ROOTS OF POLYNOMIALS OF DEGREES 3 AND 4

SVANTE JANSON

Abstract. We present the solutions of equations of degrees 3 and 4 using Galois theory and some simple Fourier analysis for finite groups.

1. Introduction

The purpose of this note is to present the solutions of equations of degrees 3 and 4 (a.k.a. cubic and quartic equations) in a way connected to Galois theory. This is, of course, not the historical path; the solutions were found by del Ferro, Tartaglia, Cardano (Cardan) and Ferrari in the 16th century, see Appendix B, about 300 years before Galois theory was created. But in retrospect, Galois theory yields the solutions rather easily. More precisely, we will see below that Galois theory, together with some simple Fourier analysis for (small) finite Abelian groups, suggests the crucial constructions in the solutions; however, all calculations are easily verified directly, and we do not really need any results from Galois theory (or Fourier analysis) for the solution. Nevertheless, we find it instructive to use Galois theory as much as possible in order to motivate the constructions. (See also [21, Section 8.8] for a similar, but not identical, treatment.) The Galois theory used here can be found in e.g. [2], [4], [8], [9] or [21].

The appendices contain comments on the history of the problem, other solutions, and (Appendix A) the complications that may arise when we work with real numbers instead of complex.

Remark 1.1. In contrast, full use of Galois theory is needed to show the impossibility of similar formulas for solutions of equations of degree 5 or more. This will not be discussed here; see instead e.g. [2], [4], [8], [9] or [21].

We let throughout K be a field with characteristic 0. (Actually, everything in this note is valid also for a field K of positive characteristic $p \neq 2, 3$. However, the cases when the characteristic is 2 or 3 are different since we divide by 2 and 3 in the formulas below; there are also problems with separability in these cases.)

The roots of a polynomial in $K[x]$ are, in general, not elements of K, so we will work in some unspecified extension of K. This extension could be the algebraic closure $\overline{K}$ of K or some other algebraically closed field containing K; in particular, if $K = \mathbb{Q}$ or another subfield of $\mathbb{C}$ (as the reader may assume for simplicity), we can work in $\mathbb{C}$.

Date: 1 December 2009; revised 17 August 2010.

For simplicity we consider monic polynomials only. (It is trivial to reduce to this case by dividing by the leading coefficient.)

2. Polynomials of degree 3

Let $f(x) = x^3 + bx^2 + cx + d$, with $b, c, d \in K$, be a polynomial of degree 3, and let $\alpha_1, \alpha_2, \alpha_3$ be its roots in some extension of K. Thus

$$f(x) = x^3 + bx^2 + cx + d = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3). \tag{2.1}$$

It is convenient to make the translation $x = y - b/3$, converting $f(x)$ into

$$g(y) := f(y - b/3) = y^3 + py + q \tag{2.2}$$

(without second degree term) for some $p, q \in K$. (Such polynomials, without the second highest degree term, are called *reduced* or sometimes *depressed*.) Thus g has the roots $\beta_1, \beta_2, \beta_3$ with $\beta_i = \alpha_i + b/3$, so $\alpha_i = \beta_i - b/3$, $i = 1, \dots, 3$. Hence,

$$g(y) = y^3 + py + q = (y - \beta_1)(y - \beta_2)(y - \beta_3). \tag{2.3}$$

Consequently, identifying coefficients,

$$\beta_1 + \beta_2 + \beta_3 = 0, \tag{2.4}$$

$$\beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3 = p, \tag{2.5}$$

$$\beta_1\beta_2\beta_3 = -q, \tag{2.6}$$

Remark 2.1. Explicitly,

$$p = c - \tfrac{1}{3}b^2, \tag{2.7}$$

$$q = d - \tfrac{1}{3}bc + \tfrac{2}{27}b^3. \tag{2.8}$$

The polynomials f and g have the same discriminant

$$\Delta := \operatorname{Dis}(f) = \operatorname{Dis}(g) := \prod_{1 \le i < j \le 3} (\alpha_i - \alpha_j)^2 = \prod_{1 \le i < j \le 3} (\beta_i - \beta_j)^2. \tag{2.9}$$

Since Δ is a symmetric polynomial in $\alpha_1, \alpha_2, \alpha_3$ (or $\beta_1, \beta_2, \beta_3$), it can be written as a polynomial in the coefficients of f or g. A well-known calculation yields, see e.g. [14],

$$\Delta = b^2c^2 - 4c^3 - 4b^3d + 18bcd - 27d^2 = -4p^3 - 27q^2. \tag{2.10}$$

We also define the square root of Δ:

$$\delta := \prod_{1 \le i < j \le 3} (\alpha_i - \alpha_j) = \prod_{1 \le i < j \le 3} (\beta_i - \beta_j) = \sqrt{\Delta}. \tag{2.11}$$

Note that while Δ is independent of the ordering of the roots, the sign of δ may change if we permute $\alpha_1, \alpha_2, \alpha_3$. More precisely, the sign is preserved by an even permutation but is changed by an odd permutation.

Let $E = K(\alpha_1, \alpha_2, \alpha_3) = K(\beta_1, \beta_2, \beta_3)$ be the splitting field of f, or g, over K, and let $G := \operatorname{Gal}(E : K)$ be the Galois group of the extension $E \supseteq K$. The elements of the Galois group G permute the roots α_i (or β_i), and G

may be regarded as a subgroup of the symmetric group S_3. As said above, $\sigma(\delta) = \delta$ if $\sigma \in G$ is an even permutation, while $\sigma(\delta) = -\delta$ if σ is odd. Since $K \subseteq K(\delta) \subseteq E$, E is a Galois extension of $K(\delta)$, and the Galois group $\mathrm{Gal}(E : K(\delta))$ is the subgroup of G fixing δ:

$$\mathrm{Gal}(E : K(\delta)) = \{\sigma \in G : \sigma(\delta) = \delta\} = \{\sigma \in G : \sigma \text{ is even}\} = G \cap A_3 \quad (2.12)$$

(where A_3 is the alternating group consisting of all even permutations in S_3), at least if $\delta \neq 0$, or equivalently $\Delta \neq 0$, which is equivalent to f separable (i.e., f has no multiple roots in $\overline{K}$). In particular, if f is irreducible, in which case G is transitive and thus $G = S_3$ or A_3, $\mathrm{Gal}(E : K(\delta)) = A_3$, which is the cyclic group C_3. Moreover, in this case, $\mathrm{Gal}(E : K(\delta)) = A_3 \cong C_3$ acts on the vectors $(\alpha_1, \alpha_2, \alpha_3)$ and $(\beta_1, \beta_2, \beta_3)$ by cyclic permutations; equivalently, if we regard these vectors as functions on $\mathbb{Z}_3 \cong C_3$, $\mathrm{Gal}(E : K(\delta)) \cong C_3$ acts by translations in C_3. This suggests using Fourier analysis, or equivalently group representation theory, for $A_3 \cong C_3$. (For Fourier analysis on finite Abelian groups, see e.g. [7]; in this case, the Fourier transform is often called the *discrete Fourier transform*. The more complicated theory of group representations for general finite groups is treated by [20].)

Remark 2.2. The method below was given by Lagrange [17] in 1770–1771, as part of his study of equations of higher degree, see [4, Sections 8.3, 12.1 and p. 14]. The method is thus some decades older than both Galois theory and Fourier analysis. In this context, the Fourier transforms u and v in (2.17)–(2.18) below (or rather $3u$ and $3v$) are known as the *Lagrange resolvents* for the equation. (They were also used earlier by Bézout and Euler [2, p. 46], and at the same time by Vandermonde [22], but Lagrange made a profound use of them.) Lagrange and others used this method to study equations of arbitrary degree, see [4, Sections 8.3 and 12.1] and, for example, the solutions by Vandermonde and Malfatti of some quintic equations givin in [2, Chapters 7–8]. This is an important forerunner of Galois theory. In retrospect, the Lagrangre resolvents can perhaps also be seen as the beginning of discrete Fourier analysis.

We assume, for simplicity, that $K \subseteq \mathbb{C}$, and we then define

$$\omega := \exp(2\pi \mathrm{i}/3) = -\frac{1}{2} + \frac{\sqrt{3}}{2}\mathrm{i}, \quad (2.13)$$

a primitive third root of unity. Note that

$$\omega^3 = 1, \qquad 1 + \omega + \omega^2 = 0, \quad (2.14)$$

which will be used repeatedly below without further comment.

Remark 2.3. For a general field K, not necessarily contained in $\mathbb{C}$, we can let ω be a primitive third root of unity in $\overline{K}$. It is easily verified that the formulas below make sense, and are correct, in $\overline{K}$, so the result holds in full generality.

We then define the Fourier transform of a vector (z_1, z_2, z_3) (regarded as a function on $\mathbb{Z}_3 \cong C_3$) as $(\widehat{z}_1, \widehat{z}_2, \widehat{z}_3)$, with

$$\widehat{z}_k := \tfrac{1}{3}\bigl(z_1 + \omega^{-(k-1)} z_2 + \omega^{-2(k-1)} z_3\bigr), \tag{2.15}$$

and note the Fourier inversion formula, which in this case is easily verified directly,

$$z_k = \widehat{z}_1 + \omega^{k-1}\widehat{z}_2 + \omega^{2(k-1)}\widehat{z}_3. \tag{2.16}$$

Hence, if we define

$$u := \tfrac{1}{3}(\alpha_1 + \omega^2\alpha_2 + \omega\alpha_3) = \tfrac{1}{3}(\beta_1 + \omega^2\beta_2 + \omega\beta_3), \tag{2.17}$$

$$v := \tfrac{1}{3}(\alpha_1 + \omega\alpha_2 + \omega^2\alpha_3) = \tfrac{1}{3}(\beta_1 + \omega\beta_2 + \omega^2\beta_3), \tag{2.18}$$

and note that

$$-\tfrac{1}{3}b = \tfrac{1}{3}(\alpha_1 + \alpha_2 + \alpha_3), \tag{2.19}$$

$$0 = \tfrac{1}{3}(\beta_1 + \beta_2 + \beta_3), \tag{2.20}$$

we see that the Fourier transforms of the vectors $(\alpha_1, \alpha_2, \alpha_3)$ and $(\beta_1, \beta_2, \beta_3)$ are $(-\frac{1}{3}b, u, v)$ and $(0, u, v)$, respectively. Consequently, the inversion formula (2.16) yields

$$\alpha_1 = -\tfrac{1}{3}b + u + v, \tag{2.21}$$

$$\alpha_2 = -\tfrac{1}{3}b + \omega u + \omega^2 v, \tag{2.22}$$

$$\alpha_3 = -\tfrac{1}{3}b + \omega^2 u + \omega v, \tag{2.23}$$

and, equivalently,

$$\beta_1 = u + v, \tag{2.24}$$

$$\beta_2 = \omega u + \omega^2 v, \tag{2.25}$$

$$\beta_3 = \omega^2 u + \omega v. \tag{2.26}$$

To solve the equation $f(x) = 0$, it thus suffices to find u and v.

The objects u and v are elements of the field $E(\omega)$, which is the splitting field of f (or g) over $K(\omega)$. It is thus a Galois extension of $K(\omega)$, and also of the intermediate field $K(\delta, \omega)$. An element of the Galois group $\mathrm{Gal}(E(\omega) : K(\omega))$ maps E into itself (because it fixes K and E is a normal extension of K), and thus its restriction to E is an element of $\mathrm{Gal}(E : K)$. This defines a group homomorphism $\mathrm{Gal}(E(\omega) : K(\omega)) \to \mathrm{Gal}(E : K)$, which is injective because $E(\omega)$ is generated by E and $K(\omega)$; thus we can regard $\mathrm{Gal}(E(\omega) : K(\omega))$ as a subgroup of $\mathrm{Gal}(E : K)$. Similarly, $\mathrm{Gal}(E(\omega) : K(\delta, \omega))$ is a subgroup of $\mathrm{Gal}(E : K(\delta))$.

