POLYNOMIALS WITH GALOIS GROUP OF ORDER 3

JOHN MURRAY
NATIONAL UNIVERSITY OF IRELAND MAYNOOTH

1. Roots $\alpha, \alpha^2 - a, (\alpha^2 - a)^2 - a$

Let g be an irreducible monic polynomial over $\mathbb{Q}$ with Galois group G of order 3. Then g is a cubic with roots α_i', $i = 1, 2, 3$ mod 3. Moreover $\mathbb{Q}(\alpha_i') = \mathbb{Q}(\alpha_1', \alpha_2', \alpha_3')$ is a splitting field for g over $\mathbb{Q}$. Now there exist $\lambda, \mu, \nu \in \mathbb{Q}$ such that

$$\alpha_{i+1}' = \lambda(\alpha_i')^2 + \mu\alpha_i' + \nu, \quad \text{for } i = 1, 2, 3.$$

Consider the monic polynomial $f(x) := \lambda^3 g((x - \mu/2)/\lambda)$. It has roots $\alpha_i := \lambda\alpha_i' + \mu/2$, $i = 1, 2, 3$. Set $a := (\mu/2)^2 - \mu/2 - \lambda\nu$. Then

$$\alpha_i^2 - a = \lambda^2(\alpha_i')^2 + \lambda\mu\alpha_i' + (\mu/2)^2 - (\mu/2)^2 + \lambda\nu + \mu/2 = \lambda(\lambda(\alpha_i')^2 + \mu\alpha_i' + \nu) + \mu/2 = \alpha_{i+1}.$$

We classify all irreducible cubic polynomials f which have roots

$$\alpha, \alpha^2 - a, (\alpha^2 - a)^2 - a = \alpha^4 - 2a\alpha^2 + (a^2 - a).$$

Note that if $g(x) = x^3 + b_1x^2 + c_1x + d_1$, then

$$f(x) = x^3 + (\frac{-3\mu}{2} + \lambda b_1)x^2 + (\frac{3\mu^2}{4} - \lambda\mu b_1 + \lambda^2 c_1)x + (\frac{-\mu^3}{8} + \frac{\lambda\mu^2 b_1}{4} - \frac{\lambda^2\mu c_1}{2} + d_1\lambda^3).$$

Lemma 1. $f(x^2 - a) = -f(-x)f(x)$.

Proof. As $\alpha^2 - a$ is a root of f, α is a root of $f(x^2 - a)$. So $f \mid f(x^2 - a)$, by the irreducibility of f. Now $f(-x)$ is an irreducible cubic distinct from f, and $-\alpha$ is a root of $f(x^2 - a)$ and $f(-x)$. So $f(-x) \mid f(x^2 - a)$. As $\gcd(f(x), f(-x)) = 1$, we have $f(-x)f(x) \mid f(x^2 - a)$. The result now follows from the fact that $f(x^2 - a)$ is a monic sextic, as is $-f(-x)f(x)$. □

From now on

$$f(x) = x^3 + bx^2 + cx + d, \quad b, c, d \in \mathbb{Q}.$$

Lemma 2. $c = b^2 - 2a + 1, d = bc + 1 = b^3 + (1 - 2a)b + 1$.

Proof. We note that $-b$ is the sum of the roots of f. So

$$\alpha^4 + (1 - 2a)\alpha^2 + \alpha + (a^2 - 2a + b) = 0.$$

Thus $f \mid (x^4 + (1 - 2a)x^2 + x + (a^2 - 2a + b))$, whence

$$(x - b)(x^3 + bx^2 + cx + d) = x^4 + (1 - 2a)x^2 + x + (a^2 - 2a + b).$$

Date: 3rd January 2012.

