}{2}$ for all $n \in \mathbb{Z}$. It is left as an exercise to the reader, then, to fix the solution given above.

39. Let $\mathbb{R}[\epsilon]$ be the real numbers together with some new element $\epsilon \neq 0$ such that $\epsilon^2 = 0$.

a. Does there exist β in $\mathbb{R}[\epsilon]$ such that $\beta\epsilon = 1$ (i.e. does ϵ have a multiplicative inverse)?

b. When does $(a + b\epsilon)^{-1}$ exist?

c. Solve $x^2 - 1 = 2\epsilon$ in $\mathbb{R}[\epsilon]$.

(a) Suppose such a β exists. Then:

$$\beta\epsilon = 1 \iff \beta\epsilon^2 = \epsilon \iff \beta \cdot 0 = \epsilon \iff 0 = \epsilon.$$

But (by definition) $\epsilon \neq 0$; so no such β exists.

(b) Let $a + b\epsilon$ be in the set. We compute its inverse $c + d\epsilon$:

$$\begin{aligned} & (a + b\epsilon)(c + d\epsilon) = 1 \\ \iff & ac + (ad + bd)\epsilon = 1 \\ \iff & ad + bc = 0 \text{ and } ac = 1 \end{aligned}$$

So $c = a^{-1}$, and $d = -\frac{b}{a^2}$. Hence the inverse of $a + bi$ exists iff $a \neq 0$, and such an inverse is $\frac{1}{a} - \frac{b}{a^2}\epsilon$.

(c) We wish to find $x = a + b\epsilon$ such that $x^2 = 2\epsilon + 1$:

$$a^2 + 2ab\epsilon = 2\epsilon + 1$$

So $a^2 = 1 \implies a = \pm 1$, and $ab = 1$ so $b = a$. Hence we have exactly two solutions: $\pm 1 \pm \epsilon$.

40. Suppose $p(x) = \sum_{i=0}^{n} a_i x^i$ and $q(x) = \sum_{i=0}^{m} b_i x^i$ are polynomials. Show that $p(x)q(x) = \sum_{i=0}^{m+n} c_i x^i$, where each c_i is a constant. Give an expression for c_i in terms of the coefficients of $p(x)$ and $q(x)$.

$$\begin{aligned} p(x)q(x) &= \left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{i=0}^{m} b_j x^j\right) \\ &= \sum_{i=0}^{n}\left(\left(\sum_{i=0}^{m} b_j x^j\right) a_i x^i\right) \\ &= \sum_{i=0}^{n}\sum_{i=0}^{m} a_i b_j x^{i+j} \\ &= \sum_{k=0}^{m+n}\sum_{j=0}^{k} a_{k-j} b_j x^k \quad \text{(where } k = i + j\text{)} \\ &= \sum_{i=0}^{m+n}\sum_{j=0}^{i} a_{i-j} b_j x^i \quad \text{(renaming } k \text{ to } i\text{)} \\ &= \sum_{i=0}^{m+n} c_i x^i, \end{aligned}$$

where $c_i = \sum_{j=0}^{i} a_{i-j} b_j$.

41. In this exercise, we will prove the division theorem that we stated without proof in section 3: if f and $g \neq 0$ are polynomials, then there exist unique polynomials q and r such that $\partial r < \partial g$ and

$$f(x) = g(x)q(x) + r(x).$$

a. Consider the set S of all polynomials of the form $f(x) - g(x)q(x)$ for some polynomial $q(x)$. Show that S is non-empty (i.e. exhibit some polynomial in S).

b. Explain why there must be some polynomial in S with minimal degree (that is, you cannot exhibit an infinite sequence of polynomials $p_1, p_2, \ldots$ in S such that $\partial p_1 > \partial p_2 > \cdots > \partial p_i > \cdots$).

c. Pick such a polynomial of minimal degree; call it r. Fix also the associated q (i.e. now we have $f(x) = g(x)q(x) + r(x)$ for our fixed r and q). Show that if $\partial r \geq \partial g$, then it is possible to construct another polynomial in S with lower degree than r. Conclude that $\partial r < \partial g$.

d. Show that q and r are uniquely determined by f and g.

The interested reader may note that this proof is very similar to the standard proof of the division theorem for integers; it is a little more fiddly (it is instructive to try to write down a concise reason for this similarity).

(a) The set S is non-empty, since $f(x) = f(x) - g(x) \cdot 0 \in S$.

(b) We know that there is some polynomial $q(x) \in S$; the set of all degrees of polynomials in S is therefore a non-empty subset of the natural numbers and hence has a least element.