Let $H := \mathrm{Gal}(E(\omega) : K(\delta, \omega))$. Then $H \subseteq \mathrm{Gal}(E : K(\delta)) \subseteq A_3$, so if H is not trivial, then $H = A_3$ and H is generated by a cyclic permutation σ with $\sigma(\alpha_k) = \alpha_{k+1}$ (with indices modulo 3). Then, by (2.17)–(2.18), $\sigma(u) = \omega u$ and $\sigma(v) = \omega^2 v$. Consequently, $\sigma(u^3) = u^3$, and $\sigma(v^3) = v^3$. This implies that u^3 and v^3 are fixed by the Galois group H, and thus u^3 and v^3 belong to the fixed field $\mathrm{Fix}_{E(\omega)}(H) = K(\delta, \omega)$. We can find them as follows, using

$x^3-1=(x-1)(x-\omega)(x-\omega^2)$ and thus $x^3-y^3=(x-y)(x-\omega y)(x-\omega^2 y)$: First, by (2.24)–(2.26) and (2.6),

$$u^3+v^3=(u+v)(u+\omega v)(u+\omega^2 v)=\beta_1\beta_2\beta_3=-q. \tag{2.27}$$

Next, by (2.17)–(2.18),

$$u-v=\tfrac13(\omega^2-\omega)(\alpha_2-\alpha_3) \tag{2.28}$$

$$u-\omega v=\tfrac13(1-\omega)(\alpha_1-\alpha_3) \tag{2.29}$$

$$u-\omega^2 v=\tfrac13(1-\omega^2)(\alpha_1-\alpha_2) \tag{2.30}$$

and thus, using (2.11),

$$\begin{aligned} u^3-v^3=(u-v)(u-\omega v)(u-\omega^2 v)&=\frac{-\sqrt{3}\,\mathrm{i}}{9}(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_2-\alpha_3)\\ &=-\frac{\sqrt{3}\,\mathrm{i}}{9}\delta=\sqrt{-\frac{\Delta}{27}}. \end{aligned} \tag{2.31}$$

Remark 2.4. The choice of square root in (2.31) is not important, since a change of sign of it is equivalent to an interchange of u and v, which just permutes the roots α_2 and α_3 (β_2 and β_3).) This reflects the fact that if the Galois group $\mathrm{Gal}(E(\omega):K(\omega))$ contains an odd permutation τ, then $\tau(u)=\omega^j v$ and $\tau(v)=\omega^j u$ for some $j=0,1,2$; thus $\tau(u^3)=v^3$ and $\tau(v^3)=u^3$.

We thus find, recalling (2.10),

$$u^3=\frac{-q+\sqrt{-\Delta/27}}{2}=-\frac{q}{2}+\sqrt{\frac{-\Delta}{108}}=-\frac{q}{2}+\sqrt{\Big(\frac{p}{3}\Big)^3+\Big(\frac{q}{2}\Big)^2}, \tag{2.32}$$

$$v^3=\frac{-q-\sqrt{-\Delta/27}}{2}=-\frac{q}{2}-\sqrt{\frac{-\Delta}{108}}=-\frac{q}{2}-\sqrt{\Big(\frac{p}{3}\Big)^3+\Big(\frac{q}{2}\Big)^2}. \tag{2.33}$$

We then find u and v by taking cube roots. In order to choose the right roots, we also compute, from (2.17)–(2.18) and (2.4)–(2.5),

$$\begin{aligned} uv&=\tfrac19\big(\beta_1^2+\beta_2^2+\beta_3^2+(\omega+\omega^2)(\beta_1\beta_2+\beta_1\beta_3+\beta_2\beta_3)\big)\\ &=\tfrac19\big((\beta_1+\beta_2+\beta_3)^2-3(\beta_1\beta_2+\beta_1\beta_3+\beta_2\beta_3)\big)\\ &=-\tfrac13 p. \end{aligned} \tag{2.34}$$

If we replace u by the alternative cube root ωu or $\omega^2 u$, we thus have to replace v by $\omega^2 v$ or ωv, respectively, which by (2.21)–(2.23) and (2.24)–(2.26) yields a cyclic permutation of the roots $\alpha_1,\alpha_2,\alpha_3$ or β_1,β_2,β_3. We summarize:

Theorem 2.5 (Cardano's formula)**.** *The roots of $g(y)=y^3+py+q$ are given by*

$$\sqrt[3]{-\frac{q}{2}+\sqrt{\Big(\frac{p}{3}\Big)^3+\Big(\frac{q}{2}\Big)^2}}+\sqrt[3]{-\frac{q}{2}-\sqrt{\Big(\frac{p}{3}\Big)^3+\Big(\frac{q}{2}\Big)^2}}, \tag{2.35}$$

where the two square roots are chosen to be the same, and the two cube roots are chosen such that their product is $-p/3$*; this gives* 3 *choices for the cube roots, which gives the* 3 *roots of* $g(y) = 0$*. (In the exceptional case* $p = q = 0$*, the only root* 0 *is counted thrice.)*

Equivalently, the roots of $f(x) = x^3 + bx^2 + cx + d$ *are given by*

$$\begin{aligned} -\frac{b}{3} &+ \sqrt[3]{-\frac{q}{2}+\sqrt{\Big(\frac{p}{3}\Big)^3+\Big(\frac{q}{2}\Big)^2}} + \sqrt[3]{-\frac{q}{2}-\sqrt{\Big(\frac{p}{3}\Big)^3+\Big(\frac{q}{2}\Big)^2}} \\ &= -\frac{b}{3} + \sqrt[3]{-\frac{q}{2}+\sqrt{\frac{-\Delta}{108}}} + \sqrt[3]{-\frac{q}{2}-\sqrt{\frac{-\Delta}{108}}}, \end{aligned} \tag{2.36}$$

with p *and* q *given by* (2.7)–(2.8)*, and* Δ *given by* (2.10).

Remark 2.6. This formula is known as Cardano's formula since it was first published by Cardano in *Ars Magna* [3], although it is attributed by him to Scipione del Ferro, see Appendix B.

Remark 2.7. The case $p = q = 0$ is exceptional because then (and only then) $u^3 = v^3 = 0$. This is the trivial case when f and g are cubes $(x+b/3)^3$ and y^3 and thus have triple roots $-b/3$ and 0, respectively.

The case with a double (but not triple) root are handled correctly by Theorem 2.5. This is the case when $\Delta = 0$ (but not $p = q = 0$), and thus $u^3 = v^3$ ($\neq 0$). We can find a cube root $u = v$ with $uv = u^2 = -p/3$, and then the other eligible pairs of cube roots are $(\omega u, \omega^2 u)$ and $(\omega^2 u, \omega u)$, yielding the roots $\beta_1 = 2u$, $\beta_2 = \beta_3 = -u$, and thus $\alpha_1 = -b/3 + 2u$, $\alpha_2 = \alpha_3 = -b/3 - u$.

Similarly, there are no problems in the case when u^3 or v^3 is 0, but not both. This happens, by (2.32)–(2.33) and (2.34), when $p = 0$ but $q \neq 0$. Choosing the square root such that $v^3 = 0$, we have $u^3 = -q$; the polynomial $g(y)$ equals $y^3 + q$ which has the three roots u, ωu, $\omega^2 u$.

Remark 2.8. By (2.27) and (2.34), which implies $u^3v^3 = -p^3/27$, u^3 and v^3 are the roots of the *quadratic resolvent*

$$r(x) := x^2 + qx - p^3/27 \in K[x]. \tag{2.37}$$

Note that the quadratic resolvent has discriminant, by (2.31),

$$\operatorname{Dis}(r) := (u^3 - v^3)^2 = -\frac{\Delta}{27} = -\frac{1}{27}\operatorname{Dis}(f). \tag{2.38}$$

3. Polynomials of degree 4

Let $f(x) = x^4 + bx^3 + cx^2 + dx + e$, with $b, c, d, e \in K$, be a polynomial of degree 4, and let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ be its roots in some extension of K. Thus

$$f(x) = x^4 + bx^3 + cx^2 + dx + e = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4). \tag{3.1}$$

It is convenient to make the translation $x = y - b/4$, converting $f(x)$ into

$$g(y) := f(y - b/4) = y^4 + py^2 + qy + r \tag{3.2}$$

(without third degree term) for some $p, q, r \in K$. Thus g has the roots $\beta_1, \beta_2, \beta_3, \beta_4$ with $\beta_i = \alpha_i + b/4$, so $\alpha_i = \beta_i - b/4$, $i = 1, \dots, 4$. Hence,

$$g(y) = y^4 + py^2 + qy + r = (y - \beta_1)(y - \beta_2)(y - \beta_3)(y - \beta_4). \tag{3.3}$$

The polynomials f and g have the same discriminant

$$\Delta := \operatorname{Dis}(f) = \operatorname{Dis}(g) = \prod_{1 \le i < j \le 4} (\alpha_i - \alpha_j)^2 = \prod_{1 \le i < j \le 4} (\beta_i - \beta_j)^2. \tag{3.4}$$

Since Δ is a symmetric polynomial in $\alpha_1, \dots, \alpha_4$ (or $\beta_1, \dots, \beta_4$), it can be written as a polynomial in the coefficients of f or g. A well-known calculation yields, see e.g. [14],

$$\begin{aligned}
\Delta = b^2c^2d^2 - 4\,b^2c^3e - 4\,b^3d^3 + 18\,b^3cde - 27\,b^4e^2 - 4\,c^3d^2 \\
+ 16\,c^4e + 18\,bcd^3 - 80\,bc^2de - 6\,b^2d^2e + 144\,b^2ce^2 \\
- 27\,d^4 + 144\,cd^2e - 128\,c^2e^2 - 192\,bde^2 + 256\,e^3 \qquad (3.5) \\
= -4\,p^3q^2 - 27\,q^4 + 16\,p^4r + 144\,pq^2r - 128\,p^2r^2 + 256\,r^3. \qquad (3.6)
\end{aligned}$$

We also define the square root of Δ:

$$\delta := \prod_{1 \le i < j \le 4} (\alpha_i - \alpha_j) = \prod_{1 \le i < j \le 4} (\beta_i - \beta_j) = \sqrt{\Delta}. \tag{3.7}$$

Again, the sign of δ may change if we permute $\alpha_1, \dots, \alpha_4$; the sign is preserved by an even permutation but is changed by an odd permutation.

Let $E = K(\alpha_1, \dots, \alpha_4) = K(\beta_1, \dots, \beta_4)$ be the splitting field of f, or g, over K, and let $G := \operatorname{Gal}(E : K)$ be the Galois group of the extension $E \supseteq K$. The elements of the Galois group G permute the roots α_i (or β_i), and G may be regarded as a subgroup of S_4.

S_4 has a normal subgroup V consisting of the 4 permutations ι (identity) and (12)(34), (13)(24), (14)(23). Thus G has a normal subgroup $G \cap V$. Let the fixed field of $G \cap V$ be F. Then F is a Galois extension of K with Galois group $G/G \cap V \subseteq S_4/V \cong S_3$.