Equating coefficients gives

$$-b^2 + c = 1 - 2a, \quad d - bc = 1.$$

The lemma follows from this. □

Lemma 3. *$b^2 = a + b - 2$ and hence*

$$f(x) = x^3 + bx^2 + (-b^2 + 2b - 3)x + (-b^3 + 2b^2 - 3b + 1).$$

Proof. We expand the equality $f(x^2 - a) = -f(-x)f(x)$, using $f = x^3 + bx^2 + cx + d$:

$$x^6 + (b-3a)x^4 + (3a^2 - 2ab + c)x^2 + (-a^3 + a^2b - ca + d) = x^6 + (2c - b^2)x^4 + (-2bd + c^2)x^2 - d^2.$$

Equating the coefficients of x^4, we get

$$2c = b^2 + b - 3a.$$

But $c = b^2 - 2a + 1$, by the previous lemma. So

$$2(b^2 - 2a + 1) = b^2 + b - 3a \quad \text{whence} \quad b^2 - b - a + 2 = 0.$$

This rearranges to $a = b^2 - b + 2$. So

$$c = b^2 - 2(b^2 - b + 2) + 1 = -b^2 + 2b - 3 \quad \text{and} \quad d = bc + 1 = -b^3 + 2b^2 - 3b + 1.$$

□

Calculation confirms that

$$((x^2 - a)^2 - a)^2 - a - x = x^8 - 4ax^6 + 2a(3a - 1)x^4 + 4a^2(1 - a)x^2 - x + (a^4 - 2a^3 + a^2 - a).$$

Lemma 4. *Let x, y be commuting indeterminates. Set $a := y^2 - y + 2$ and*

$$f(x, y) := x^3 + yx^2 + (-y^2 + 2y - 3)x + (-y^3 + 2y^2 - 3y + 1).$$

Then

$$\begin{aligned} ((x^2 - a)^2 - a)^2 - a - x &= (x^2 - a - x)f(x, y)f(x, 1 - y) \\ f(x^2 - a, y) &= -f(-x, y)f(x, y). \end{aligned}$$

Proof. This is straightforward, but tedious, calculation. □

Theorem 5. *$f(x) \in \mathbb{Q}[x]$ is a cubic polynomial whose roots are*

$$\alpha, \quad \alpha^2 - a, \quad (\alpha^2 - a)^2 - a,$$

for some rational a iff $a = b^2 - b + 2$, for some $b \in \mathbb{Q}$ and

$$f(x) = x^3 + bx^2 + (-b^2 + 2b - 3)x + (-b^3 + 2b^2 - 3b + 1).$$

Lemma 6. *$f(x - b/3) = x^3 + px + q$, where*

$$p = (-4/3)b^2 + 2b - 3, \quad q = (-16/27)b^3 + (4/3)b^2 - 2b + 1 = ((4/9)b - 1/3)p.$$

In particular the discriminant of f is the square rational number

$$\Delta(f) = -4p^3 - 27q^2 = (3p)^2 = (4b^2 - 6b + 9)^2.$$

Note: we have

$$p = -\frac{1}{3}\left(4b^2 - 6b + 9\right) = -\frac{1}{3}\left((2b - 3/2)^2 + 27/4\right)$$

So $p \leq -27/4$. Equality occurs when

$$p = -27/4,\ q = 0,\ a = 29/16,\ b = 3/4,\ c = -33/16,\ d = -35/64.$$

Then

$$f(x) = x^3 + (3/4)x^2 + (-33/16)x + (-35/64) = (x - 5/4)(x + 1/4)(x + 7/4)$$

has rational roots $5/4, -1/4, -7/4$. Notice that

$$(5/4)^2 - 29/16 = -1/4, \quad (-1/4)^2 - 29/16 = -7/4, \quad (-7/4)^2 - 29/16 = 5/4.$$

Also, the octic $((x^2 - a)^2 - a)^2 - a - x$ factors as

$$((x^2 - 29/16)^2 - 29/16)^2 - 29/16 - x = (x^2 - 29/16 - x)(x^3 + x^2/4 - 41x/16 + 23/64)\, f(x).$$

2. Irreducibility and uniqueness

Let ω be a primitive cubed root of unity and set $K := \mathbb{Q}(\omega)$. As $K = \mathbb{Q}(\sqrt{-3})$ and $-3 \equiv 1 \bmod 4$, it follows that the ring of integers of K is $\mathcal{O}_K = \mathbb{Z}(\omega)$. It is easy to show that $\mathcal{O}_K$ is a unique factorization ideal (indeed even a Euclidean domain). The norm map $N : \mathcal{O}_K \to \mathbb{Z}$ is given by $N(u + v\omega) = u^2 - uv + v^2$. The group of multiplicative units in $\mathcal{O}_K$ is cyclic of order 6, generated by $-\omega$:

$$U(\mathcal{O}_K) = \{1, -\omega, -1 - \omega, -1, \omega, 1 + \omega\}.$$

Some facts: let $s + t\omega \in K$. Then the associates of $s + t\omega$ are

$$\pm(s + t\omega), \quad \pm(t + (t - s)\omega), \quad \pm((t - s) - s\omega).$$

