to solve the third equation for s in terms of r. Finally, substitute all of this into the fourth equation:

$$((b + r^2 - a^2/4)/2)^2 - (\frac{-2c + a(b + r^2 - a^2/4)}{4r})^2 - d = 0$$

and multiply by r^2 to remove denominators. This yields

$$0 = \frac{1}{4}r^6 + \left(\frac{b}{2} - \frac{3a^2}{16}\right)r^4 + \left(\frac{3a^4}{64} - \frac{a^2}{4q} + \frac{b^2}{4} + \frac{ac}{4} - d\right)r^2 + \left(-\frac{a^6}{256} + \frac{a^4 b}{32} - \frac{a^2}{16b^2} - \frac{a^3 c}{16} + \frac{abc}{4} - \frac{c^2}{4}\right)$$

which is a cubic in r^2.

1.14 (a) F. (b) T. (c) T. (d) T. (e) F. (f) F. (g) F. (h) T. (i) F. (j) F.

2 The Fundamental Theorem of Algebra

2.1 Use induction on ∂p. If p has no rational zeros then $q = p$ and we are done. Otherwise, p has a zero $\alpha_1 \in \mathbb{Q}$. By the Remainder Theorem, $(t - \alpha_1)|p$, so $p(t) = (t - \alpha_1)s(t)$ with $\partial s = \partial p - 1 < \partial p$. Inductively,

$$s(t) = (t - \alpha_2) \cdots (t - \alpha_r)q(t)$$

where a has no rational zeros and the $\alpha_j \in \mathbb{Q}$.

Clearly $p(\beta) = 0$ for rational β if and only if $\beta = \alpha_j$ for some j, since q has no rational zeros.

For uniqueness, suppose that also

$$p(t) = (t - \beta_1) \cdots (t - \beta_s)Q(t)$$

where the $\beta_j \in \mathbb{Q}$ and Q has no rational zeros. Then

$$(t - \alpha_1) \cdots (t - \alpha_r)q(t) = (t - \beta_1) \cdots (t - \beta_s)Q(t)$$

Cancelling any common linear factors we can assume that the α_i and β_j are distinct.

If $r > 0$ then

$$0 = p(\alpha_1) = (\alpha_1 - \beta_1) \cdots (\alpha_1 - \beta_s)Q(\alpha_1)$$

so $Q(\alpha_1) = 0$, a contradiction. Therefore $r = 0$. Similarly $s = 0$, so $q = Q$ and the result follows.

2.2 As an example, we prove the commutative law for addition. By definition,

$$(a_n) + (b_n) = (t_n), \text{ where } t_n = a_n + b_n$$
$$(b_n) + (a_n) = (u_n), \text{ where } u_n = b_n + a_n$$

Therefore $u_n = t_n$ for all n, so $(a_n) + (b_n) = (b_n) + (a_n)$.

The associative law for addition is similar. The commutative law for multiplication follows from:

$$(a_n)(b_n) = (t_n), \text{ where } t_n = a_n b_0 + \cdots + a_0 b_n$$
$$(b_n)(a_n) = (u_n), \text{ where } u_n = b_n a_0 + \cdots + b_0 a_n$$

Therefore $u_n = t_n$ for all n, so $(a_n)(b_n) = (b_n)(a_n)$.

The remaining laws can be checked in the same manner.

Next, observe that

$$\begin{aligned}\theta(k+l) &= (k+l, 0, 0, \ldots) \\ &= (k, 0, 0, \ldots) + (l, 0, 0, \ldots) \\ &= \theta(k) + \theta(l)\end{aligned}$$

$$\begin{aligned}\theta(kl) &= (kl, 0, 0, \ldots) \\ &= (k, 0, 0, \ldots)(l, 0, 0, \ldots) \\ &= \theta(k)\theta(l)\end{aligned}$$

Finally, $\theta(k) = 0$ if and only if $(k, 0, 0, \ldots) = (0, 0, 0, \ldots)$, which is true if and only if $k = 0$. Therefore θ is an isomorphism between $\mathbb{C}$ and $\theta(\mathbb{C})$.

Identify $a \in \mathbb{C}$ with $\theta(a)$, and let $t = (0, 1, 0, \ldots)$. Then $t^2 = (0, 0, 1, 0, \ldots)$, $t^3 = (0, 0, 0, 1, \ldots)$, and inductively

$$t^N = (\underbrace{0, \ldots, 0}_{N}, 1, 0, \ldots)$$

for all $N \in \mathbb{N}$. Therefore

$$a_0 + a_1 t + \cdots + a_N t^N = (a_0, a_1, \ldots a_N, 0, \ldots) = (a_n)$$

since $a_n = 0$ for $n > N$.