Fourier analysis on V is especially simple because every element has order 1 or 2, and thus every character is ± 1 (again, see e.g. [7] or [20]). We identify functions on V by vectors (z_1, z_2, z_3, z_4), with z_1 the value at ι, and define the Fourier transform of (z_1, z_2, z_3, z_4) as $(\widehat{z}_1, \widehat{z}_2, \widehat{z}_3, \widehat{z}_4)$ with

$$\widehat{z}_1 := \tfrac{1}{2}(z_1 + z_2 + z_3 + z_4), \tag{3.8}$$

$$\widehat{z}_2 := \tfrac{1}{2}(z_1 + z_2 - z_3 - z_4), \tag{3.9}$$

$$\widehat{z}_3 := \tfrac{1}{2}(z_1 - z_2 + z_3 - z_4), \tag{3.10}$$

$$\widehat{z}_4 := \tfrac{1}{2}(z_1 - z_2 - z_3 + z_4). \tag{3.11}$$

For V, with our chosen normalization, the Fourier inversion formula takes the especially simple form $\widehat{\widehat{z}} = z$, i.e., the Fourier transform is its own inverse. (This is easily verified directly.)

Since $\beta_1+\beta_2+\beta_3+\beta_4=0$, the Fourier coefficient $\widehat{\beta}_1=0$. For convenience, we shift the indices and define $\gamma_i := \widehat{\beta}_{i+1}$, $i=0,1,2,3$, where thus $\gamma_0=0$. The Fourier transforms of $(\alpha_1,\alpha_2,\alpha_3,\alpha_4)$ and $(\beta_1,\beta_2,\beta_3,\beta_4)$ are thus $(-\frac12 b,\gamma_1,\gamma_2,\gamma_3)$ and $(0,\gamma_1,\gamma_2,\gamma_3)$, where

$$\gamma_1 := \widehat{\beta}_2 := \tfrac12(\alpha_1+\alpha_2-\alpha_3-\alpha_4) = \beta_1+\beta_2 = -\beta_3-\beta_4, \tag{3.12}$$

$$\gamma_2 := \widehat{\beta}_3 := \tfrac12(\alpha_1-\alpha_2+\alpha_3-\alpha_4) = \beta_1+\beta_3 = -\beta_2-\beta_4, \tag{3.13}$$

$$\gamma_3 := \widehat{\beta}_4 := \tfrac12(\alpha_1-\alpha_2-\alpha_3+\alpha_4) = \beta_1+\beta_4 = -\beta_2-\beta_3. \tag{3.14}$$

Permutations in V act on the vectors (regarded as functions on V) by translations in V, and thus on the Fourier transforms by multiplying by characters, which are ±1. In other words, permutations in V act on γ_1, γ_2 and γ_3 by multiplying by ±1 (as is easily seen directly from (3.12)–(3.14)). Consequently, if we define

$$u := \gamma_1^2 = (\beta_1+\beta_2)^2 = (\beta_3+\beta_4)^2, \tag{3.15}$$

$$v := \gamma_2^2 = (\beta_1+\beta_3)^2 = (\beta_2+\beta_4)^2, \tag{3.16}$$

$$w := \gamma_3^2 = (\beta_1+\beta_4)^2 = (\beta_2+\beta_3)^2, \tag{3.17}$$

then u, v and w are fixed by $V\cap G$, and the thus belong to the fixed field F. We can easily find them explicitly. If σ is any element of the Galois group G, then σ permutes $\beta_1,\dots,\beta_4$, and it follows from (3.15)–(3.17) that σ permutes u,v,w. Hence any symmetric polynomial in u,v,w is fixed by every $\sigma\in G$, and thus it belongs to K. In particular, this applies to the coefficients of the polynomial $R(x):=(x-u)(x-v)(x-w)$, which thus has coefficients in K. Calculations yield the explicit formulas

$$u+v+w = -2p, \tag{3.18}$$

$$uv+uw+vw = p^2-4r, \tag{3.19}$$

$$uvw = q^2. \tag{3.20}$$

Hence, u, v, w are the three roots of the *cubic resolvent*

$$R(x) := (x-u)(x-v)(x-w) = x^3+2px^2+(p^2-4r)x-q^2 \in K[x]. \tag{3.21}$$

Remark 3.1. Note that $u-v=(\beta_1-\beta_4)(\beta_2-\beta_3)$, $u-w=(\beta_1-\beta_3)(\beta_2-\beta_4)$, $v-w=(\beta_1-\beta_2)(\beta_3-\beta_4)$. Hence the discriminant $(u-v)^2(u-w)^2(v-w)^2$ of the cubic resolvent R equals the discriminant of g or f given by (3.5)–(3.6).

Having found u,v,w, we take their square roots to find $\gamma_1,\gamma_2,\gamma_3$. By (3.20), $\gamma_1\gamma_2\gamma_3=\pm q$. In fact, using (3.12)–(3.14) and $\beta_1+\beta_2+\beta_3+\beta_4=0$,

$$\begin{aligned}
\gamma_1\gamma_2\gamma_3+q &= \gamma_1\gamma_2\gamma_3-(\beta_1\beta_2\beta_3+\beta_1\beta_2\beta_4+\beta_1\beta_3\beta_4+\beta_2\beta_3\beta_4)\\
&= -(\beta_3+\beta_4)(\beta_2+\beta_4)(\beta_2+\beta_3)+(\beta_2+\beta_3+\beta_4)(\beta_2\beta_3+\beta_2\beta_4+\beta_3\beta_4)\\
&\qquad -\beta_2\beta_3\beta_4\\
&= 0.
\end{aligned}$$

Hence,

$$\gamma_1\gamma_2\gamma_3 = -q, \tag{3.22}$$

which provides the information we need on the signs of $\gamma_1, \gamma_2, \gamma_3$. We then find $\beta_1, \dots, \beta_4$ by taking the (inverse) Fourier transform of $(0, \gamma_1, \gamma_2, \gamma_3)$. We summarize the resulting algorithm:

Theorem 3.2. *Let $g(y) = y^4 + py^2 + qy + r$, and define the cubic resolvent $R(x)$ by (3.21). Let the roots of R by u, v, w (for example found by Theorem 2.5), and let $\gamma_1 := \sqrt{u}$, $\gamma_2 := \sqrt{v}$, $\gamma_3 := \sqrt{w}$, where we choose the signs so that $\gamma_1\gamma_2\gamma_3 = -q$. Then the roots of g are given by*

$$\beta_1 = \tfrac{1}{2}(\gamma_1 + \gamma_2 + \gamma_3), \tag{3.23}$$

$$\beta_2 = \tfrac{1}{2}(\gamma_1 - \gamma_2 - \gamma_3), \tag{3.24}$$

$$\beta_3 = \tfrac{1}{2}(-\gamma_1 + \gamma_2 - \gamma_3), \tag{3.25}$$

$$\beta_4 = \tfrac{1}{2}(-\gamma_1 - \gamma_2 + \gamma_3). \tag{3.26}$$

The roots of $f(x) = x + bx^3 + cx^2 + dx + e$ are $\alpha_i = \beta_i - b/4$, $i = 1, \dots, 4$, where $g(y) := f(y - b/4)$.

Note that changing the signs of some of $\gamma_1, \gamma_2, \gamma_3$ while still preserving (3.22) (i.e., changing the sign of exactly two of them), just yields a permutation of $\beta_1, \dots, \beta_4$.

Remark 3.3. The formulas (3.23)–(3.26) were given by Euler [5, §5] in 1733. Euler's motivation was different. For the cubic, Cardano's formula is $\sqrt[3]{U} + \sqrt[3]{V}$ where $U := u^3$ and $V := v^3$ are roots of the quadratic resolvent (2.37). Further, for a quadratic $x^2 = a$ there is the trivial formula $\sqrt{a}$. Hence, Euler sought by analogy a formula for the roots of a quartic in the form $\sqrt{A}+\sqrt{B}+\sqrt{C}$, and found a cubic equation for A, B, C by substituting in $g(y) = 0$, see [5] for details. (In our notation, $A = u/4$, $B = v/4$ and $C = v/4$, so Euler's cubic equation is our $R(4x) = 0$; the difference from our cubic resolvent equation $R(u) = 0$ is thus only a trivial matter of normalization.)

Euler [5, §§6–8] proceeded to write the solution as $\sqrt[4]{E} + \sqrt[4]{F} + \sqrt[4]{G}$ (with $E = A^2$, $F = B^2$, $G = C^2$), and found another cubic equation satisfied by E, F, G. Euler conjectured that similar formulas existed for higher degrees too, and in particular that the roots of a fifth degree equation could be found as $\sqrt[5]{A} + \sqrt[5]{B} + \sqrt[5]{C} + \sqrt[5]{D}$, where A, B, C, D were the roots of some fourth degree resolvent; however, he could not find such a resolvent. Of course, we know that Euler's conjecture cannot hold, since 100 years later it was proved by Abel and Galois that in general there is no solution by radicals for a fifth degree equation.

Remark 3.4. A simple calculation yields, by (3.23)–(3.26) and (3.18),

$$\begin{aligned}\beta_1\beta_2+\beta_3\beta_4&=\frac14\bigl(\gamma_1^2-(\gamma_2+\gamma_3)^2+\gamma_1^2-(\gamma_2-\gamma_3)^2\bigr)\\&=\frac14\bigl(2\gamma_1^2-2\gamma_2^2-2\gamma_3^2\bigr)=\frac12\bigl(u-v-w\bigr)=u+p\end{aligned}\tag{3.27}$$

and similarly

$$\beta_1\beta_3+\beta_2\beta_4=v+p,\tag{3.28}$$

$$\beta_1\beta_4+\beta_2\beta_3=w+p.\tag{3.29}$$

Hence, the roots of the cubic resolvent are the three values of $\beta_i\beta_j+\beta_k\beta_l-p$ for different permutations $ijkl$ of 1234.

For the roots α_i of f we have, since $\alpha_i=\beta_i-b/4$ and $\beta_1+\beta_2+\beta_3+\beta_4=0$,

$$\alpha_1\alpha_2+\alpha_3\alpha_4=\beta_1\beta_2+\beta_3\beta_4+\frac{b^2}{8}=u+p+\frac{b^2}{8},\tag{3.30}$$

and similarly $\alpha_1\alpha_3+\alpha_2\alpha_4=v+p+b^2/8$, $\alpha_1\alpha_4+\alpha_2\alpha_3=w+p+b^2/8$.

Remark 3.5. Another method to solve the quartic equation $x^4+bx^3+cx^2+dx+e=0$, also due to Lagrange [17], is to form (cf. Remark 3.4)

$$s_1:=\alpha_1\alpha_2+\alpha_3\alpha_4,\qquad s_2:=\alpha_1\alpha_3+\alpha_2\alpha_4,\qquad s_3:=\alpha_1\alpha_4+\alpha_2\alpha_3,\tag{3.31}$$

and the cubic polynomial $\widetilde{R}(z)=(z-s_1)(z-s_2)(z-s_3)$ with these as roots. This polynomial can be expressed in the coefficients of the equation as, see [4, Section 12.1],

$$\widetilde{R}(z)=z^3-cz^2+(bd-4e)z-d^2-b^2e+4ce.\tag{3.32}$$

By Remark 3.4 and (3.21), $\widetilde{R}(z)=R(z-p-b^2/8)$, so this is our usual cubic resolvent in disguise.

Having found s_1,s_2,s_3 by solving the resolvent equation $\widetilde{R}(s)=0$, one notes, for $k=1,2,3$,

$$(2\gamma_k)^2-4s_k=b^2-4c,\tag{3.33}$$

and thus

$$\gamma_k=\pm\sqrt{s_k-c+b^2/4},\tag{3.34}$$

which, recalling (3.22), yields the roots by (3.23)–(3.26).

Appendix A. Real cubic equations

Assume that $f(x)=x^3+ax^2+bx+c$ is a polynomial of degree 3 with real coefficients.