Also

$$(s + t\omega)^3 = (s^3 - 3st^2 + t^3) + 3st(s - t)\omega.$$

Now ω has minimal polynomial $x^2 + x + 1 = (x^3 - 1)/(x - 1)$ over $\mathbb{Z}$. If $p \in \mathbb{Z}$ is prime, then $\mathbb{F}_p$ has primitive cubed roots of unity $w_p, -1 - w_p$ iff $p \equiv 1 \bmod 3$. Using Kummer's theorem, we get in $\mathcal{O}_K$:

$$p \quad \begin{cases} = \pi_p\overline{\pi_p}, \text{where } \pi_p, \overline{\pi_p} \text{ are irreducible, if } p \equiv 1 \bmod 3. \\ \text{is irreducible, if } p \equiv 2 \bmod 3. \\ = -(1 + 2\omega)^2, \text{if } p = 3. \end{cases}$$

We make extensive use of 6.4.2 from [1]. Suppose that θ is an algebraic number such that $K : \mathbb{Q}$ is a Galois extension of degree 3, where $K = \mathbb{Q}(\theta)$. Let σ generate $\mathrm{Gal}(K : \mathbb{Q})$. Then $K(\omega) : \mathbb{Q}$ is a Galois extension whose Galois group is S_3. Set $\gamma := \theta + \omega^2\sigma(\theta) + \omega\sigma^2(\theta)$ and $\alpha := \gamma^2/\overline{\gamma}$. Define

$$e := N(\alpha) = \alpha\overline{\alpha}, \quad u := T(\alpha) = \alpha + \overline{\alpha}.$$

Then $\alpha \in \mathbb{Q}(\omega)$ and the minimal polynomial of θ over $\mathbb{Q}$ is

$$f(x) = x^3 + bx^2 + \frac{b^2 - e}{3}x + \frac{b^3 + 3be + eu}{27}.$$

Comparing this with Theorem 5, we get

$$\begin{array}{ll} e = b^2 - 3c = 4b^2 - 6b + 9 & = N(2b + 3\omega), \\ u = (16b^3 - 36b^2 + 54b - 27)/(4b^2 - 6b + 9) = 4b - 3 & = T(2b + 3\omega). \end{array}$$

The important parameter is the following element of K:

$$\beta := 2b + 3\omega = \frac{(4b-3) + 3\sqrt{-3}}{2} \quad \text{or} \quad (2b-3) - 3\omega = \frac{(4b-3) - 3\sqrt{-3}}{2}.$$

Example: Consider $f(x) := x^3 + bx^2 + (-b^2 + 2b - 3)x + (-b^3 + 2b^2 - 3b + 1)$, where $b \in \mathbb{Q}$. Then $f(x)$ has rational roots iff $2b + 3\omega = qz^3$, for some $q \in \mathbb{Q}$ and $z \in K$. Now up to a rational multiple, $z = s + t\omega$, where $s, t \in \mathbb{Z}$ are coprime, with $s, t \neq 0$, $s \neq t$. Then

$$z^3 = (s^3 - 3st^2 + t^3) + 3st(s-t)\omega = st(s-t)\left(2\frac{s^3 - 3st^2 + t^3}{2st(s-t)} + 3\omega\right).$$

It follows that

$$b = \frac{s^3 - 3st^2 + t^3}{2st(s-t)}.$$

Example: $s = 2, t = 1$. Then $b = 3/4$ and $a = 29/16$ and

$$f(x) = x^3 + (3/4)x^2 - (33/16)x - (35/64).$$

This has roots $5/4, -1/4, -7/4$, related by

$$-1/4 = (-5/4)^2 - 29/16, \quad -7/4 = (-1/4)^2 - 29/16, \quad 5/4 = (-7/4)^2 - 29/16.$$