2.3 Use similar calculations but express them in the standard notation $a_0 + a_1 t + \cdots + a_N t^N$ for polynomials.

2.4 Let $f(t) = t + 1, g(t) = -t$. Then $\partial f = \partial g = 1$, but $\partial(f + g) = 0$.

2.5* Follow the hint. Consider the z_j as independent indeterminates over $\mathbb{C}$. Then D is a polynomial in the z_j of total degree $0 + 1 + 2 + \cdots + (n-1) = \frac{1}{2}n(n-1)$. Moreover, D vanishes whenever $z_j = z_k$ for all $j \neq k$, and these linear polynomials have no common factor, so D is divisible by $\prod_{j<k}(z_j - z_k)$.

The total degree in the z_j of this product is also $\frac{1}{2}n(n-1)$. Therefore $\prod_{j<k}(z_j - z_k) = kD$ where $k \in \mathbb{C}$. The main diagonal of D contributes a term $1.z_2.z_3^2 \cdots z_n^{n-1}$ to D. Group the factors of $\prod_{j<k}(z_j - z_k)$ as:

$$\begin{aligned}&(z_1 - z_2) \times \\ &(z_1 - z_3)(z_2 - z_3) \times \\ &(z_1 - z_4)(z_2 - z_4)(z_3 - z_4) \times \\ &\cdots \\ &(z_1 - z_n)(z_2 - z_n) \cdots (z_{n-1} - z_n)\end{aligned}$$

The coefficient of $1.z_2.z_3^2 \cdots z_n^{n-1}$ is clearly $1.(-1).1.(-1)\ldots$, where there are $n-1$ factors. So this product equals $(-1)^{-n(n+1)/2}$. Putting it all together,

$$D = (-1)^{-n(n+1)/2} \prod_{j<k} (z_j - z_k)$$

2.6 Suppose that $f(t) = a_0 + a_1 t + \cdots + a_n t^n$ and $f(t) = 0$ for all $t \in \mathbb{C}$. Substitute $t = 1, 2, 3, \ldots$ to get

$$\begin{aligned} a_0 + a_1 + \cdots + a_n &= 0 \\ a_0 + 2a_1 + \cdots + 2^n a_n &= 0 \\ a_0 + 3a_1 + \cdots + 3^n a_n &= 0 \\ &\cdots \\ a_0 + na_1 + \cdots + n^n a_n &= 0 \end{aligned}$$

Consider this as a system of n linear equations in n unknowns a_j. The determinant is

$$\begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & 2 & 4 & \cdots & 2^n \\ 1 & 3 & 9 & \cdots & 3^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & n & n^2 & \cdots & n^n \end{vmatrix}$$

which is nonzero by Exercise 2.5. Therefore all $a_j = 0$.

2.7 Let $f(t) = t^3 + pt^2 + qt + r$ where $p, q, r \in \mathbb{R}$. (Without loss of generality the leading coefficient is 1.) There exists $M > 0$ such that

$$\begin{aligned} t < -M &\implies f(t) < 0 \\ t > M &\implies f(t) > 0 \end{aligned}$$

Since f is continuous, the Intermediate Value Theorem implies that $f(a) = 0$ for some $a \in (-M, M)$. Therefore $f(t) = (t-a)(t^2 + \alpha t + \beta)$ for some $\alpha, \beta \in \mathbb{R}$. Now use the quadratic formula to write $t^2 + \alpha t + \beta = (t-b)(t-c)$ for $b, c \in \mathbb{C}$.

2.8* There are at least two ways to answer this question.

(a) Use Cardano's formula to find at east one complex root, and then argue as in the real case by factoring out that root to get a quadratic. (Or use Cardano's formula to find three complex roots.) You will need to prove that every complex number has a cube root. This can be done using DeMoivre's Formula

$$(r(\cos\theta + i\sin\theta))^3 = r^3(\cos 3\theta + i \sin 3\theta)$$

or equivalently

$$\sqrt[3]{r(\cos\theta + i\sin\theta)} = \sqrt[3]{r}\left(\cos\frac{\theta}{3} + i\sin\frac{\theta}{3}\right)$$

(b) The second, which probably resembles what Euler had in mind, is to analyse the curves in the plane defined by the vanishing of the real and imaginary parts of the cubic. Where the curves cross, we obtain a root.

We sketch the method, which is topological. Intuitively plausible features of the geometry will not be verified here. (I am not claiming that these verifications are trivial!)

