POLYNOMIALS OF DEGREE 3 AND 4

Cardano formulas.

Let $f(x) = x^3 + ax + b \in \mathbb{Q}[x]$ be irreducible. The Galois group G is isomorphic to S_3 or A_3, therefore $f(x) = 0$ is solvable in radicals. Let $\alpha_1, \alpha_2, \alpha_3$ be the roots of $f(x)$, then

$$\alpha_1 + \alpha_2 + \alpha_3 = 0,\ \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 = a,\ \alpha_1\alpha_2\alpha_3 = -b.$$

Introduce

$$\omega = -\frac{1}{2} + \frac{\sqrt{3}i}{2},$$
$$D = -4a^3 - 27b^2 = (\alpha_1 - \alpha_2)^2 (\alpha_2 - \alpha_3)^2 (\alpha_3 - \alpha_1)^2,$$
$$F = \mathbb{Q}(\omega),\ K = \mathbb{Q}\left(\sqrt{D}, \omega\right),\ E = K(\alpha_1, \alpha_2, \alpha_3).$$

Then $\mathrm{Aut}_K(E) = A_3 = \mathbb{Z}_3$, $K \subset E$ is a Kummer extension. If s is an element in $\mathrm{Aut}_K E$ such that $s(\alpha_1) = \alpha_2$, $s(\alpha_2) = \alpha_3$, $s(\alpha_3) = \alpha_1$, then

$$\gamma_1 = \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3 \text{ and } \gamma_2 = \alpha_1 + \omega^2\alpha_2 + \omega\alpha_3$$

satisfy the relation

$$s(\gamma_1) = \omega\gamma_1,\ s(\gamma_2) = \omega^2\gamma_2.$$

Then γ_1^3, $\gamma_2^3 \in K$. One can write the expressions for γ_1 and γ_2

$$\gamma_1^3 = \alpha_1^3+\alpha_2^3+\alpha_3^3+6\alpha_1\alpha_2\alpha_3+3\omega\left(\alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1\right)+3\omega^2\left(\alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2\right),$$
$$\gamma_1^3 = \alpha_1^3+\alpha_2^3+\alpha_3^3+6\alpha_1\alpha_2\alpha_3+3\omega^2\left(\alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1\right)+3\omega\left(\alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2\right).$$

Note that $\alpha_1 + \alpha_2 + \alpha_3 = 0$, therefore

$$(\alpha_1 + \alpha_2 + \alpha_3)^3 = \alpha_1^3+\alpha_2^3+\alpha_3^3+6\alpha_1\alpha_2\alpha_3+3\left(\alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1\right)+3\left(\alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2\right) = 0.$$

Introduce notations

$$A = \alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1,\ B = \alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2.$$

Subtract the last equation from the expressions for γ_1 and γ_2 and get

$$\gamma_1^3 = 3(\omega - 1)A + 3\left(\omega^2 - 1\right)B = \frac{-9}{2}(A + B) + \frac{3\sqrt{3}i}{2}(A - B).$$

Now use the relations

$$A + B = \alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1 + \alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2 =$$
$$(\alpha_1 + \alpha_2 + \alpha_3)(\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1) - 3\alpha_1\alpha_2\alpha_3 = 3b,$$
$$B - A = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_{1.}) = \sqrt{D}.$$

Date: April 8, 2006.

Therefore

$$\gamma_1^3 = \frac{-9}{2}3b - \frac{3\sqrt{3}i}{2}\sqrt{D} = \frac{-27b}{2} - \frac{3}{2}\sqrt{-3D},$$
$$\gamma_2^3 = \frac{-27b}{2} + \frac{3}{2}\sqrt{-3D}.$$

To find γ_1 and γ_2 we have to take the cube root of $\frac{-27b}{2} \pm \frac{3}{2}\sqrt{-3D}$. We have 3 choices for a cube root. We have to choose them in such a way that

$\gamma_1\gamma_2 = \left(\alpha_1 + \omega\alpha_2 + \omega^2\alpha_3\right)\left(\alpha_1 + \omega^2\alpha_2 + \omega\alpha_3\right) = \alpha_1^2+\alpha_2^2+\alpha_3^2+\left(\omega + \omega^2\right)\left(\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1\right) =$

