SOLUTIONS MANUAL FOR

Galois Theory

by

Ian Stewart

CRC Press
Taylor & Francis Group

SOLUTIONS MANUAL FOR
Galois Theory

by

Ian Stewart

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed on acid-free paper
Version Date: 20150825

International Standard Book Number-13: 978-1-4822-4586-8 (Ancillary)

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Galois Theory
Fourth Edition

Solutions Manual

Ian Stewart
Mathematics Institute
University of Warwick
Coventry CV4 7AL
United Kingdom

October 2, 2014

Introduction

This *Solutions Manual* contains solutions to all of the exercises in the Fourth Edition of *Galois Theory*.

Many of the exercises have several different solutions, or can be solved using several different methods. If your solution is different from the one presented here, it may still be correct—unless it is the kind of question that has only one answer.

The written style is informal, and the main aim is to illustrate the key ideas involved in answering the questions. Instructors may need to fill in additional details where these are straightforward, or explain assumed background material. On the whole, I have emphasised 'bare hands' methods whenever possible, so some of the exercises may have more elegant solutions that use higher-powered methods.

Ian Stewart
Coventry October 2014

1 Classical Algebra

1.1 Let $u = x + iy \equiv (x, y), v = a + ib \equiv (a, b), w = p + iq \equiv (p, q)$. Then

$$\begin{aligned} uv &= (x, y)(a, b) \\ &= (xa - yb, xb + ya) \\ &= (ax - by, bx + ay) \\ &= (a, b)(x, y) \\ &= vu \end{aligned}$$

$$\begin{aligned} (uv)w &= [(x, y)(a, b)](p, q) \\ &= (xa - yb, xb + ya)(p, q) \\ &= (xap - ybp - xbq - yaq, xaq - ybq + xbp + yap) \\ &= (x, y)(ap - bq, aq + bp) \\ &= (x, y)[(a, b)(p, q)] \\ &= (uv)w \end{aligned}$$

1.2

(1) Changing the signs of a, b does not affect $(a/b)^2$, so we may assume $a, b > 0$.

(2) Any non-empty set of positive integers has a minimal element. Since $b > 0$ is an integer, the set of possible elements b has a minimal element.

(3) We know that $a^2 = 2b^2$. Then

$$\begin{aligned} (2b - a)^2 - 2(a - b)^2 &= 4b^2 - 4ab + a^2 - 2(a^2 - 2ab + b^2) \\ &= 2b^2 - a^2 = 0 \end{aligned}$$

(4) If $2b \leq a$ then $4b^2 \leq a^2 = 2b^2$, a contradiction. If $a \leq b$ then $2a^2 \leq 2b^2 = a^2$, a contradiction.

(5) If $a - b \geq b$ then $a \geq 2b$ so $a^2 \geq 4b^2 = 2a^2$, a contradiction. Now (3) contradicts the minimality of b.

Note on the Greek approach.

The ancient Greeks did not use algebra. They expressed them same underlying idea in terms of a geometric figure, Figure 1.

Start with square ABCD and let CE = AB. Complete square AEFG. The rest of the figure leads to a point H on AF. Clearly AC/AB = AF/AE. In modern notation, let AB = b', AC = a'. Since AB = HF = AB and BH = AC, we have AE = $a' + b' - b$, say, and AF = $a' + 2b' = a$, say. Therefore $a' + b' - b, b' = a - b$, and $\frac{a}{b} = \frac{a'}{b'}$.

If $\sqrt{2}$ is rational, we can make a, b integers, in which case a', b' are also integers, and the same process of constructing rationals equal to $\sqrt{2}$ with ever-decreasing numerators

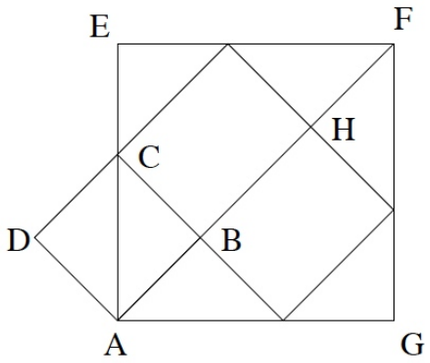

Figure 1: Greek proof that $\sqrt{2}$ is irrational.

and denominators could be carried out. The Greeks didn't argue the proof quite that way: they observed that the 'anthyphaeresis' of AF and AE goes on forever. This process was their version of what we now call the continued fraction expansion (or the Euclidean algorithm, which is equivalent). It stops after finitely many steps if and only if the initial ratio lies in $\mathbb{Q}$. See Fowler (1987) pages 33–35.