Then f has always 3 complex roots (not necessarily distinct, and as always given by Theorem 2.5), but the number of real roots may be smaller. The following theorem shows that the number of real roots is 1 or 3, and that the discriminant discriminates between the possible cases.

Theorem A.1. *Let Δ be the discriminant of f given by* (2.10)*; thus Δ is real.*

(i) *If* $\Delta > 0$, *then* f *has three simple real roots.*
(ii) *If* $\Delta < 0$, *then* f *has one simple real root, and two non-real complex roots forming a pair of complex conjugates.*
(iii) *If* $\Delta = 0$, *then* f *has either one double and one simple real root, or a triple real root.*

Proof. Let, as in Section 2, the 3 roots of f in $\mathbb{C}$ be α_1, α_2, α_3. Note that $\alpha_1 + \alpha_2 + \alpha_3 = -b$. Δ is real by (2.10). By (2.9), $\Delta = 0$ if and only if two of the three roots coincide, i.e., f has a double or triple root. This root has to be real, since otherwise its conjugate would be another double or triple root and f would have at least 4 roots (counted with multiplicity), which is impossible. If there is a real double root $\alpha_1 = \alpha_2$, then $\alpha_3 = -b - \alpha_1 - \alpha_2$ is real too. This shows (iii).

Now suppose that $\Delta \neq 0$; thus f has three distinct simple roots in $\mathbb{C}$. Since $f(x) \to -\infty$ as $x \to -\infty$ and $f(x) \to \infty$ as $x \to \infty$, f has at least one real root by the intermediate value theorem. Further, since the roots are simple, f changes sign at each root, so f has an odd number of real roots. Hence f has either 1 or 3 real roots.

If f has 3 distinct real roots α_1, α_2, α_3, then (2.9) yields $\Delta > 0$.

If f has only one real root, then the roots are α_1, α_2, $\overline{\alpha_2}$ with $\alpha_1 \in \mathbb{R}$ and $\alpha_2 \notin \mathbb{R}$, and (2.9) yields

$$\Delta = (\alpha_1 - \alpha_2)^2(\alpha_1 - \overline{\alpha_2})^2(\alpha_2 - \overline{\alpha_2})^2 = |\alpha_1 - \alpha_2|^4(2\mathrm{i}\operatorname{Im}\alpha_2)^2 < 0. \qquad \square$$

Remark A.2. For a cubic y^3+py+q without second degree term, $\Delta/108 = -(p/3)^3 - (q/2)^2$ by (2.10), and thus the criterion for case (i) is $(p/3)^3 + (q/2)^2 < 0$; equivalently, $p < 0$ and $|p/3|^3 > |q/2|^2$. This was found already by Cardano, see Remark B.4.

The number of real roots is thus easily found. Now let us consider finding the root(s). There are by Theorem A.1 three cases, which we treat separately since they turn out to be quite different. (Of course, the roots are always given by Theorem 2.5, but we now want to perform only real arithmetic, if possible.)

A.1. $\Delta = 0$**, a double or triple root.** In the case $\Delta = 0$, the roots are easily found. The double (or triple) root $\alpha_1 = \alpha_2$ is also a root of the quadratic equation $f'(x) = 0$ (choosing the root that also satisfies $f(x) = 0$), and then α_3 is given by $\alpha_3 = -b - 2\alpha_1$. It is easily seen that $\alpha_1 = \alpha_2 = -b/3 + \delta$, and thus $\alpha_3 = -b/3 - 2\delta$, where $\delta = \pm\sqrt{-p/3}$ with the correct sign given by $\operatorname{sign}(\delta) = \operatorname{sign}(q)$. (See also Remarks 2.7 and A.5.)

A.2. $\Delta < 0$**, one simple real root.** If $\Delta < 0$, then Cardano's formula (2.36) yields the unique real root of f by choosing the real cube roots. Note that $-q/2 \pm \sqrt{-\Delta/108}$ is real and that the product of the real cube roots in (2.36) is $-p/3$ as required, because the product is a cube root of $(-p/3)^3$ and $-p/3$ is real.

A.3. $\Delta > 0$**, three simple real roots:** ***casus irreducibilis*****.** The case $\Delta > 0$ is much more complicated. Of course, Cardano's formula (2.36) still applies, but now $\sqrt{-\Delta/108}$ is imaginary and $-q/2 \pm \sqrt{-\Delta/108}$ complex, so the formula necessarily involves taking cube roots of complex (nonreal) numbers, even though we know that the final answer is a real root of f; the three different choices of cube roots of $-q/2 + \sqrt{-\Delta/108}$ lead to the three different real roots of $f(x) = 0$.

In this case the imaginary parts thus cancel in (2.36) for any admissible choice of cube roots. This can also be seen as follows: since $-q/2+\sqrt{-\Delta/108}$ and $-q/2-\sqrt{-\Delta/108}$ are complex conjugates, we may, and have to, choose cube roots of them that are complex conjugates in (2.36); recall that the product of these cube roots has to be $-p/3$, which is real. Hence, Cardano's formula (2.36) for the roots may be written

$$-\frac{b}{3}+\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{-\Delta}{108}}}+\overline{\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{-\Delta}{108}}}}=-\frac{b}{3}+2\operatorname{Re}\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{-\Delta}{108}}}. \tag{A.1}$$

Every complex number may be represented by a pair of real numbers, viz. its real and imaginary parts, but taking the cube root of a complex number may *not* be reduced to a combination of real cube roots (or real square and higher roots) and usual algebraic algebraic operations. In fact, it can be shown by Galois theory that if f is any polynomial with rational coefficients (i.e., $f(x) \in \mathbb{Q}[x]$) such that f is irreducible over $\mathbb{Q}$ and has positive discriminant, and α is a root of f, then α cannot be expressed by real radicals; in other words, there does not exist a sequence of field extensions $\mathbb{Q} = F_0 \subset F_1 \subset F_2 \cdots \subset F_N$ where $F_k = F_{k-1}[u_k]$ for some real u_k with $u_k^{n_k} \in F_{k-1}$ for some positive integer n_k, $k = 1, \dots, N$, and $\alpha \in F_N$; see [21, Section 8.8] or [4, Section 8.6]. (Here $\mathbb{Q}$ may be replaced by any subfield of $\mathbb{R}$.)

The case $\Delta > 0$ is known as the *casus irreducibilis*; in this case, thus the equation cannot (in general) be solved by radicals using only real numbers (somewhat paradoxically, since the answers all are real). This case is, by (2.10), characterized by $-4p^3 > 27q^2$, or equivalently

$$p < 0 \quad \text{and} \quad 4|p|^3 > 27q^2 \geq 0 \tag{A.2}$$

or

$$p < 0 \quad \text{and} \quad |p/3|^3 > (q/2)^2. \tag{A.3}$$

An alternative to Cardano's formula (A.1) in the case $\Delta > 0$ are the following trigonometric formulas, which involves only real numbers but use transcendental functions instead of algebraic expressions.

Theorem A.3. *If the real cubic polynomial* $f(x) = x^3 + bx^2 + cx + d$ *has positive discriminant* $\Delta > 0$*, or equivalently,* (A.3) *holds, then* f *has three* *real roots given by*

$$-\frac{b}{3}+2\sqrt{\frac{-p}{3}}\cos\left(\frac{1}{3}\arccos\left(\frac{-q/2}{(-p/3)^{3/2}}\right)\right) \tag{A.4}$$

where different branches of arccos *yield the three different roots.*

Equivalently, the roots are given by the three different values of

$$-\frac{b}{3}+2\sqrt{\frac{-p}{3}}\sin\left(\frac{1}{3}\arcsin\left(\frac{q/2}{(-p/3)^{3/2}}\right)\right). \tag{A.5}$$

Proof. Let $z := u^3 = -q/2+\sqrt{-\Delta/108} = -q/2+\mathrm{i}\sqrt{\Delta/108}$, see (2.32). Then, using (2.10),

$$|z|^2 = \frac{q^2}{4}+\frac{\Delta}{108} = -\frac{p^3}{27} = \left(\frac{-p}{3}\right)^3 = \left|\frac{p}{3}\right|^3.$$

We write z in polar coordinates: $z = re^{\mathrm{i}\varphi}$, where thus $r = |z| = (|p|/3)^{3/2}$ and

$$\cos\varphi = \frac{\operatorname{Re} z}{|z|} = \frac{-q/2}{r} = \frac{-q/2}{(-p/3)^{3/2}}.$$

By (A.1), a root of f is given by

$$-\frac{b}{3}+2\operatorname{Re} z^{1/3} = -\frac{b}{3}+2\operatorname{Re} r^{1/3}e^{\mathrm{i}\varphi/3} = -\frac{b}{3}+2r^{1/3}\cos(\varphi/3),$$

which yields (A.4), with different choices of φ yielding the three roots.

To see (A.5), let $\psi := \varphi+3\pi/2$ and note that $\sin\psi = -\cos\varphi$ and $\sin(\psi/3) = \cos(\varphi/3)$. □

In (A.4) and (A.5) we find the different roots by choosing different values of arccos or arcsin. Often it is more convenient to make a single choice (for example the principal value with $0\le\varphi\le\pi$ or $-\pi/2\le\psi\le\pi/2$, but any choice will do).

Theorem A.4. *Suppose that the real cubic polynomial $f(x) = x^3+bx^2+cx+d$ has positive discriminant $\Delta>0$, or equivalently, that* (A.3) *holds. Then, for any choice of*

$$\varphi := \arccos\left(\frac{-q/2}{(-p/3)^{3/2}}\right), \tag{A.6}$$

f has three real roots

$$-\frac{b}{3}+2\sqrt{\frac{-p}{3}}\cos\frac{\varphi}{3}, \qquad -\frac{b}{3}-\sqrt{\frac{-p}{3}}\left(\cos\frac{\varphi}{3}\pm\sqrt{3}\sin\frac{\varphi}{3}\right). \tag{A.7}$$

Similarly, for any choice of

$$\psi := \arcsin\left(\frac{q/2}{(-p/3)^{3/2}}\right), \tag{A.8}$$

f has three real roots

$$-\frac{b}{3}+2\sqrt{\frac{-p}{3}}\sin\frac{\psi}{3}, \qquad -\frac{b}{3}-\sqrt{\frac{-p}{3}}\Bigl(\sin\frac{\psi}{3}\pm\sqrt{3}\cos\frac{\psi}{3}\Bigr). \tag{A.9}$$

Proof. The other possible values of arccos in (A.6) are $\pm\varphi+2\pi n$, $n\in\mathbb{Z}$. Hence, the three values of the cos in (A.4) are $\cos(\varphi/3)$ and

$$\cos\frac{\varphi\pm 2\pi}{3}=\cos\frac{\varphi}{3}\cos\frac{2\pi}{3}\mp\sin\frac{\varphi}{3}\sin\frac{2\pi}{3}=-\frac{1}{2}\cos\frac{\varphi}{3}\mp\frac{\sqrt{3}}{2}\sin\frac{\varphi}{3},$$

and (A.4) yields (A.7).