(c) Suppose that $\partial r \geq \partial g$; let $m = \partial r$ and $n = \partial g$. Suppose also that the coefficient of the x^m term in r is r_m, and suppose that the coefficient of the x^n term in g is g_n. Consider, then:

$$\begin{aligned} f(x) - g(x)\left[q(x) + \frac{r_m}{g_n}x^{m-n}\right] &= f(x) - g(x)q(x) - \frac{r_m}{g_n}x^{m-n}g(x) \\ &= r(x) - \frac{r_m}{g_n}x^{m-n}g(x) \\ &= r_m x^m + r'(x) - \frac{r_m}{g_n}x^{m-n}g_n x^n - \frac{r_m}{g_n}x^{m-n}g'(x) \\ &= r'(x) - \frac{r_m}{g_n}x^{m-n}g'(x), \end{aligned}$$

where $r'(x) = r(x) - r_m x^m$ and $g'(x) = g(x) - g_n x^n$; in particular, $\partial[r'(x) - \frac{r_m}{g_n}x^{m-n}g'(x)] < \partial r(x)$. But by the LHS of the above manipulation, $r'(x) - \frac{r_m}{g_n}x^{m-n}g'(x) \in S$! This is a contradiction, since r had minimal degree in S, and hence $\partial r < \partial g$ as required.

(d) Suppose that $f(x) = g(x)q(x) + r(x)$ and $f(x) = g(x)q'(x) + r'(x)$, where both r and r' satisfy the criteria. In particular, we have $0 = g(x)(q(x) - q'(x)) + (r(x) - r'(x))$. By definition, the degrees of both r and r' are less than that of g; in particular, the degree of $r - r'$ is less than that of g. It follows that the coefficient of the highest-degree term on the right-hand side comes from the $g(q - q')$ term; but $g \neq 0$, so $q - q' = 0$ (because, comparing coefficients of the LHS and RHS the coefficient of the highest-degree term is zero). Immediately we also have $r - r' = 0$; uniqueness follows.

42. Take the polynomial $x^2 = 4$ in the integers modulo 6 (i.e. the integers 0, 1, 2, 3, 4, 5 such that $5 + 1 = 0$). Solve for all possible values of x.

One solution is $x = 2$, as $2^2 = 4 \mod 6$. However, a second solution is $x = 4$, as $4^2 = 16 = 2 \times 6 + 4 = 4 \mod 6$.

43. Bonus exercise I: In general, what numbers will work in the place of 3 and 9 in the XKCD comic at the bottom of the bibliography?

This exercise and the next are bonus in that they should be incredibly easy, but still satisfying for those who have completed all other exercises.

We want positive integers to satisfy $a\sqrt{b} = a)\overline{b} = \frac{b}{a}$.

$$\begin{aligned} a\sqrt{b} &= \frac{b}{a} \\ a^2 b &= \frac{b^2}{a^2} \\ a^4 &= b \\ a^2 &= \sqrt{b} \end{aligned}$$

So when we take $a \times a^2$, the result is the same as $a\sqrt{a^4}$ and $a)\overline{a^4}$ — namely a^3.

44. Bonus exercise II: Notice that $\frac{3}{16} - \frac{3}{19} = \frac{3}{16} \cdot \frac{3}{19}$. For which values of a, b, and d is the identity $\frac{a}{b} - \frac{a}{d} = \frac{a}{b} \cdot \frac{a}{d}$ true?

We have the following:

$$\begin{aligned} \frac{a}{b} - \frac{a}{d} &= \frac{a^2}{bd} \\ \frac{ad - ab}{bd} &= \frac{a^2}{bd} \\ a^2 &= a(d - b) \end{aligned}$$

Hence $a = d - b$.

10 Bibliography and Further Reading

[1] Michael Artin. *Algebra*. First Edition. Pearson, 1991.

[2] Marcel Berger. *Geometry I*. Trans. by M. Cole and S. Levy. Corrected Second Printing. Springer-Verlag, 1994.

[3] David A. Cox. *Galois Theory*. Wiley, 2004.

[4] David Crowdis and Brandon Wheeler. *Precalculus Mathematics*. Glencoe Press, 1976.

[5] Underwood Dudley. *Elementary Number Theory*. Second Edition. Dover Publications, 2008.

[6] Harold M. Edwards. *Galois Theory*. Springer-Verlag, 1984.

[7] D. K. Faddeev and I. S. Sominskii. *Problems in Higher Algebra*. Trans. by J. L. Brenner. W. H. Freeman and Company, 1965.

[8] Stephen D. Fisher. *Complex Variables*. Second Edition. Dover Books, 1990.

[9] A. K. Kapoor. *Complex Variables: Principles and Problem Sessions*. World Scientific Publishing, 2011.

[10] Ian Stewart. *Galois Theory*. Fourth Edition. CRC Press, 2015.

[11] Ian Stewart. *Taming the Infinite*. Quercus Publishing, 2008.

With thanks to Heydin Leeet for highlighting a typo in an exercise.

How to solve problems

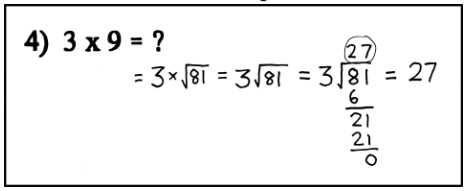


Image from `http://xkcd.com/759/`*, CC BY-NC 2.5*