According to Cohen, the cyclic cubic fields are parametrized by certain elements $\frac{u+3v\sqrt{-3}}{2}$ of $\mathcal{O}_K$ (i.e. $u, v \in \mathbb{Z}$), with $u \equiv v \bmod 2$, $v > 0$ and (Case (1)) $u \equiv 6 \bmod 9$, or (Case (2)) $u \equiv 2 \bmod 3$. Set $e = \frac{u^2+27v^2}{4}$. It is necessary and sufficient in Case (1) that $e/9$ is a product of t distinct primes, each $\equiv 1 \bmod 3$. There are 2^t solutions. In Case (2) the condition is that e is a product of $t > 0$ distinct primes, each $\equiv 1 \bmod 3$. There are 2^{t-1} solutions. Factorize $e/9$ or e as a product $e = \prod_{i=1}^{t} \pi_i \overline{\pi_i}$ of $2t$ prime elements of K.

In either case, write

$$\frac{u + 3v\sqrt{-3}}{2} = v(2b + 3\omega), \quad \text{where } b = (u + 3v)/4v.$$

Recall that $a = b^2 - b + 2$. So

$$a = \frac{7}{4} + \left(\frac{u+v}{4v}\right)^2.$$

Thus $K = \mathbb{Q}(\alpha)$, where α has minimal polynomial

$$f(x) = x^3 + \frac{u+3v}{4v}x^2 - \frac{(u-v)^2 + 32v^2}{16v^2} - \frac{u^3 + u^2v + 27uv^2 + 35v^3}{64v^3}.$$

The conjugates of α are

$$\alpha, \alpha^2 - a, -\alpha^2 - \alpha + (a - b).$$

Case (1) is that 3 is ramified in K. There are 2^t products $(-\omega)^n(\epsilon)3p_1\dots p_t = (u+3v\sqrt{-3})/2$ with $\epsilon = \pm 1$, $p_i \in \{\pi_i, \overline{\pi_i}\}$ and $0 \le n \le 5$ such that $u \equiv 6 \bmod 9$, $3 \nmid v$, $u \equiv v \bmod 2$ and $v > 0$. In particular

$$e = \frac{u^2 + 27v^2}{4}.$$

Then $K = \mathbb{Q}(\theta)$, where θ is an algebraic integer whose minimal polynomial over $\mathbb{Q}$ is

$$P(x) = x^3 - (e/3)x - (eu/27) \in \mathbb{Z}[x].$$

The parameters associated with this polynomial are

$$\lambda = -\frac{1}{v}, \quad \mu = -\frac{3v+u}{6v}, \quad \nu = \frac{2e}{9v}.$$

Now consider the minimal polynomial of $\alpha := \lambda\theta + \mu/2$. The coefficient of x^2 is minus the sum of the roots, which evaluates to

$$b = -\frac{3\mu}{2} = \frac{u+3v}{4v}.$$

So

$$\beta = \frac{u+3v}{2v} + 3\omega = \frac{u/v + 3\sqrt{-3}}{2}.$$

Hence $N(\beta) = (u^2 + 27v^2)/(4v^2)$.

Example: $e = 7$. So $t = 1$. Then the two solutions to $9 \times 7 = (u^2 + 27v^2)/4$ are:

$$u = -12, v = 2, \quad \text{and} \quad u = 15, v = 1.$$

Suppose $u = -12, v = 2$. Then $b = (-12+6)/8 = -3/4$ and $a = 53/16$ and

$$f(x) = x^3 - \frac{3}{4}x^2 - \frac{81}{16}x + \frac{307}{64}.$$

Suppose $u = 15, v = 1$. Then $b = 9/2$ and $a = 71/4$ and

$$f(x) = x^3 + \frac{9}{2}x^2 - \frac{57}{4}x - \frac{505}{8}.$$

Case (2) is that 3 is not ramified in K. There are 2^{t-1} products $(-\omega)^n p_1 \dots p_t = (u + 3v\sqrt{-3})/2$ with $p_i \in \{\pi_i, \overline{\pi_i}\}$ and $0 \le n \le 5$ such that $u \equiv 2 \bmod 3$, $3 \nmid v$, $u \equiv v \bmod 2$ and $v > 0$. In particular

$$e = \frac{u^2 + 27v^2}{4}.$$

Then $K = \mathbb{Q}(\theta)$, where θ is an algebraic integer whose minimal polynomial over $\mathbb{Q}$ is

$$P(x) = x^3 - x^2 + \frac{1-e}{3}x - \frac{1-3e+eu}{27} \in \mathbb{Z}[x].$$

The parameters associated with this polynomial are

$$\lambda = \frac{1}{v}, \quad \mu = -\frac{u+3v+4}{6v}, \quad \nu = \frac{9v+u+2-4e}{18v}.$$