Similarly, the other possible values of arcsin in (A.8) are $\psi+2\pi n$ and $3\pi-\psi+2\pi n$, $n\in\mathbb{Z}$, and the three values of the sin in (A.5) are $\sin(\psi/3)$ and

$$\sin\frac{\psi\pm 2\pi}{3}=\sin\frac{\psi}{3}\cos\frac{2\pi}{3}\pm\cos\frac{\psi}{3}\sin\frac{2\pi}{3}=-\frac{1}{2}\sin\frac{\psi}{3}\pm\frac{\sqrt{3}}{2}\cos\frac{\psi}{3}. \qquad \square$$

Remark A.5. The formulas (A.4)–(A.9) are meaningful (with real quantities only), exactly when $p<0$ and $|q/2|\le|p/3|^{3/2}$, i.e., when (A.3) holds or in the limiting case $\Delta=0$ and $p\neq 0$. The formulas (A.4)–(A.9) are valid in the latter case too, and then yield the roots $-b/3+\delta$, $-b/3+\delta$, $-b/3-2\delta$, where $\delta=\pm\sqrt{-p/3}$ with $\operatorname{sign}(\delta)=\operatorname{sign}(q)$, as found more easily in Subsection A.1.

Example A.6. Let $f(x)=x^3-x$, which evidently has the three real roots 0, ±1.

We have $b=0$, $p=c=-1$, $q=d=0$, and, by (2.10), $\Delta=4$ (which is verified by (2.9)). Hence, $u^3=-q/2+\sqrt{-\Delta/108}=\sqrt{-1/27}=3^{-3/2}\mathrm{i}$, and we find the three cube roots

$$\begin{aligned} u_1&=\frac{-\mathrm{i}}{\sqrt{3}},\\ u_2&=\frac{-\mathrm{i}}{\sqrt{3}}\Bigl(-\frac{1}{2}+\mathrm{i}\frac{\sqrt{3}}{2}\Bigr)=\frac{1}{2}+\frac{\mathrm{i}}{2\sqrt{3}},\\ u_3&=\frac{-\mathrm{i}}{\sqrt{3}}\Bigl(-\frac{1}{2}-\mathrm{i}\frac{\sqrt{3}}{2}\Bigr)=-\frac{1}{2}+\frac{\mathrm{i}}{2\sqrt{3}}. \end{aligned}$$

Hence (2.35) and (2.36) yield the three roots of f as

$$u_1+\overline{u_1}=0, \qquad u_2+\overline{u_2}=1, \qquad u_3+\overline{u_3}=-1.$$

Alternatively, we may use the trigonometric formula (A.4). We have $\arccos\bigl(-(q/2)/(-p/3)^{3/2}\bigr)=\arccos 0=\pi/2+n\pi$, $n\in\mathbb{Z}$, and thus the three roots are

$$\frac{2}{\sqrt{3}}\cos\frac{\pi}{6}=1, \qquad \frac{2}{\sqrt{3}}\cos\frac{5\pi}{6}=-1, \qquad \frac{2}{\sqrt{3}}\cos\frac{9\pi}{6}=0.$$

Similarly, (A.5) yields, since $\arcsin\bigl((q/2)/(-p/3)^{3/2}\bigr) = \arcsin 0 = n\pi$, $n \in \mathbb{Z}$, the three roots as

$$\frac{2}{\sqrt{3}}\sin 0 = 0, \qquad \frac{2}{\sqrt{3}}\sin\frac{2\pi}{3} = 1, \qquad \frac{2}{\sqrt{3}}\sin\frac{4\pi}{3} = -1.$$

Using (A.7) with $\varphi = \pi/2$ we find the same roots given as

$$\frac{2}{\sqrt{3}}\cos\frac{\pi}{6}, \qquad -\frac{1}{\sqrt{3}}\Bigl(\cos\frac{\pi}{6} \pm \sqrt{3}\sin\frac{\pi}{6}\Bigr)$$

while (A.9) with $\psi = 0$ yields

$$\frac{2}{\sqrt{3}}\sin 0 = 0, \qquad -\frac{1}{\sqrt{3}}\Bigl(\sin 0 \pm \sqrt{3}\cos 0\Bigr) = \mp 1.$$

Example A.7. Let $f(x) = x^3 - 7x - 6$, which has the roots 3, -1, -2. We have $p = -7$, $q = -6$ and $\Delta = 400$. Thus, $u^3 = -q/2 + \sqrt{-\Delta/108} = 3 + \sqrt{-100/27} = 3 + \frac{10}{3^{3/2}}\mathrm{i}$, and we find the three cube roots

$$u_1 = -1 + \frac{2}{\sqrt{3}}\mathrm{i}, \qquad u_2 = -\frac{1}{2} - \frac{5}{2\sqrt{3}}\mathrm{i}, \qquad u_3 = \frac{3}{2} + \frac{1}{2\sqrt{3}}\mathrm{i}.$$

Hence, (2.35) and (2.36) yield the three roots of f as

$$2\operatorname{Re} u_1 = -2, \qquad 2\operatorname{Re} u_2 = -1, \qquad 2\operatorname{Re} u_3 = 3.$$

The trigonometric solution (A.4) yields

$$2\sqrt{\frac{7}{3}}\cos\left(\frac{1}{3}\arccos\sqrt{\frac{243}{343}} + \frac{2\pi k}{3}\right), \qquad k = 0, 1, 2, \tag{A.10}$$

and it is far from obvious that this yields three integers 3, -2, -1.

Example A.8. Let $f(x) = x^3 - 7x^2 + 14x - 8$, which has the roots 1, 2, 4. Then, by (2.7)–(2.10), $p = -7/3$, $q = -20/27$ and $\Delta = 36$. Thus, $u^3 = -q/2 + \sqrt{-\Delta/108} = \frac{10}{27} + \frac{\mathrm{i}}{\sqrt{3}}$, and we find the three cube roots

$$u_1 = -\frac{2}{3} + \frac{1}{\sqrt{3}}\mathrm{i}, \qquad u_2 = -\frac{1}{6} - \frac{\sqrt{3}}{2}\mathrm{i}, \qquad u_3 = \frac{5}{6} + \frac{1}{2\sqrt{3}}\mathrm{i}.$$

Hence, (2.36) yields the three roots of f as

$$\frac{7}{3} + 2\operatorname{Re} u_1 = 1, \qquad \frac{7}{3} + 2\operatorname{Re} u_2 = 2, \qquad \frac{7}{3} + 2\operatorname{Re} u_3 = 4.$$

The trigonometric solution (A.4) yields

$$\frac{7}{3} + \frac{2\sqrt{7}}{3}\cos\left(\frac{1}{3}\arccos\frac{10}{7\sqrt{7}} + \frac{2\pi k}{3}\right), \qquad k = 0, 1, 2, \tag{A.11}$$

which, again surprisingly, yields three integers 4, 1, 2.

Example A.9. Cardano saw the problem with the *casus irreducibilis* and asked Tartaglia about it, giving $x^3 = 9x+10$ as an example, see Remark B.4. In this case, thus $f(x) = x^3 - 9x - 10$, so $p = -9$, $q = -10$ and $\Delta/108 = (-p/3)^3 - (q/2)^2 = 2$. Thus, $u^3 = -q/2 + \sqrt{-\Delta/108} = 5 + \sqrt{2}\mathrm{i}$, and we find the three cube roots

$$u_1 = -1 + \sqrt{2}\,\mathrm{i}, \quad u_2 = \frac{1+\sqrt{6}}{2} + \frac{\sqrt{3}-\sqrt{2}}{2}\mathrm{i}, \quad u_3 = \frac{1-\sqrt{6}}{2} - \frac{\sqrt{3}+\sqrt{2}}{2}\mathrm{i}.$$

Hence, (2.35) and (2.36) yield the three roots of f as

$$2\operatorname{Re} u_1 = -2, \qquad 2\operatorname{Re} u_2 = 1+\sqrt{6}, \qquad 2\operatorname{Re} u_3 = 1-\sqrt{6}.$$

Example A.10. Cardano [3, Chapter XIII] considered also the equation $y^3 = 8y + 3$. He saw that $y = 3$ is one solution (without discussing the problem of the *casus irreducibilis*, see Remark B.4). In modern terms he then found the other two solutions by finding the roots of the quadratic polynomial $(y^3 - 8y - 3)/(y - 3) = y^2 + 3y + 1$; he gave a general formula for this. (The other two solutions are $-(3 \pm \sqrt{5})/2$; these are negative, and Cardano changes the sign and interprets the result $(3 \pm \sqrt{5})/2$ as the two positive solutions of $x^3 + 3 = 8x$.)

Let us instead use Cardano's formula. In this case, $p = -8$, $q = -3$ and $\Delta = -4p^3 - 27q^2 = 1805$. Thus,

$$u^3 = -q/2 + \sqrt{-\Delta/108} = \frac{3}{2} + \frac{19\sqrt{5}}{6\sqrt{3}}\mathrm{i}, \tag{A.12}$$

and we find the three cube roots

$$u_1 = \frac{3}{2} + \frac{\sqrt{5}}{2\sqrt{3}}\mathrm{i}, \quad u_2 = \frac{\sqrt{5}-3}{4} - \frac{9+\sqrt{5}}{4\sqrt{3}}\mathrm{i}, \quad u_3 = -\frac{\sqrt{5}+3}{4} + \frac{9-\sqrt{5}}{4\sqrt{3}}\mathrm{i}.$$

Hence, (2.35) and (2.36) yield the three solutions of $y^3 = 8y + 3$ as

$$2\operatorname{Re} u_1 = 3, \qquad 2\operatorname{Re} u_2 = -(3-\sqrt{5})/2, \qquad 2\operatorname{Re} u_3 = -(3+\sqrt{5})/2.$$

Example A.11. Bombielli (1550) considered the equation $y^3 - 15y - 4 = 0$. Cardano's formula (2.35) yields the roots as

$$\sqrt[3]{2+\sqrt{-121}} + \sqrt[3]{2-\sqrt{-121}} = \sqrt[3]{2+11\mathrm{i}} + \sqrt[3]{2-11\mathrm{i}}. \tag{A.13}$$

Bombielli noted that 4 is a root, and showed in a pioneering calculation with complex numbers that $(2 \pm \mathrm{i})^3 = 2 \pm 11\mathrm{i}$, and thus (A.13) correctly yields the root $(2+\mathrm{i}) + (2-\mathrm{i}) = 4$.

The two other cube roots of $2 + 11\,\mathrm{i}$ are

$$u_2 = -1 - \frac{\sqrt{3}}{2} + \frac{2\sqrt{3}-1}{2}\mathrm{i}, \qquad u_3 = -1 + \frac{\sqrt{3}}{2} + \frac{-2\sqrt{3}-1}{2}\mathrm{i}.$$

Hence, the three solutions of $y^3 - 15y - 4 = 0$ are 4 and $-2 \pm \sqrt{3}$.

A.4. **Further comments for real coefficients.**

Remark A.12. In the *casus irreducibilis* we thus always obtain the roots as complicated expression involving complex cube roots, even when the roots are, for example, simple integers. (See Examples A.6–A.11 for simple cases.)

Also in the case of a single real root, Cardano's formula typically yields complicated expressions (but now involving real roots only) also for simple integer solutions.

Example A.13. The equation $x^3 + 6x = 20$ [3, Chapter XI] has the real root $x = 2$ (and the complex roots $-1 \pm 3\mathrm{i}$). Cardano's formula yields the root as

$$\sqrt[3]{10 + \sqrt{108}} + \sqrt[3]{10 - \sqrt{108}} = \sqrt[3]{10 + \sqrt{108}} - \sqrt[3]{\sqrt{108} - 10}. \tag{A.14}$$

This indeed equals 2 because $\sqrt{108} \pm 10 = (\sqrt{3} \pm 1)^3$, but this is far from obvious and it is hard to see how (A.14) can be simplified without knowing the answer.

Remark A.14. The trigonometric formulas (A.4)–(A.9) are valid also when $\Delta < 0$ (and, more generally, for arbitrary complex coefficients with $p \neq 0$), but then the angles φ and ψ are complex and the formulas less useful.