By scaling z to make the polynomial have leading coefficient 1, and using a Tschirnhaus transformation to remove the quadratic term, we can without loss of generality start with $f(z) = z^3 + pz + q$ where $p, q \in \mathbb{C}$. Define $z = x + iy$, so that

$$\begin{aligned} z^2 &= (x^2 - y^2) + 2ixy \\ z^3 &= (x^3 - 3xy^2) + i(3x^2y - y^3) \end{aligned}$$

Let

$$p = a + ib \qquad q = c + id$$

Then

$$\begin{aligned} g(x, y) = \mathrm{Re} f(z) &= x^3 - 3xy^2 + ax - by + c \\ h(x, y) = \mathrm{Im} f(z) &= 3x^2y - y^3 + bx + ay + d \end{aligned}$$

and we want to prove that the curves

$$R = \{(x, y) : g(x, y) = 0\} \qquad I = \{(x, y) : h(x, y) = 0\}$$

in $\mathbb{R}^2$ must intersect. Any such intersection point corresponds to a zero (x, y) of f.

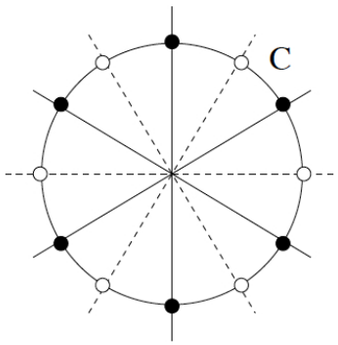

Figure 3: Asymptotic form of the curves.

If $|z|^2 = x^2 + y^2$ is very large, then the behaviour of g and g is dominated by their highest order terms, the cubic terms $\hat{g}(x, y) = x^3 - 3xy^2$ and $\hat{h}(x, y) = 3x^2y - y^3$. So the curve R is asymptotic to the curve

$$\hat{R} = \{(x, y) : \hat{g}(x, y) = 0\}$$

which consists of three straight lines through the origin: $x = 0, x = \sqrt{3}y$, and $x = -\sqrt{3}y$, shown by the solid lines in Figure 3. Similarly the curve I is asymptotic to the curve

$$\hat{I} = \{(x, y) : \hat{h}(x, y) = 0\}$$

which consists of the three dotted lines in Figure 3.

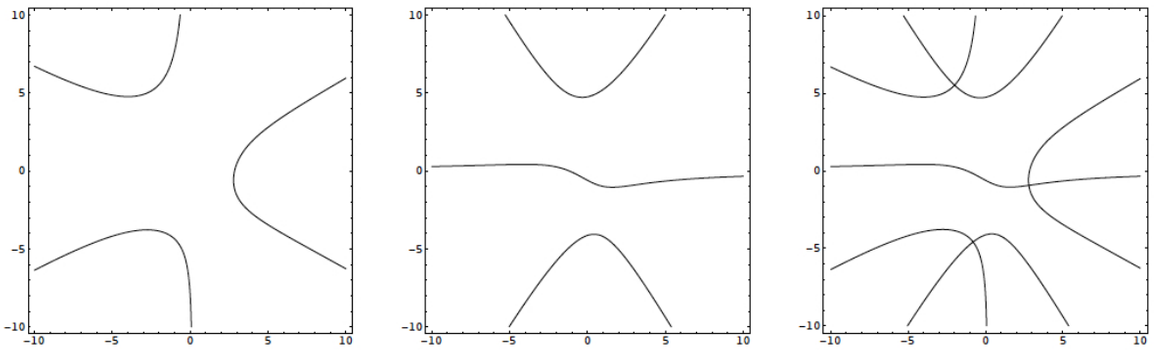

Figure 4: Curves defined by real (left) and imaginary (centre) parts of cubic polynomial. When they are superposed (right) it can be seen that they meet in 3 points.

Each of these sets of lines cuts any circle C in 6 points, which alternate between $\hat{R}$ and $\hat{I}$ round the circle (black and white dots).

If the circle is large enough, we can drop the hats: R meets C in 6 points very close to those to $\hat{R}$, and I meets C in 6 points very close to those to $\hat{I}$. Figure 4 shows a typical case. Here $a = 20, b = 10, c = -80, d = 12$. The curves R, I meet in three points, corresponding to the three zeros.

We claim that whatever the values of a, b, c, d may be, the corresponding curves R, I must have at least one point of intersection. The argument is topological.