Now $T(\theta) = 1$. Consider the minimal polynomial of $\alpha := \lambda\theta + \mu/2$. Then $T(\alpha) = \lambda + 3\mu/2$. So

$$b = \frac{1}{v} - \frac{u + 3v + 4}{4v} = \frac{u + 3v}{4v}.$$

So

$$\beta = \frac{u + 3v}{2v} + 3\omega = \frac{u/v + 3\sqrt{-3}}{2}.$$

Hence $N(\beta) = (u^2 + 27v^2)/(4v^2)$. Recall that $a = b^2 - b + 2$. So

$$a = \frac{7}{4} + \left(\frac{u + v}{4v}\right)^2.$$

Example: $e = 7$. Then the unique solution to $7 = (u^2 + 27v^2)/4$ is $u = -1, v = 1$. So $b = 1/2$ and $a = 7/4$ and

$$f(x) = x^3 + \frac{1}{2}x^2 - \frac{9}{4}x - \frac{1}{8}. \tag{1}$$

Now we find all polynomials parametrized by b that give isomorphic cyclic cubic extensions to that defined by (1). We have:

$$\frac{-1 + 3\sqrt{-3}}{2} = (1 + 3\omega).$$

The condition on b is $2b + 3\omega = qz^3(1 + 3\omega)$, or $(2b - 3) - 3\omega = qz^3(1 + 3\omega)$, for some $q \in \mathbb{Q}$ and $z \in K$. Now up to a rational multiple, $z = s + t\omega$, where $s, t \in \mathbb{Z}$ are coprime, with $s, t \neq 0$, $s \neq t$. Then

$$\begin{aligned} z^3(1 + 3\omega) &= (s^3 - 9s^2t + 6st^2 + t^3) + 3(s^3 - 2s^2t - st^2 + t^3)\omega \\ &= (s^3 - 2s^2t - st^2 + t^3)\left(2\tfrac{s^3 - 9s^2t + 6st^2 + t^3}{2(s^3 - 2s^2t - st^2 + t^3)} + 3\omega\right). \end{aligned}$$

It follows that

$$b, 3 - 2b = \frac{s^3 - 9s^2t + 6st^2 + t^3}{2(s^3 - 2s^2t - st^2 + t^3)}.$$

For example, if $s = 1, t = -11$ we get $b = 15/2$ and $a = 203/4$ and

$$f(x) = x^3 + (15/2)x^2 - (177/4)x - (2647/8),$$

while if $s = -1, t = 3$ we get $b = -1/58$, $a = 7687/3364$.

Example: $s = 2, t = 3$. Then $b = -5/2$ and $a = -43/4$ and the polynomial is:

$$f(x) = x^3 - (5/2)x^2 - (57/4)x + (293/8).$$

Or else $3 - 2b = -5/2$ and hence $b = 1/4$ and $a = 29/16$. In this case

$$f(x) = x^3 + (1/4)x^2 - (41/16)x + (23/64).$$

3. Symmetric Polynomials

Let F be a field and let (u, v, w) be elements of an extension field of F such that

$$b := -(u + v + w), \quad c := (uv + vw + wu), \quad d := -uvw$$

all belong to F. Then u, v, w are the roots of the cubic $f(x) := x^3 + bx^2 + cx + d \in F[x]$. Suppose also that

$$\delta = \delta(u, v, w) := (v - u)(w - v)(u - w)$$

belongs to F. Then f has discriminant $\Delta = \delta^2$ and Galois group or order 1 or 3 over F. Consequently, there exist unique $\lambda = \lambda(f), \mu = \mu(f), \nu = \nu(f)$ in F such that

$$v = \lambda u^2 + \mu u + \nu, \quad w = \lambda v^2 + \mu v + \nu, \quad u = \lambda w^2 + \mu w + \nu.$$

These can be got by solving the matrix equation

$$\begin{bmatrix} u^2 & u & 1 \\ v^2 & v & 1 \\ w^2 & w & 1 \end{bmatrix} \begin{bmatrix} \lambda \\ \mu \\ \nu \end{bmatrix} = \begin{bmatrix} v \\ w \\ u \end{bmatrix}.$$