For real coefficients with $\Delta < 0$ (the case of a single real root), we can choose φ in (A.6) or ψ in (A.8) purely imaginary (after a change of sign of the roots and q in the case $p < 0 < q$), and the formulas (A.7) and (A.9) can be rewritten with real hyperbolic functions as follows [12].

Theorem A.15. *If the real cubic polynomial $f(x) = x^3 + bx^2 + cx + d$ has negative discriminant $\Delta < 0$, then f has one real and two conjugate complex roots given as follows.*

(i) *If $p < 0$ and $q/2 < -|p/3|^{3/2}$, then the roots are*

$$-\frac{b}{3} + 2\sqrt{\frac{-p}{3}} \cosh\left(\frac{1}{3} \operatorname{arccosh}\left(\frac{-q/2}{(-p/3)^{3/2}}\right)\right),$$
$$-\frac{b}{3} - \sqrt{\frac{-p}{3}} \left(\cosh\left(\frac{1}{3} \operatorname{arccosh}\left(\frac{-q/2}{(-p/3)^{3/2}}\right)\right) \pm \sqrt{3}\,\mathrm{i} \sinh\left(\frac{1}{3} \operatorname{arccosh}\left(\frac{-q/2}{(-p/3)^{3/2}}\right)\right)\right).$$

(ii) *If $p < 0$ and $q/2 > |p/3|^{3/2}$, then the roots are*

$$-\frac{b}{3} - 2\sqrt{\frac{-p}{3}} \cosh\left(\frac{1}{3} \operatorname{arccosh}\left(\frac{q/2}{(-p/3)^{3/2}}\right)\right),$$
$$-\frac{b}{3} + \sqrt{\frac{-p}{3}} \left(\cosh\left(\frac{1}{3} \operatorname{arccosh}\left(\frac{q/2}{(-p/3)^{3/2}}\right)\right) \pm \sqrt{3}\,\mathrm{i} \sinh\left(\frac{1}{3} \operatorname{arccosh}\left(\frac{q/2}{(-p/3)^{3/2}}\right)\right)\right).$$

(iii) *If $p > 0$, then the roots are*

$$-\frac{b}{3} - 2\sqrt{\frac{p}{3}} \sinh\left(\frac{1}{3} \operatorname{arcsinh}\left(\frac{q/2}{(p/3)^{3/2}}\right)\right),$$

$$-\frac{b}{3}+\sqrt{\frac{p}{3}}\left(\sinh\left(\frac{1}{3}\operatorname{arcsinh}\left(\frac{q/2}{(p/3)^{3/2}}\right)\right)\pm\sqrt{3}\,\mathrm{i}\cosh\left(\frac{1}{3}\operatorname{arcsinh}\left(\frac{q/2}{(p/3)^{3/2}}\right)\right)\right).$$

Remark A.16. The three cases in Theorem A.1 can also be seen geometrically by considering the graph of f (or g) as follows (based on [18]).

Denote the stationary points of g, i.e. the roots of $g'(y)=0$, by $\pm\delta$; thus the stationary points of f are $-\frac{b}{3}\pm\delta$. (Note also that f has an inflection point at $(-\frac{b}{3},q)$.) Since $g'(y)=3y^2+p$, we have

$$\delta=\sqrt{-p/3}. \tag{A.15}$$

In particular, δ is either real ($p\le 0$) or imaginary ($p>0$); when $p<0$, we choose for convenience the positive square root in (2.11). Let further

$$h:=-\bigl(g(\delta)-g(0)\bigr)=-\bigl(\delta^3+p\delta\bigr)=2\delta^3. \tag{A.16}$$

(We choose this sign so that $h>0$ when $\delta>0$.) Thus

$$f(-\tfrac{b}{3}\pm\delta)=g(\pm\delta)=g(0)\mp h=q\mp h. \tag{A.17}$$

If $\delta>0$, then f thus has a local maximum at $-\frac{b}{3}-\delta$ with value $q+h$, and a local minimum at $-\frac{b}{3}+\delta$ with value $q-h$. Considering the graph of f, we see that $f(x)=0$ then has three real roots if $0\in(q-h,q+h)$, two real roots (of which one double) if $0=q\pm h$, and one (simple) real root if $0\notin[q-h,q+h]$. We thus see the three different cases in Theorem A.1, with (i) if $h>|q|$, i.e. $h^2>q^2$, (ii) if $h<|q|$, i.e. $h^2<q^2$, and (iii) if $h=|q|$, i.e. $h^2=q^2$.

In the limiting case $\delta=0$ (which entails $h=0$), f has no local maximum or minimum, but a saddle point at $-\frac{b}{3}$ with $f(-\frac{b}{3})=g(0)=q$. In this case there is a triple root (case (iii)) if $q=0$ and otherwise one simple real root (case (ii)).

If δ is imaginary (and non-zero), then $f'(x)\neq 0$ for all real x, and thus $f'(x)>0$ (since this certainly holds for large x); hence f is strictly increasing and $f(x)=0$ has a single, simple root for any q (case (ii)). In this case, h is imaginary too, so $h^2<0\le q^2$.

We thus see that in all cases, Theorem A.1 holds with case (i) when $h^2-q^2>0$, (ii) when $h^2-q^2<0$, and (iii) when $h^2-q^2=0$. This is also confirmed by a simple calculation showing that

$$\Delta=-4p^3-27q^2=108\delta^6-27q^2=27(h^2-q^2). \tag{A.18}$$

Using parameters δ and h also simplify the formulas above a little. Since $h^2=4\delta^6=-4p^3/27$, (2.32) becomes

$$u^3=\tfrac12\bigl(-q+\sqrt{q^2-h^2}\bigr) \tag{A.19}$$

so Cardano's formula (2.36) for the roots of f becomes

$$-\frac{b}{3}+\sqrt[3]{\tfrac12\bigl(-q+\sqrt{q^2-h^2}\bigr)}+\sqrt[3]{\tfrac12\bigl(-q-\sqrt{q^2-h^2}\bigr)}. \tag{A.20}$$

Similarly, in the *casus irreducibilis*, which now is characterized by $h > |q|$, (A.4) and (A.5) can be written

$$-\frac{b}{3} + 2\delta \cos\left(\frac{1}{3}\arccos\Bigl(-\frac{q}{h}\Bigr)\right) = -\frac{b}{3} + 2\delta \sin\left(\frac{1}{3}\arcsin\Bigl(\frac{q}{h}\Bigr)\right). \tag{A.21}$$

Remark A.17. Consider the case of a real cubic $f(x) = ax^3 + bx^2 + cx + d$ with a single real root ($\Delta < 0$). A geometric way to find the two complex roots from the graph of f (on $\mathbb{R}$) has been given by e.g. [13; 11]: Let A be the intersection of the curve $y = f(x)$ and the x-axis (i.e., the real root), and let ℓ be a tangent from A to the curve. If the tangent point has x-coordinate x_0, and the slope of the tangent is k, then the complex roots are $x_0 \pm \sqrt{k}\,\mathrm{i}$.

Appendix B. History[1]

The solution to cubic equations was first found c. 1515 by Scipione del Ferro (1465–1526) in Bologna, at least for some cases. At this time, negative numbers were not used, nor was 0. Thus (in modern notation) $x^3 + px = q$, $x^3 = px + q$ and $x^3 + q = px$, with positive p and q, were regarded as different types of equations. (The third type was often ignored. We know today that it always has one negative solution, which generally was disregarded, and either zero positive solutions or two (*casus irreducibilis*); hence Cardano's formula will never yield a positive solution using real roots only. The negative solution was treated by Tartaglia and Cardano by, in modern terms, changing the sign of x, which transforms $x^3 + q = px$ to $x^3 = px + q$.) Scipione del Ferro could solve the first type and possibly the second (researchers disagree).

Remark B.1. There are 13 types of nontrivial cubic equations with positive coefficients: $x^3+cx = d$, $x^3 = cx+d$, $x^3+d = cx$, $x^3 = bx^2+d$, $x^3+bx^2 = d$, $x^3 + d = bx^2$, $x^3 + bx^2 + cx = d$, $x^3 + cx = bx^2 + d$, $x^3 + bx^2 = cx + d$, $x^3 = bx^2 + cx + d$, $x^3 + d = bx^2 + cx$, $x^3 + cx + d = bx^2$, $x^3 + bx^2 + d = cx$. These are, for example, discussed separately in Cardano's *Ars Magna* [3, Chapters XI–XXIII].

Similarly, Cardano [3, Chapter V] considers three different types of quadratic equations: $x^2 = bx + c$, $x^2 + bx = c$, $x^2 + c = bx$ (as did al-Khwarizmi c. 800, while Brahmagupta in 628 used both zero and negative numbers and treated all quadratic equations together), and many types of quartic equations, see Remark B.5 below.

Note that Cardano discusses negative numbers and negative *solutions* (called "false solutions") to equations [3, in particular Chapters I and XXXVII];

[1]This appendix is largely based on the Foreword (by Oystein Ore) and Preface (by T. Richard Witmer) to the English translation of *Ars Magna* [3], the text itself of *Ars Magna* [3], Katscher [15; 16], van der Waerden [22], and *The MacTutor History of Mathematics* [19] on the Internet (the articles Quadratic, cubic and quartic equations; Scipione del Ferro; Nicolo Tartaglia; Girolamo Cardano; Lodovico Ferrari; Tartaglia versus Cardan); much more details can be found in these references. For the history after Cardano's *Ars Magna* [3], see van der Waerden [22].

however, he does not consider negative *coefficients* (at least not usually, although there are occasional uses in a few examples, for example [3, Chapter XXXIX, Problem IX]).

Cardano even makes a pioneering tentative use of imaginary numbers and complex solutions [3, Chapter XXXVII, Rule II], although he clearly does not understand them and he seems sceptical to his calculation. Complex numbers were introduced in a consistent way somewhat later by Rafael Bombelli (1526–1572) in his book *Algebra* (1572), where he also shows how to work with negative numbers [19, Rafael Bombielli].

Remark B.2. It is claimed in [19, Scipione del Ferro] that the reduction (2.2) to an equation without quadratic term (which seems trivial to us) was known at the time of del Ferro, but this seems incorrect, and I rather believe the claim by [15] that del Ferro considered only such cubics because the others were too difficult to be solved. See further Remark B.3.

However, del Ferro kept his solution secret. The traditional story is that he did not tell anyone about it until his deathbed in 1526, when he told the solution to his student Antonio Maria Fior. (This seems a bit exaggerated, since his son-in-law Hannibal della Nave much later showed Cardano a notebook written by del Ferro presenting the solution, but he certainly told very few.)

Fior let it become known that he could solve cubic equations (without disclosing the method). This prompted Nicolo Tartaglia (1500–1557) in Venice to find solutions. He first found a solution to some equations of the type $x^3 + bx = d$. He claims [16, XIIII p. 12, XXV p. 15, p. 64] that he found the solution to all such equations in 1530, but he really could solve (and construct) only special cases, in modern terms having a negative integer solution. A public contest was held between Fior and Tartaglia in 1535, where each was to solve 30 problems set by the other (within 40 or 50 days); according to himself [16, XXV p. 13], Tartaglia managed to find the solutions to the two types $x^3 + px = q$ and $x^3 = px + q$ on 12 and 13 February 1535, only 8 days before the deadline of the contest[2], and then Tartaglia easily won by solving all 30 problems in 2 hours. (Fior's problems, which are given in [16, XXXI pp. 29–31], were all of the type $x^3 + px = q$, which he did not believe that Tartaglia could solve.)