1.3 A nonzero rational can be written *uniquely*, up to order, as a produce of prime powers (with a sign $\pm$):

$$r = \pm p_1^{m_1} \cdots p_k^{m_k}$$

where the m_j are integers. So

$$r^2 = \pm p_1^{2m_1} \cdots p_k^{2m_k}$$

Now $\sqrt{q} = r$ if and only if $q = r^2$, and all exponents $2m_j$ are even.

1.4* Clearly $18 \pm \sqrt{325} = 18 \pm 5\sqrt{13}$. A little experiment shows that

$$\left(\frac{3 \pm \sqrt{13}}{2}\right)^3 = 18 \pm 5\sqrt{13}$$

(The factor $\frac{1}{2}$ is the only real surprise here: it occurs 'because' 13 is of the form $4n+1$, but it would take us too far afield to explain that.) At any rate,

$$\sqrt[3]{18 \pm 5\sqrt{13}} = \frac{3 \pm \sqrt{13}}{2}$$

so that

$$\begin{aligned}\sqrt[3]{18 + 5\sqrt{13}} + \sqrt[3]{18 - 5\sqrt{13}} &= \frac{3 + \sqrt{13}}{2} + \frac{3 - \sqrt{13}}{2} \\ &= \frac{3}{2} + \frac{3}{2} = 3\end{aligned}$$

1.5 Let K be the set of all $p + q\alpha + r\alpha^2$, where $p, q, r \in \mathbb{Q}$. Clearly K is closed under addition and subtraction. Since $\alpha^3 = 2$ we also have $\alpha^4 = 2\alpha$, and it follows easily that K is closed under multiplication.

Tedious but elementary calculations, or computer algebra, show that

$$(p+q\alpha+r\alpha^2)(p+q\omega\alpha+r\omega^2\alpha^2)(p+q\omega^2\alpha+r\omega\alpha^2) = p^3+2(q^3-3pqr)+4r^3 \qquad (1)$$

so that

$$(p+q\alpha+r\alpha^2)^{-1} = \frac{(p+q\omega\alpha+r\omega^2\alpha^2)(p+q\omega^2\alpha+r\omega\alpha^2)}{p^3+2(q^3-3pqr)+4r^3}$$

implying closure under inverses, hence division. (It is necessary to check that $p^3+2(q^3-3pqr)+4r^3=0$ in rational numbers implies $p=q=r=0$. By (1) $p^3+2(q^3-3pqr)+4r^3=0$ implies that $p+q\alpha+r\alpha^2=0$ or $p+q\omega\alpha+r\omega^2\alpha^2=0$ or $p+q\omega^2\alpha+r\omega\alpha^2=0$. The required result follows since $1,\alpha,\alpha^2$ are linearly independent over $\mathbb{Q}$.)

1.6 The map is one-to-one since it is linear in (p,q,r) and $p+q\omega^2\alpha+r\omega\alpha^2=0$ implies $p=q=r=0$. Compute

$$(p+q\alpha+r\alpha^2)(a+b\alpha+c\alpha^2) = (pa+2qc+2rb)+(pb+qa+2rc)\alpha+(pc+qb+ra)\alpha^2$$

and compare with

$$(p+q\omega\alpha+r\omega^2\alpha^2)(a+b\omega\alpha+c\omega^2\alpha^2) = (pa+2qc+2rb)+(pb+qa+2rc)\omega\alpha+(pc+qb+ra)\omega^2\alpha^2$$

The coefficients are there same in both formulas, so products are preserved as required. Thus the map is a monomorphism.

All maps are onto their image. But the image here is not $\mathbb{Q}(\alpha)$ because $\mathbb{Q}(\alpha)\subseteq\mathbb{R}$, but $\omega\notin\mathbb{R}$. So the map is not an automorphism.

1.7 Observe that

$$(2+i)^3 = 2\pm 11i = 2\pm\sqrt{-121}$$

and $(2+11i)+(2-11i)=4$.