$\alpha_1^2+\alpha_2^2+\alpha_3^2-\left(\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1\right) = \left(\alpha_1 + \alpha_2 + \alpha_3\right)^2 - 3\left(\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1\right) = -3a.$

To find the roots $\alpha_1, \alpha_2, \alpha_3$ solve the linear system

$$\alpha_1 + \alpha_2 + \alpha_3 = 0,\ \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3 = \gamma_1,\ \alpha_1 + \omega^2\alpha_2 + \omega\alpha_3 = \gamma_2;$$

get the answer

$$\alpha_1 = \frac{\gamma_1 + \gamma_2}{3},\ \alpha_2 = \frac{\omega^2\gamma_1 + \omega\gamma_2}{3},\ \alpha_3 = \frac{\omega\gamma_1 + \omega^2\gamma_2}{3}.$$

Example. Consider the equation

$$x^3 - 3x + 1 = 0.$$

Then $D = 81$,

$$\gamma_{1,2} = (\frac{-27}{2} \pm \frac{3}{2}\sqrt{-243})^{1/3}.$$

Quartic polynomial.

Let $f(x) = x^4 + ax^2 + bx + c \in F[x]$ be an irreducible polynomial. The possible Galois groups for $f(x)$ are $\mathbb{Z}_4$, K_4 (Klein group), D_4, A_4 or S_4. We start by solving this polynomial equation in radicals. For this note that K_4 is a normal subgroup of S_4 and the quotient S_4/K_4 is isomorphic to S_3. Let $\alpha_1, \alpha_2, \alpha_3$ and α_4 be the roots of $f(x)$. Then

$$\theta_1 = \left(\alpha_1 + \alpha_2\right)\left(\alpha_3 + \alpha_4\right),\ \theta_2 = \left(\alpha_1 + \alpha_3\right)\left(\alpha_2 + \alpha_3\right),\ \theta_3 = \left(\alpha_1 + \alpha_4\right)\left(\alpha_2 + \alpha_3\right)$$

are fixed by K_4. Therefore $F(\theta_1, \theta_2, \theta_3) \subset E^{K_4}$, where E is the splitting field of $f(x)$. Note that

$$\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$$

implies

$$\theta_1 = -\left(\alpha_1 + \alpha_2\right)^2,\ \theta_2 = -\left(\alpha_1 + \alpha_3\right)^2,\ \theta_3 = -\left(\alpha_1 + \alpha_4\right)^2,$$

and we can easily obtain

$$\alpha_1 = \left(\sqrt{-\theta_1} + \sqrt{-\theta_2} + \sqrt{-\theta_3}\right)/2,$$
$$\alpha_2 = \left(\sqrt{-\theta_1} - \sqrt{-\theta_2} - \sqrt{-\theta_3}\right)/2,$$
$$\alpha_3 = \left(-\sqrt{-\theta_1} + \sqrt{-\theta_2} - \sqrt{-\theta_3}\right)/2,$$

$$\alpha_3 = \left(-\sqrt{-\theta_1} - \sqrt{-\theta_2} + \sqrt{-\theta_3}\right)/2.$$

We suspect that $\theta_1, \theta_2, \theta_3$ are the roots of a certain cubic polynomial with coefficients in F.

Lemma 0.1.

$$\theta_1 + \theta_2 + \theta_3 = 2a,\ \theta_1\theta_2 + \theta_2\theta_3 + \theta_3\theta_1 = a^2 - 4c,\ \theta_1\theta_2\theta_3 = -b^2.$$