Girolamo Cardano (1501–1576) in Milan then invited Tartaglia, and managed to make him disclose the method (25 March 1539), after Cardano had promised Tartaglia to keep it secret until Tartaglia had published the method himself (something Tartaglia never did, preferring to keep it secret and regretting that he had told Cardano). Cardano worked on the solution together with his young assistant Lodovico Ferrari (1522–1565), who in 1541 found a solution to quartic equations.

[2]According to [16, XXXI p. 29], the contest was on 22 February, which yields a discrepancy in the exact dates.

Cardano found out that the cubic equation had been solved by del Ferro before Tartaglia, and used this as an excuse to break his promise to Tartaglia and publish (in 1545) the solutions of cubic and quartic equations in his large algebra book *Ars Magna* [3], where they form a major part. (All 13 types of cubic equations are discussed separately in detail, but only some of the possible quartic equations, see below.) Cardano introduces the solution of the cubic equation with:

> Scipio Ferro of Bologna well-nigh thirty years ago discovered this rule and handed it on to Antonio Maria Fior of Venice, whose contest with Niccolò Tartaglia of Brescia gave Niccolò occasion to discover it. He [Tartaglia] gave it to me in reponse to my entreaties, though withholding the demonstration. Armed with this assistance, I sought out its demonstration in [various] forms. This was very difficult. My version of it follows. [3, Chapter XI]

The publication led to a bitter dispute between Tartaglia and Cardano–Ferrari. Tartaglia accused in a book [16, XXXIIII p. 42] (1546) Cardano of breaking an oath to him to keep the solution secret; he also added some insults against Cardano. This led to a series of equally insulting pamphlets (6 each) by Ferrari (defending Cardano, who kept a low profile in the dispute) and Tartaglia (renewing his accusations and insults), and finally to a public contest between Tartaglia and Ferrari in Milan on 10 August 1548. (Each posed 62 problems to the other. Ferrari won clearly; Tartaglia left Milan after the first day of the contest, when he saw that he was losing.)

Remark B.3. del Ferro, Fior and Tartaglia (with the exception $x^3+bx^2 = d$ discussed above) considered only cubics without second degree term, see Remark B.2, It seems that the reduction (2.2) of general cubic equations to this case is due to Cardano, who in [3] uses this reduction in 9 of the 10 types with a quadratic term (the exception is $x^3 + d = bx^2$, which is reduced by the substitution $x = d^{2/3}/y$). (Cardano claims in the beginning of [3] that those things to which he has not attached any name are his own discoveries. This is of course no proof that this reduction is his own invention, but it suggests that he regarded the reduction either as his own contribution or trivial.) Note that Cardano does the reduction separately for each type and that he does not discuss the reduction in his earlier chapters on some transformatons of equations. Moreover, he surprisingly does *not* use the corresponding reduction for fourth degree equations (see Remark B.5). Furthermore, Tartaglia did not know this reduction (until he read [3]); note that Tartaglia himself only mentions cubics without second degree term in the poem that he later claimed that he gave Cardano with the solution (see Remark C.1), and that when he claims to have solved $x^3 + bx^2 = d$ in 1530, he says that he had not been able to solve $x^3 + bx^2 + cx = d$ [16, XIIII p. 12] (and there is no indication that he found a solution later).

Remark B.4. Cardano quickly realized the problem with the *casus irreducibilis*, see Appendix A, and wrote to Tartaglia about it on 4 August 1539 [16, XXXVIII p. 48], giving the correct condition for it (see Remark A.2) and giving $x^3 = 9x + 10$ as an example (see Example A.9). Tartaglia was no longer cooperative, but it seems that neither Cardano nor Tartaglia understood how to handle this case.

Cardano ignores the complications of the *casus irreducibilis* in *Ars Magna* [3]. In [3, Chapter XIII] he solves $y^3 = 8y + 3$, and claims that he obtains $y = 3$ (which clearly is a solution) by his method, which seems to be at best an oversimplification. (Cf. Example A.10.)

Remark B.5. Cardano lists [3, Chapter XXXIX] 20 types of quartic equations that he can solve; these are the 10 nontrivial cases without cubic term (excluding the ones with only even powers of x, which are quadratic equations in x^2) and, symmetrically, the 10 nontrivial cases without linear term (which are reduced to the former by inversion).

Cardano states that these cases "are the most general as there are 67 others"; I do not understand which these 67 other cases are. Moreover, there are 15 cases with all possible terms (cubic, quadratic, linear and constant), and 7 additional without quadratic terms; these are not mentioned as far as I can see.

Cardano gives several examples where quartic equations are solved by Ferrari's method (see Appendix D); these examples illustrate 4 of the 10 types without cubic term and 2 of the 10 types without linear term, and it is clear that the method applies to all 20 types.

There is also a single example of an equation with both linear and cubic terms ($x^4 + 2x^3 = x + 1$, [3, Problem XXXIX.XIII]), but this is solved by special argument reducing this equation to a succession of two quadratic equations (the equation implies $(x(x+1))^2 = x(x+1)+1$ so $x(x+1)$ is the golden ratio $(\sqrt{5}+1)/2$).

Note that Cardano [3] does *not* use the general reduction (3.2) to eliminate the cubic term (in analogy with his treatment of cubic equations), which, together with Ferrari's method, would have given the solution of all types of quartic equations. I do not know whether this reduction, and thus the solution to general quartics, was found by Cardano, Ferrari or someone else.

Appendix C. del Ferro's solution of the cubic equation

Of course, del Ferro, Tartaglia and Cardano did not know Galois theory when they found the solution in Theorem 2.5. Their method is more direct, and consists in observing (by a stroke of genius) that if $y = u + v$, then

$$y^3 = (u+v)^3 = u^3 + v^3 + 3uv(u+v) = u^3 + v^3 + 3uvy; \tag{C.1}$$

hence, if we can find two numbers u and v such that

$$u^3 + v^3 = -q \tag{C.2}$$

$$3uv = -p, \tag{C.3}$$

then $y^3 = -py - q$, so y is a root of $g(y) = 0$. Note that (C.2)–(C.3) are the same as (2.27) and (2.34). To find u and v, we multiply (C.2) by u^3 and substitute (C.3), yielding

$$u^6 + qu^3 + (-p/3)^3 = 0. \tag{C.4}$$

This is a quadratic equation in u^3, which is readily solved and yields (2.32); then u is found by taking the cube root and v is found from (C.3). We see that this yields the same u and v as the argument in Section 2. (In particular, (2.33) holds, which shows that choosing the other root in (C.4) just means interchanging u and v, which does not change the root $u + v$; this should be no surprise, since u and v have identical roles in the *ansatz* $y = u + v$.) Consequently, this straightforward method yields the same solution $u + v$ as given in (2.24) and (2.35), and we obtain another proof of Theorem 2.5. (To see that the three different choices of u as a cube root of u^3 really yield the three different roots of $g(y) = 0$, with correct multiplicities if there is a double root, is perhaps less obvious by this method. We do not give a direct proof since we already know from Section 2 that this indeed is the case.)

Remark C.1. Actually, the method just described, with $y = u + v$, is Tartaglia's and Cardano's (and possibly del Ferros's) version for the equation $y^3 = cy + d$ (with $c, d > 0$) [3, Chapter XII] which corresponds to our $p < 0$, $q < 0$. For the equation $y^3 + cy = d$, which corresponds to our $p > 0$, $q < 0$, del Ferro, Tartaglia and Cardano instead set $y = u - v$ [3, Chapter XI], using

$$y^3 = (u - v)^3 = u^3 - v^3 - 3uv(u - v) = u^3 - v^3 - 3uvy, \tag{C.5}$$

and then find u and v such that $u^3 - v^3 = -q$ and $3uv = p$. This just means changing the sign of v in the equations above, which of course yields the same final result. (But it keeps u and v positive in both cases.)

The third case without second degree term, $y^3 + d = cy$ is reduced by Cardano to the case $y^3 = cy+d$ [3, Chapter XIII], essentially by substituting $-y$ for y, although Cardano expresses this differently.

According to Tartaglia [16, XXXIIII pp. 42–43], he gave these rules 25 March 1539 to Cardano in form of the following poem (English translation from [19, Tartaglia versus Cardan]):

When the cube and things together
Are equal to some discreet number,
Find two other numbers differing in this one.
Then you will keep this as a habit
That their product should always be equal
Exactly to the cube of a third of the things.
The remainder then as a general rule
Of their cube roots subtracted
Will be equal to your principal thing
In the second of these acts,

When the cube remains alone,
You will observe these other agreements:
You will at once divide the number into two parts
So that the one times the other produces clearly
The cube of the third of the things exactly.
Then of these two parts, as a habitual rule,
You will take the cube roots added together,
And this sum will be your thought.
The third of these calculations of ours
Is solved with the second if you take good care,
As in their nature they are almost matched.
These things I found, and not with sluggish steps,
In the year one thousand five hundred, four and thirty.[3]
With foundations strong and sturdy
In the city girdled by the sea.

The Italian original (which rhymes in the form *terza rima*) is [15]:

Quando chel cubo con le cose appresso
Se agguaglia qualche numero discreto
Trouan dui altri differenti in esso.

Dapoi terrai questo per consueto
Che'llor produtto sempre sia eguale
Alterzo cubo delle cose neto,

El residuo poi suo generale
Delli lor lati cubi ben sottratti
Varra la tua cosa principale.

In el secondo de cotestiatti
Quando che'l cubo restasse lui solo
Tu osseruarai quest'altri contratti,

Del numer farai due tal part'à uolo
Che l'una in l'altra si produca schietto
El terzo cubo delle cose in stolo

Delle qual poi, per communprecetto
Torrai li lati cubi insieme gionti
Et cotal somma sara il tuo concetto.

El terzo poi de questi nostri conti
Se solue col secondo se ben guardi
Che per natura son quasi congionti.

Questi trouai, & non con paßi tardi
Nel mille cinquecentè, quatroe trenta
Con fondamenti ben sald'è gagliardi

[3]Venice reckoned the year from 1 March, so February 1735 was still 1734 in Venice [15].

Nella citta dal mar'intorno centa.

Remark C.2. An equivalent, and somewhat quicker, way to obtain Cardano's formula is to use *Viète's substitution* $y = u - p/(3u)$ in $y^3 + py + q = 0$, which yields (C.4) directly. (This is obviously equivalent to setting $y = u + v$ with $3uv = -p$ as above. See [22, Chapter 3] for Viète's version of this.)

Appendix D. Ferrari's solution of the quartic equation

Consider again a fourth degree polynomial $g(y) = y^4 + py^2 + qy + r$ as in (3.3). The solution to the equation $g(y) = 0$ given in Theorem 3.2 is not the solution originally found by Ferrari and presented by Cardano in *Ars Magna* [3, Chapter XXXIX] (cf. Appendix B).

Ferrari's method is as follows (in a modern version). From $y^4 + py^2 + qy + r = 0$ we obtain, for any z,

$$(y^2 + z)^2 = y^4 + 2y^2 z + z^2 = (2z - p)y^2 - qy + z^2 - r. \tag{D.1}$$

We let $z := (p + u)/2$ and obtain, for any u,

$$\Bigl(y^2 + \frac{p+u}{2}\Bigr)^2 = uy^2 - qy + \frac{(p+u)^2}{4} - r. \tag{D.2}$$

The right-hand side is a quadratic polynomial in y, and its discriminant is

$$q^2 - 4u\left(\frac{(p+u)^2}{4} - r\right) = -u^3 - 2pu^2 - p^2 u + 4ru + q^2 = -R(u), \tag{D.3}$$

where R is the cubic resolvent (3.21). Hence, if we choose u as a non-zero root of R, then the right-hand side of (D.2) is the square of a linear polynomial. More precisely, if we further let $\gamma = \sqrt{u}$, then the right-hand side of (D.2) is

$$uy^2 - qy + \frac{q^2}{4u} = u\Bigl(y - \frac{q}{2u}\Bigr)^2 = \Bigl(\gamma y - \frac{q}{2\gamma}\Bigr)^2, \tag{D.4}$$

and thus (D.2) yields

$$\Bigl(y^2 + \frac{p+u}{2}\Bigr)^2 = \Bigl(\gamma y - \frac{q}{2\gamma}\Bigr)^2. \tag{D.5}$$

Consequently,

$$y^2 + \frac{p+u}{2} = \pm\Bigl(\gamma y - \frac{q}{2\gamma}\Bigr). \tag{D.6}$$

This yields a pair of quadratic equations in y, whose solutions are the four roots of $g(y) = 0$. (It thus suffices to choose one non-zero root of $R(u) = 0$ in order to find all roots of $g(y) = 0$. See Remark D.2 below for a justification.)