1.8 The inequality $27pq^2+4p^3<0$ implies that $p<0$, so we can find a,b such that $p=-3a^2, q=-a^2b$, and the cubic becomes

$$t^3-3a^2t=a^2b$$

The inequality becomes $a>|b|/2$. Substitute $t=2a\cos\theta$, and observe that

$$t^3-3a^2t = 8a^3\cos^3\theta-6a^3\cos\theta = 2a^3\cos 3\theta$$

The cubic thus reduces to

$$\cos 3\theta = \frac{b}{2a}$$

which we can solve using $\cos^{-1}$ because $|\frac{b}{2a}|\le 1$, getting

$$\theta = \frac{1}{3}\cos^{-1}\frac{b}{2a}$$

There are three possible values of θ, the other two being obtained by adding $\frac{2\pi}{3}$ or $\frac{4\pi}{3}$. Finally, eliminate θ to get

$$t = 2a\cos\left(\frac{1}{3}\cos^{-1}\frac{b}{2a}\right)$$

where $a = \sqrt{\frac{-p}{3}}, b = \frac{3q}{p}$.

1.9 By inspection one root is $t = 4$. Factoring out $t - 4$ leads to a quadratic whose roots are $-2 + \sqrt{3}$ and $-2 - \sqrt{3}$.

1.10 If you carry out the algebra, it turns out that trying to solve for α and β leads back to the original cubic equation. Unless the solutions are obvious (in which case the method is pointless) no progress is made.

Specifically, suppose we want to solve $(u + \sqrt{v})^3 = a + \sqrt{b}$ for rational u, v given rational a, b. Then assuming $\sqrt{b}, \sqrt{v}$ are irrational, we are led to

$$u^3 + 3uv = a$$
$$(3u^2 + v)\sqrt{v} = \sqrt{b}$$

It follows easily that $(u - \sqrt{v})^3 = a - \sqrt{b}$, whence

$$u^2 - v = \sqrt[3]{a^2 - b}$$

Therefore we seek a rational solution u of the cubic

$$4u^3 - 3(\sqrt[3]{a^2 - b})u - a = 0$$

and then $v = u^2 - \sqrt[3]{a^2 - b}$.

In our case $a = -\frac{q}{2}, b = \frac{q^2}{4} + \frac{p^3}{27}$, so the cubic is

$$4u^3 + pu = -\frac{q}{2}$$

which is equivalent to $x^3 + px + q = 0$ with $x = 2u$.

1.11* Let $A(n)$ be the number of permissible sequences of length n ending in 0, and let $B(n)$ be the number of permissible sequences of length n ending in 1. We claim that

$$A(n) = A(n-1) + B(n-1) \tag{2}$$
$$B(n) = B(n-1) + A(n-3) \tag{3}$$

Equation (2) holds because every permissible sequence of length n ending in 0 is uniquely of the form $S \cdot 0$ where S is a permissible sequence of length $n - 1$.

Equation (3) holds because every permissible sequence of length n ending in 1 is *either* of the form $S \cdot 1$ where S is a permissible sequence of length $n - 1$ ending with 1, *or* $T \cdot 1$ where S is a permissible sequence of length $n - 1$ ending with 011 (which is not permissible). But sequences of the latter form are precisely those of the form $U \cdot 11$ where U is a permissible sequence of length $n - 3$ ending with 0. Clearly

$$P(n) = A(n) + B(n)$$

From (2, 3)

$$0 = [A(n) - A(n-1) - B(n-1)] + B(n-1) + A(n-3) - B(n)]$$

so

$$B(n-1) = A(n) - A(n-1)$$

and eliminating $B(n-1)$ leads to

$$A(n) = 2A(n-1) - A(n-2) + A(n-4)$$

Similarly

$$B(n) = 2B(n-1) - B(n-2) + B(n-4)$$

Adding and using (2) we get

$$P(n) = 2P(n-1) - P(n-2) + P(n-4) \tag{4}$$

The theory of linear recurrences, see for example Slomson (1991) chapter 6, now tells us that $\frac{P(n+1)}{P(n)}$ tends to a limit as $n \to \infty$. Dividing the recurrence (4) by $P(n-4)$ we get

$$\frac{P(n)}{P(n-4)} = 2\frac{P(n-1)}{P(n-4)} - \frac{P(n-2)}{P(n-4)} + 1$$

which we rewrite as

$$\frac{P(n)}{P(n-1)}\frac{P(n-1)}{P(n-2)}\frac{P(n-2)}{P(n-3)}\frac{P(n-3)}{P(n-4)}$$
$$= 2\frac{P(n-1)}{P(n-2)}\frac{P(n-2)}{P(n-3)}\frac{P(n-3)}{P(n-4)} - \frac{P(n-2)}{P(n-3)}\frac{P(n-3)}{P(n-4)} + 1$$