We solve to get

$$\begin{bmatrix} \lambda \\ \mu \\ \nu \end{bmatrix} = \frac{1}{\delta} \begin{bmatrix} v - w & w - u & u - v \\ w^2 - v^2 & u^2 - w^2 & v^2 - u^2 \\ vw(v - w) & wu(w - u) & uv(v - u) \end{bmatrix} \begin{bmatrix} v \\ w \\ u \end{bmatrix}.$$

Thus

$$\begin{aligned} \lambda &= \frac{1}{\delta}((u^2 + v^2 + w^2) - (uv + vw + wu)), \\ \mu &= \frac{1}{\delta}((uv^2 + vw^2 + wu^2) - (u^3 + v^3 + w^3)), \\ \nu &= \frac{1}{\delta}((u^3v + v^3w + w^3u) - (u^2v^2 + v^2w^2 + w^2u^2)). \end{aligned}$$

Theorem 7. *Notation as above. Then*

$$\lambda = \frac{b^2 - 3c}{\delta}, \quad \mu = \frac{2b^3 - 7bc + 9d}{2\delta} - \frac{1}{2}, \quad \nu = \frac{b^2c - 4c^2 + 3bd}{2\delta} - \frac{b}{2}.$$

Proof. These are formal rational function identities. □

4. Trigonometric Identity

Lemma 8. *Let $0 < \theta < 2\pi$. Then*

$$\cos(\theta + 4\pi/3) = \frac{\sqrt{3}}{\sin(3\theta)} \cos^2 \theta - \left(\frac{\sqrt{3}}{2} \frac{\cos(3\theta)}{\sin(3\theta)} + \frac{1}{2} \right) \cos \theta - \frac{\sqrt{3}}{2 \sin(3\theta)}.$$

Proof. This is equivalent to

$$\Big(-\cos\theta+\sqrt{3}\sin\theta\Big)\sin(3\theta)=2\sqrt{3}\cos^2\theta-\sqrt{3}\cos(3\theta)\cos\theta-\cos\theta\sin(3\theta)-\sqrt{3}.$$

which can be simplified to

$$\cos(3\theta)\cos\theta-\sin(3\theta)\sin(-\theta)=2\cos^2\theta-1.$$

This holds because each side is equal to $\cos(2\theta)$. □

Now suppose that $f(x)=x^3+px+q\in\mathbb{Q}[x]$ is a cubic, with $\Delta(f)=-4p^3-27q^2>0$. In particular $p<0$. There are trigonomteric expressions for the 3 real roots of f:

$$\alpha_1=2\sqrt{-p/3}\cos\theta,\quad \alpha_2=2\sqrt{-p/3}\cos(\theta+4\pi/3),\quad \alpha_3=2\sqrt{-p/3}\cos(\theta+2\pi/3),$$

where $\cos(3\theta)=\frac{3\sqrt{3}q}{2p\sqrt{-p}}$. Without loss of generality $\sin(3\theta)>0$. So $\sin(3\theta)=\frac{-\sqrt{\Delta}}{2p\sqrt{-p}}$.

Theorem 9. *With the above notation, the roots of f have the form*

$$\alpha,\quad \frac{-3p}{\sqrt{\Delta}}\alpha^2+\left(\frac{9q}{2\sqrt{\Delta}}-\frac{1}{2}\right)\alpha-\frac{2p^2}{\sqrt{\Delta}},\qquad \frac{3p}{\sqrt{\Delta}}\alpha^2-\left(\frac{9q}{2\sqrt{\Delta}}+\frac{1}{2}\right)\alpha+\frac{2p^2}{\sqrt{\Delta}}.$$

Corollary 10. *In the special case (which involves scaling roots) that $f=x^3+px+q$ with $p=-(4b^2-6b+9)/3$ and $q=(4b-3)p/9$, and in particular $\sqrt{\Delta}=-3p$, the roots of f are:*

$$\alpha,\quad \alpha^2-\frac{2b}{3}\alpha-\frac{2}{9}(4b^2-6b+9),\quad -\alpha^2+(\frac{2b}{3}-1)\alpha+\frac{2}{9}(4b^2-6b+9)$$