Proof. First identity

$$\theta_1 + \theta_2 + \theta_3 = 2\sum_{i<j} \alpha_i\alpha_j = 2a.$$

For the second identity let

$$X = \theta_1\theta_2 + \theta_2\theta_3 + \theta_3\theta_1 = 6\alpha_1\alpha_2\alpha_3\alpha_4 + \sum_{i<j} \alpha_i^2\alpha_j^2 + 3\sum_{i\neq j\neq k, j<k} \alpha_i^2\alpha_j\alpha_k,$$

$$Y = a^2 - 4c = \left(\sum_{i<j} \alpha_i\alpha_j\right)^2 - 4\alpha_1\alpha_2\alpha_3\alpha_4 = 2\alpha_1\alpha_2\alpha_3\alpha_4 + \sum_{i<j} \alpha_i^2\alpha_j^2 + 2\sum_{i\neq j\neq k, j<k} \alpha_i^2\alpha_j\alpha_k,$$

$$X - Y = 4\alpha_1\alpha_2\alpha_3\alpha_4 + \sum_{i\neq j\neq k, j<k} \alpha_i^2\alpha_j\alpha_k = \left(\sum \alpha_i\right)\left(\sum_{i<j<k} \alpha_i\alpha_j\alpha_k\right) = 0.$$

For the last identity use

$$\theta_1\theta_2\theta_3 = -\left(\alpha_1 + \alpha_2\right)^2\left(\alpha_1 + \alpha_3\right)^2\left(\alpha_1 + \alpha_4\right)^2,$$

$$\left(\alpha_1 + \alpha_2\right)\left(\alpha_1 + \alpha_3\right)\left(\alpha_1 + \alpha_4\right) = \alpha_2\alpha_3\alpha_4 + \alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_3\alpha_4 + \alpha_1\alpha_2\alpha_4 + \alpha_1^2\left(\alpha_2 + \alpha_3 + \alpha_4\right) + \alpha_1^3 =$$

$$\alpha_2\alpha_3\alpha_4 + \alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_3\alpha_4 + \alpha_1\alpha_2\alpha_4 + \alpha_1^2\left(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4\right) =$$

$$\alpha_2\alpha_3\alpha_4 + \alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_3\alpha_4 + \alpha_1\alpha_2\alpha_4 = -b.$$

□

Corollary 0.2. *θ_1, θ_2 and θ_3 are the roots of polynomial*

$$h\left(x\right) = x^3 - 2ax^2 + \left(a^2 - 4c\right)x + b^2.$$

The polynomial $h\left(x\right)$ is called *the resolvent cubic* of $f\left(x\right)$.

To find the roots of $f\left(x\right)$ first find the roots θ_1, θ_2 and θ_3 of $h\left(x\right)$ and then use the formulas for $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ in terms of $\theta_1, \theta_2, \theta_3$.

Lemma 0.3. *The discriminant D of $f\left(x\right)$ is given by the formula*

$$D = 16a^4c - 4a^3b^2 - 128a^2c^2 + 144ab^2c - 27b^4 + 256c^3.$$

The proof is similar to one for a cubic polynomial but involves tedious calculations and we skip it.

How to determine the Galois group of a quartic polynomial.

First, check D. If D is a perfect square in F, the Galois group G is a subgroup of A_4.

Now, look at the cubic resolvent $h(x)$. If $h(x)$ is irreducible over F, then the splitting field of $f(x)$ contains a subfield of degree 3. Hence 3 divides $|G|$, and G is S_4 or A_4 depending on the discriminant test.

If $h(x)$ is reducible, then G is a subgroup of D_4. Consider two cases. If all three roots of $h(x)$ lie in F, then obviously the group is K_4. Assume that $h(x)$ splits into product of a quadratic and a linear polynomial in $F[x]$, say $\theta_1 \in F$, $\theta_2, \theta_3 \notin F$. Then the group is either D_4 or $\mathbb{Z}_4$. If $f(x)$ is irreducible over $F(\sqrt{D})$, then the group is D_4, otherwise it is $\mathbb{Z}_4$.

Example. For the polynomial $x^4 + 4x - 1$ the resolvent cubic is

$$x^3 + 4x + 16 = (x+2)\left(x^2 - 2x + 8\right).$$

Hence the Galois group over $\mathbb{Q}$ is a subgroup of D_4. We can avoid calculating the discriminant by checking that $f(x)$ has two complex and two real roots. Therefore the Galois group contains a transposition, hence it is D_4.