As $n \to \infty$, all the fractions tend to the same limit x, so

$$x^4 = 2x^3 - x^2 + 1$$

Finally, x must be the largest positive real root of this equation by the general theory of linear recurrences. Now

$$x^4 = 2x^3 - x^2 + 1 = (x^2 - x + 1)(x^2 - x - 1)$$

These two quadratic have roots $\frac{1\pm i\sqrt{3}}{2}, \frac{1\pm\sqrt{5}}{2}$ respectively. The first has complex roots; the largest real root of the second is $x = \frac{1+\sqrt{5}}{2} = 1 \cdot 618034\ldots$, often called the golden number.

1.12*

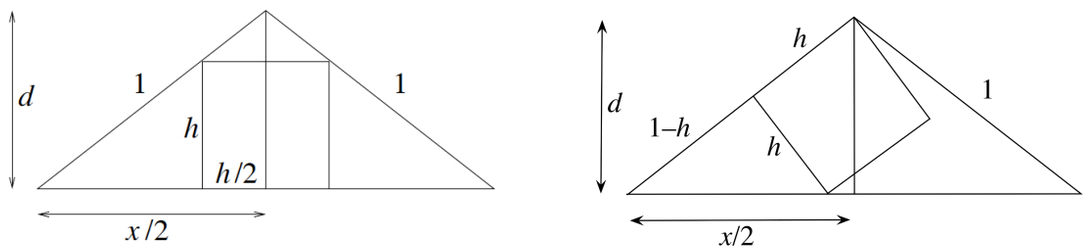

Figure 2: *Left*: Central square in Calabi's triangle. *Right*: Tilted square in Calabi's triangle.

By Pythagoras,

$$d^2 = 1 - \frac{x^2}{4} = \frac{4 - x^2}{4}$$

By similar triangles in Figure 2 (left),

$$\begin{aligned}
\frac{h}{\frac{x}{2}-\frac{h}{2}} &= \frac{d-h}{\frac{h}{2}} \\
h^2 = (d-h)(x-h) &= dx - hx - dh + h^2 \\
0 &= dx - hx - dh \\
h(x+d) &= xd \qquad (5)
\end{aligned}$$

By similar triangles in Figure 2 (right),

$$\begin{aligned}
\frac{h}{1-h} &= \frac{d}{\frac{x}{2}} = \frac{2x}{d} \\
hx &= 2d - 2dh \\
h(x+2d) &= 2d \qquad (6)
\end{aligned}$$

Eliminating h from (5, 6) we get

$$\begin{aligned}
\frac{x+d}{x+2d} &= \frac{xd}{2d} = \frac{x}{2} \\
2(x+d) &= x(x+2d) \\
2x+2d &= x^2 + dx \\
d(2-2x) &= x^2 - 2x = x(x-2) \\
d^2(2-2x)^2 &= x^2(x-2)^2 \\
\frac{4-x^2}{4}(2-2x)^2 &= x^2(x-2)^2 \\
(4-x^2)(2-2x)^2 &= x^2(x-2)^2 \\
(x-2)^2(x+2) + x^2(x-2) &= 0 \\
2x^3 - 2x^2 - 3x + 2 &= 0
\end{aligned}$$

as required. Numerically, $x \sim 1 \cdot 551$.

1.13

We seek p, q, r, s such that

$$x^4 + ax^3 + bx^2 + cx + d = (x^2 + px + q)^2 - (rx + s)^2$$

which leads to

$$\begin{aligned}
2p &= a \\
p^2 + 2q - r^2 &= b \\
2pq - 2rs &= c \\
q^2 - s^2 &= d
\end{aligned}$$

Clearly we must set $p = a/2$. Set $q = (b + r^2 - a^2/4)/2$ to solve the second equation for q in terms of r, and

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

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.

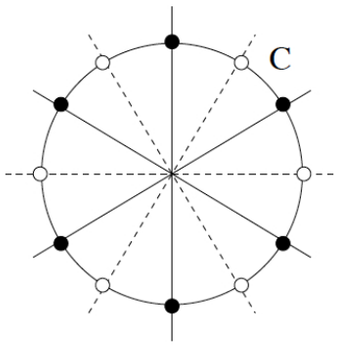

Figure 3: Asymptotic form of the curves.

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.