Example: If $b=1$, then $f(x)=x^3-(7/3)x-(7/27)$ has discriminant 7^2 and roots

$$\alpha,\quad \alpha^2-(2/3)\alpha-(14/9),\quad -\alpha^2-(1/3)\alpha+(14/9).$$

Example: If $b=3$, then $f(x)=x^3-9x-9$ has discriminant $(27)^2$ and roots

$$\alpha,\quad \alpha^2-2\alpha-6,\quad -\alpha^2+\alpha+6.$$

Example: If $b=-3$ then $f(x)=x^3-21x+35$ has discriminant $(63)^2$ and roots

$$\alpha,\quad \alpha^2+2\alpha-14,\quad -\alpha^2-3\alpha+14.$$

5. All rational roots

By translating and scaling, we consider a triple $(0,1,r)$, where $r\in\mathbb{Q}$. Calculation gives

$$\lambda(0,1,r)=(-r^2+r-1)/(r^2-r),\quad \mu(0,1,r)=(r^3-r^2+1)/(r^2-r),\quad \nu=1.$$

The transformation $x\to\lambda x+\mu/2$ produces the triple:

$$\frac{(r^3-r^2+1)}{2r(r-1)},\quad \frac{(r^3-3r^2+2r-1)}{2r(r-1)},\quad \frac{(-r^3+r^2-2r+1)}{2r(r-1)}$$

Consider the rational function $T(x):=\frac{1}{1-x}$. Then $T^{(2)}(x)=\frac{x-1}{x}$ and $T^{(3)}(x)=x$. Set $A(r):=(r^3-r^2+1)/2r(r-1)$. Then the triple is

$$A(r),\quad A(T(r)),\quad A(T^{(2)}(r)).$$

Now $a := (\mu/2)^2 - (\mu/2) - \lambda\nu$ evaluates to

$$a \;=\; (r^6 - 4r^5 + 9r^4 - 8r^3 + 4r^2 - 2r + 1)/(2r(r-1))^2$$

and

$$b = \frac{-r^3 + 3r^2 - 1}{2r(r-1)}.$$

Example: $r = 2$. Then we obtain the triple $(5/4, -1/4, -7/4)$ and $a = 29/16$ and we have

$$\begin{array}{rcrcl} -1/4 & = & (5/4)^2 & - & 29/16, \\ -7/4 & = & (-1/4)^2 & - & 29/16, \\ 5/4 & = & (-7/4)^2 & - & 29/16. \end{array}$$

Example: Take $r = -2$. Then we obtain the triple $(-11/12, -25/12, 17/12)$ and $a = 421/144$. This satisfies the rule

$$\begin{array}{rcrcl} -25/12 & = & (-11/12)^2 & - & 421/144, \\ 17/12 & = & (-25/12)^2 & - & 421/144, \\ -11/12 & = & (17/12)^2 & - & 421/144. \end{array}$$

Theorem 11. *Given $b \in \mathbb{Q}$, then $f(x) := x^3 + bx^2 + (-b^2 + 2b - 3)x + (-b^3 + 2b^2 - 3b + 1)$ has rational roots iff*

$$b = \frac{1}{2}(\alpha + T(\alpha) + T^{(2)}(\alpha))), \quad \textit{for some } \alpha = 1/r \in \mathbb{Q},\ \alpha \neq 0, 1.$$

Equivalently iff $x^3 + (2b-3)x^2 - 2bx + 1$ has a rational root. Moreover, if b has this form, then the roots of $f(x)$ are

$$\frac{1}{2}(\alpha - T(\alpha) - T^{(2)}(\alpha))), \quad \frac{1}{2}(-\alpha + T(\alpha) - T^{(2)}(\alpha))), \quad \frac{1}{2}(-\alpha - T(\alpha) + T^{(2)}(\alpha))).$$

Theorem 12. *The polynomial $f(x) := x^3 + bx^2 + (-b^2 + 2b - 3)x + (-b^3 + 2b^2 - 3b + 1)$, for $b \in \mathbb{Q}$, has rational roots iff*

$$b = \frac{-s^3 + 3s^2t - t^3}{2st(s-t)}, \quad \textit{for some } s, t \in \mathbb{Z},\ gcd(s,t) = 1,\ t \neq 0, 1.$$