Remark D.1. Ferrari and Cardano considered, as said above, only equations with positive coefficients (putting some of them on the right-hand side), so they used different versions of the method for different signs of our p, q and r, but the versions are essentially the same.

Moreover, in the original version, first $y^4 + py^2$ is completed to a square (usually, at least), yielding

$$\Bigl(y^2 + \frac{p}{2}\Bigr)^2 = -qy + \frac{p^2}{4} - r; \tag{D.7}$$

then this is further modified by considering $(y^2 + p/2 + t)^2$ and choosing t so that the right-hand side becomes a square. This is obviously equivalent to the one-step completion of a square above, with $z = p/2 + t$. We further made the substitution $t = u/2$ in order to obtain the same form of the cubic resolvent as before.

See [10] for a detailed study of Cardano's solutions to quartics.

We can connect Ferrari's method and the methods in Section 3 as follows, using the notation in Section 3. The roots β_1, β_2 are $\frac{1}{2}\gamma_1 \pm \frac{1}{2}(\gamma_2 + \gamma_3)$, and are thus the roots of the quadratic equation, using (3.16)–(3.18) and (3.22) and assuming $\gamma_1 \neq 0$,

$$(2y - \gamma_1)^2 = (\gamma_2 + \gamma_3)^2 = v + w + 2\gamma_2\gamma_3 = -2p - u - 2q/\gamma_1. \tag{D.8}$$

This equation can be rewritten, since $\gamma_1 = \sqrt{u}$,

$$4y^2 - 4y\gamma_1 + 2u + 2p + 2q/\gamma_1 = 0, \tag{D.9}$$

$$4y^2 + 2u + 2p = 4\gamma_1 y - 2q/\gamma_1, \tag{D.10}$$

$$y^2 + \frac{u + p}{2} = \gamma_1 y - \frac{q}{2\gamma_1}. \tag{D.11}$$

The other two roots β_3, β_4 are obtained by replacing γ_1 by $-\gamma_1$, the other square root of u.

We have thus obtained the equations (D.6), with $\gamma = \gamma_1 := \sqrt{u}$.

Remark D.2. This derivation of (D.6) from Theorem 3.2 shows clearly that the two roots of each of the two quadratic equations in (D.6) together yield the four different roots of $g(y) = 0$. Typically, the four roots are distinct and we obtain all roots once each, but even when g has multiple roots and there are repetitions in the roots of (D.6), we obtain the roots of g with correct multiplicities from (D.6).

Remark D.3. We started above with a reduced quartic $y^4 + py^2 + qy + r$ (as did Cardano and Ferrari), but, as noted by Lagrange [17, no. 27] the method can also be applied directly to a general quartic $f(x) = x^4 + bx^3 + cx^2 + dx + e$ by expanding $(x^2 + \frac{b}{2}x + t)^2$ and using $f(x) = 0$ in analogy with (D.1); we then continue as above, obtaining a cubic resolvent equation for t, etc., see [17, no. 27] or [4, Section 12.1.C] for details. The resolvent equation for t becomes

$$t^3 - \frac{c}{2}t^2 + \frac{bd - 4e}{4}t + \frac{(4c - b^2)e - d^2}{8} = 0. \tag{D.12}$$

Comparing with (D.1), and recalling $y = x + b/2$, we have $t = z + b^2/16 = u/2 + p/2 + b^2/16$ and thus $u = 2t - p - b^2/8$, so the resulting cubic resovent equation (D.12) is $R(2t - p - b^2/8) = 0$, with R given by (3.21). Using

Remark 3.5, this can be written as $\widetilde{R}(2t) = 0$, as also follows from (D.12) and (3.32), so the roots of this resolvent equation are simply $s_i/2$, i.e., $\frac{1}{2}(\alpha_i\alpha_j + \alpha_k\alpha_l)$ for permutations $ijkl$ of 1234.

Remark D.4. Expressed in the roots β_i, we have by Remark 3.4

$$z = (u + p)/2 = (\beta_1\beta_2 + \beta_3\beta_4)/2. \tag{D.13}$$

This also follows by (D.11), which implies $\beta_1\beta_2 = (u + p)/2 + q/2\gamma_1$ and, replacing γ_1 by $-\gamma_1$, $\beta_3\beta_4 = (u + p)/2 - q/2\gamma_1$.

Remark D.5. Ferrari's method has the following geometric interpretation in algebraic geometry, see [6] and [1] for details.

Let $w := y^2$. Then (y, w) is a simultaneous solution of $w^2+pw+qy+r = 0$ and $w - y^2 = 0$, and thus also of the linear combination

$$w^2 + pw + qy + r + u(w - y^2) = 0$$

for any u. As u varies, this equation defines a family (called *pencil*) of quadratic curves (also known as *conics*) in the (y, w)-plane. A calculation essentially equivalent to the argument above shows that this conic is singular, and thus a union of two lines, exactly when $R(u) = 0$, and then the two lines are $w + (p + u)/2 = \pm(\gamma y - q/2\gamma)$ with $\gamma = \sqrt{u}$ (assuming $u \neq 0$), corresponding to (D.6). Ferrari's method thus can be seen as finding one singular conic in the pencil and decomposing it into a pair of lines; the solutions then are given by the intersections between these lines and the conic $w = y^2$.

Remark D.6. Descartes gave in 1637 yet another method to solve quartic equations (see e.g. [10]). Descartes' s method is based on trying to factor $g(y) = (y^2+ky+l)(y^2+my+n)$ by identifying the coefficients, which yields the equations

$$k + m = 0, \qquad km + l + n = p, \qquad kn + lm = q, \qquad ln = r. \tag{D.14}$$

This yields $m = -k$ and, after some algebra, $R(k^2) = 0$, where R is the cubic resolvent (3.21). Hence we can solve $R(u) = 0$, choose one root u, let $k := \gamma := \sqrt{u}$ and $m := -k$ (the other square root of u); solving for l and n then yields (for $u \neq 0$)

$$g(y) = \Bigl(y^2 + \gamma y + \frac{p+u}{2} - \frac{q}{2\gamma}\Bigr)\Bigl(y^2 - \gamma y + \frac{p+u}{2} + \frac{q}{2\gamma}\Bigr). \tag{D.15}$$

Consequently, we see again that $g(y) = 0$ is equivalent to (D.6).

References

[1] D. Auckly, Solving the quartic with a pencil. *Amer. Math. Monthly* **114** (2007), no. 1, 29–39.

[2] J. Bewersdorff, *Algebra für Einsteiger.* 2nd ed., Friedr. Vieweg & Sohn Verlag, Wiesbaden, 2004. English transl.: *Galois Theory for Beginners. A Historical Perspective*, AMS, Providence, R.I., 2006.

[3] G. Cardano, *Artis magnae, sive de regulis algebraicis. Lib. unus. Qui & totius operis de arithmetica, quod opus perfectum inscripsit, est in ordine decimus.* (*Ars Magna.*) Johann Petreius, Nuremberg, 1545. English transl.: *The Great Art, or The Rules of Algebra.* Translated and edited by T. R. Witmer, MIT Press, Cambridge, Mass., 1968.

[4] David A. Cox, *Galois Theory*, Wiley-Interscience, Hoboken, NJ, 2004.

[5] Leonhard Euler, De formis radicum aequationum cuiusque ordinis coniectatio, *Commentarii Academiae Scientiarum Petropolitanae* **6** (1738), 216–231. (Presented to the St. Petersburg Academy on November 2, 1733.) English transl.: A conjecture on the forms of the roots of equations, translated by J. Bell. `arXiv:0806.1927`.

[6] W. M. Faucette, A geometric interpretation of the solution of the general quartic polynomial. *Amer. Math. Monthly* **103** (1996), no. 1, 51–57.

[7] M. Frazier, *An Introduction to Wavelets through Linear Algebra.* Springer, New York, 1999.

[8] D. J. H. Garling, *Galois Theory.* Cambridge Univ. Press, Cambridge, 1986.

[9] P.A. Grillet, *Abstract Algebra.* 2nd ed., Springer, New York, 2007.

[10] H. Helfgott and M. Helfgott, A modern vision of the work of Cardano and Ferrari on quartics. *Loci* (June 2009), MathDL, The Mathematical Association of America. DOI: `10.4169/loci003312` .

[11] G. Henriquez, The graphical interpretation of the complex roots of cubic equations. *Amer. Math. Monthly* **42** (1935), no. 6, 383–384.

[12] G. C. Holmes, The use of hyperbolic cosines in solving cubic polynomials. *Math. Gazette* **86** (2002), no. 507, 473–477.

[13] F. Irwin and H. N. Wright, Some properties of polynomial curves. *Ann. Math.* **19** (1917), no. 2, 152–158.

[14] S. Janson, Resultant and discriminant of polynomials. Note N5, 2007. `http://www.math.uu.se/~svante/papers/#NOTES`

[15] F. Katscher, How Tartaglia solved the cubic equation. *Loci: Convergence* **3** (2006).
`http://mathdl.maa.org/mathDL/46/?pa=content&sa=viewDocument&nodeId=2433`
retrieved August 2, 2010.

[16] F. Katscher, *Die kubischen Gleichungen bei Nicolo Tartaglia. Die relevanten Textstellen aus seinen* „Quesiti et inventioni diverse“ *auf deutsch übersetzt und kommentiert.* Verlag der Österreichischen Akademie der Wissenschaften, Vienna, 2001.

[17] J. L. Lagrange, Réflexions sur la résolution algébrique des équations, *Nouveaux Mémoires de l'Académie royale des Sciences et Belles-Lettres de Berlin*, 1770–1771. Reprinted in *Œuvres de Lagrange, vol. 3*, pp. 205–421, J.-A. Serret ed., Gauthier-Villars, Paris, 1869

[18] R. W. D. Nickalls, A new approach to solving the cubic: Cardan's solution revealed. *Math. Gazette* **77** (1993), no. 480, 354–359.

[19] J. J. O'Connor & E. F. Robertson, *The MacTutor History of Mathematics archive.* University of St Andrews, Scotland.

http://www-history.mcs.st-andrews.ac.uk/

[20] J.-P. Serre, *Représentations linéaires des groupes finis.* 2nd ed., Hermann, Paris, 1967.

[21] B. L. van der Waerden, *Algebra I* (German). 7th ed., Springer-Verlag, Berlin, 1966. English transl: *Algebra, Vol. I*, Springer-Verlag, New York, 1991.

[22] B. L. van der Waerden, *A History of Algebra.* Springer-Verlag, Berlin, 1985.

Department of Mathematics, Uppsala University, PO Box 480, SE-751 06 Uppsala, Sweden

E-mail address: svante.janson@math.uu.se

URL: http://www.math.uu.se/∼svante/