By general properties of two-variable polynomial equations, R consists of a finite set of continuous curves, each of which joins two of the associated 6 points, plus (perhaps) other isolated curves inside the circle C. These curves can cross each other, and may have cusp points, but the important property is continuity. Ignore any isolated close curves inside C, and consider one of the curves that constitute R. Call this A. It must join some two of the six black dots, and there are three possibilities, shown in Figure 5.

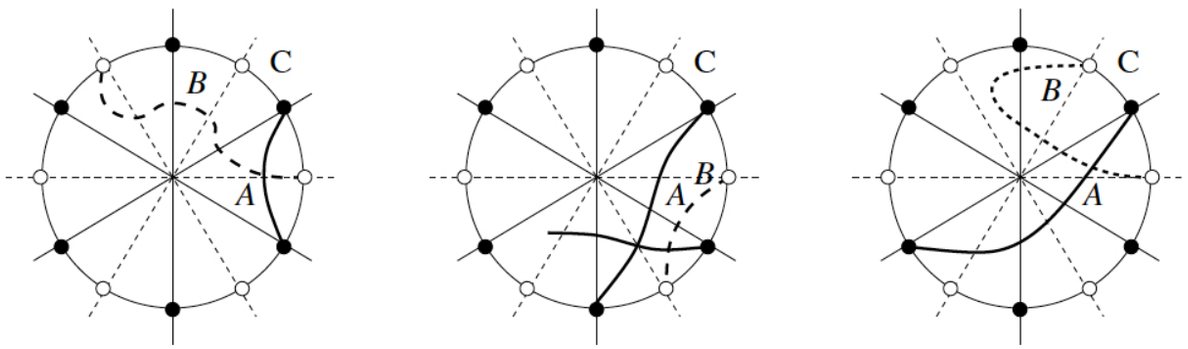

Figure 5: Topology of the intersections.

The curve A divides the interior of the circle C into two regions, one of which contains either 1, 2,or 3 white dots. If the number is odd (1 or 3) then at least one dotted

curve emanating from one of these dots does not terminate at the other,and hence must intersect A. If the number is even (hence 2) then those two white dots are joined by a curve B. Either B meets A, or it is entirely contained inside the region cut off by A. In the latter case, there is a single black dot inside the region cut off by B, and the curve emanating from that dot must meet B.

Therefore R and I must intersect in at least one point $(x, y) \in \mathbb{R}^2 \equiv \mathbb{C}$, and this point gives a zero $x + iy$ of f.

2.9 (a) F. (b) F. (c) F. (d) F. (e) T. (f) F.

3 Factorisation of Polynomials

3.1

(a) $q = t^4 - 7t + 1, r = 49t + 12$.

(b) $q = 1, r = 1$.

(c) $q = 2t^2 - \frac{27}{2}t + \frac{137}{4}, r = -\frac{697}{4}$.

(d) $q = t^2 - 1, r = 0$.

(e) $q = \frac{1}{3}t^2 - \frac{1}{3}t + \frac{1}{3}, r = -t - 1$.

3.2 (a) 1. (b) 1. (c) 1. (d) $t^2 + 1$. (e) $t + 1$.

3.3 (a)

$$a = \frac{2401}{821825}t^6 - \frac{588}{821825}t^5 + \frac{144}{821825}t^4 - \frac{16807}{821825}t^3 + \frac{343}{164363}t^2 - \frac{84}{164363}t + + \frac{23501}{164363}$$
$$b = -\frac{2401}{821815}t^2 + \frac{588}{821815}t - \frac{144}{821815}$$

(b)
$$a = 1 \qquad b = -1$$

(c)
$$a = -\frac{4}{697} \qquad b = \frac{8}{697}t^2 - \frac{54}{697}t + \frac{137}{697}$$

(d)
$$a = 1 \qquad b = 0$$

(e)
$$a = 1 \qquad b = -\frac{1}{3}t^2 + \frac{1}{3}t - \frac{1}{3}$$

3.4 (a) Reducible since $t^4 + 1 = (t^2 + 1)^2 - 2t^2 = (t^2 + 1)^2 - (\sqrt{2}t)^2 = (t^2 + \sqrt{2}t + 1)(t^2 - \sqrt{2}t + 1)$.

(b) Irreducible since the two quadratics $t^2 \pm \sqrt{2}t + 1$ have no rational zeros. (If they did, $\sqrt{2}$ would be rational.)

(c) Irreducible by Eisenstein's Criterion with $p = 11$.

(d) $t^3 + t^2 + t + 1 = t^2(t + 1) + (t + 1) = (t^2 + 1)(t + 1)$, hence reducible.

(e) $t^3 - 7t^2 + 3t = 3$ vanishes when $t = 1$, so $t - 1$ is a factor. Reducible.