Equivalently iff $x^3 + (2b-3)x^2 - 2bx + 1$ has a rational root. Moreover, if b has this form, then the roots of $f(x)$ are

$$\frac{s^3 - s^2t + t^3}{2st(s-t)}, \quad \frac{s^3 - 3s^2t + 2st^2 - t^3}{2st(s-t)}, \quad \frac{-s^3 + s^2t - 2st^2 + t^3}{2st(s-t)},$$

and the discriminant Δ of f satisfies

$$\sqrt{\Delta} \;=\; \frac{(s^2 - st + t^2)^3}{(2st(s-t))^2}.$$

The following integers are pairwise coprime:

$$s^2 - st + t^2,\ s^3 - s^2t + t^3,\ 2st(s-t),\ s^3 - 3s^2t + 2st^2 - t^3,\ -s^3 + s^2t - 2st^2 + t^3 2st(s-t).$$

Theorem 13. *The polynomial* $f(x) := x^3 + bx^2 + (-b^2 + 2b - 3)x + (-b^3 + 2b^2 - 3b + 1)$, *for* $b \in \mathbb{Q}$, *has rational roots iff*

$$b = \frac{1}{2}(\frac{t}{s} + \frac{s}{s-t} + \frac{t-s}{t}), \quad \textit{for some } s,t \in \mathbb{Z},\ gcd(s,t) = 1,\ t \neq 0, 1.$$

Equivalently iff $x^3 + (2b-3)x^2 - 2bx + 1$ *has a rational root* s/t. *Moreover, if* b *has this form, then the roots of* $f(x)$ *are*

$$\frac{1}{2}(\frac{t}{s} - \frac{s}{s-t} - \frac{t-s}{t}), \quad \frac{1}{2}(-\frac{t}{s} + \frac{s}{s-t} - \frac{t-s}{t}), \quad \frac{1}{2}(-\frac{t}{s} - \frac{s}{s-t} + \frac{t-s}{t}),$$

and the discriminant Δ *of* f *satisfies*

$$\sqrt{\Delta} = \frac{(s^2 - st + t^2)^3}{(2st(s-t))^2}.$$

The following integers are pairwise coprime:

$$s^2 - st + t^2,\ s^3 - s^2t + t^3,\ 2st(s-t),\ s^3 - 3s^2t + 2st^2 - t^3,\ -s^3 + s^2t - 2st^2 + t^3 2st(s-t).$$

Lemma 14. *Let* x *be an indeterminate. Set*

$$u := x^3 - x^2 + 1, \quad v := x^3 - 3x^2 + 2x - 1, \quad w := -x^3 + x^2 - 2x + 1.$$

Then

$$u^3 + v^3 + w^3 = uv^2 + vw^2 + wu^2.$$

Moreover, the polynomials u, v, w *are coprime and*

$$\begin{aligned} \delta(u,v,w) &= 8(x^8 - 4x^7 + 9x^6 - 13x^5 + 13x^4 - 9x^3 + 4x^2 - x) \\ &= 8x(x-1)(x^2 - x + 1)^3. \end{aligned}$$

Also the symmetric functions in u, v, w *are:*

$$\begin{aligned} b &:= -(u+v+w) &&= -x^3 + 3x^2 - 1, \\ c &:= uv + vw + wu &&= -x^6 + 2x^5 - 5x^4 + 10x^3 - 10x^2 + 4x - 1, \\ d &:= -uvw &&= x^9 - 5x^8 + 11x^7 - 16x^6 + 14x^5 - 5x^4 - 5x^3 + 7x^2 - 4x + 1. \end{aligned}$$

Setting $\lambda := 2(x^2 - x)$ *we also have*

$$4b^2 - 6b\lambda + 9\lambda^2 = (x^2 - x + 1)^3, \quad (x^2 - x + 1)^3 - 9\lambda^2 = (x^3 - 3x + 1)^2.$$

Finally,

$$c = -b^2 + 2b\lambda - 3\lambda^2, \quad d = -b^3 + 2\lambda b^2 - 3\lambda^2 b + \lambda^3.$$

References

[1] H. Cohen, *A course in computational algebraic number theorey,* Graduate Texts in Math. **138** Springer, 1996.

Department of Mathematics, National University of Ireland, Maynooth, Co. Kildare, Ireland

E-mail address: John.Murray@maths.nuim.ie