MATH 416, Modern Algebra II

Volodymyr Nekrashevych

2020, April 23

Solving equations of degree $n \le 4$

We all know how to solve quadratic equations: the roots of $x^2 + px + q$ are $\frac{-p \pm \sqrt{p^2 - 4q}}{2}$. One of the ways to deduce it is by looking at

$$(x - x_1)(x - x_2) = x^2 - (x_1 + x_2)x + x_1 x_2$$

and noting that $(x_1 - x_2)^2$ is a symmetric polynomial, so can be expressed as a function of $s_1 = x_1 + x_2$ and $s_2 = x_1 x_2$, namely

$$(x_1 - x_2)^2 = x_1^2 - 2x_1 x_2 + x_2^2 = (x_1 + x_2)^2 - 4x_1 x_2 = p^2 - 4q.$$

Then $x_1 - x_2 = \pm\sqrt{p^2 - 4q}$, and then $x_{1,2} = \frac{(x_1 + x_2) \pm (x_1 - x_2)}{2}$.

Cubic equations

Let us try to do something similar for cubic equations. First of all, we can simplify $x^3 + ax^2 + bx + c$ by substitution $x = y - \frac{a}{3}$: $(y - a/3)^3 + a(y - a/3)^2 + b(y - a/3) + c$ has coefficient at y^2 equal to $-3\frac{a}{3} + a = 0$, so we can consider polynomials of the form $x^3 + px + q$. If x_1, x_2, x_3 are its roots, then we have

$$\left\{ \begin{array}{rcl} x_1 + x_2 + x_3 & = & 0 \\ x_1x_2 + x_1x_3 + x_2x_3 & = & p \\ x_1x_2x_3 & = & -q \end{array} \right.$$

$$\begin{cases} x_1 + x_2 + x_3 & = & 0 \\ x_1x_2 + x_1x_3 + x_2x_3 & = & p \\ x_1x_2x_3 & = & -q \end{cases}$$

It follows that $0 = (x_1 + x_2 + x_3)^3 = x_1^3 + x_2^3 + x_3^3 + 3x_1x_2(x_1 + x_2) + 3x_1x_3(x_1 + x_3) + 3x_2x_3(x_2 + x_3) + 6x_1x_2x_3 = x_1^3 + x_2^3 + x_3^3 - 3x_1x_2x_3$, so that

$$x_1^3 + x_2^3 + x_3^3 = -3q.$$

We have
$(x_1x_2 + x_1x_3 + x_2x_3)^3 = x_1^3x_2^3 + x_1^3x_3^3 + x_2^3x_3^3 + 3\sum x_ix_j^2x_k^3 + 6x_1^2x_2^2x_3^2 = x_1^3x_2^3 + x_1^3x_3^3 + x_2^3x_3^3 - 3x_1x_2x_3(x_1x_2(x_1 + x_2) + x_1x_3(x_1 + x_3) + x_2x_3(x_2 + x_3)) + 6x_1^2x_2^2x_3^2 = x_1^3x_2^3 + x_1^3x_3^3 + x_2^3x_3^3 - 3x_1^2x_2^2x_3^2$, so

$$x_1^3x_2^3 + x_1^3x_3^3 + x_2^3x_3^3 = p^3 + 3q^2.$$

Cubic equations

$$x_1^3 + x_2^3 + x_3^3 = -3q, \quad x_1^3x_2^3 + x_1^3x_3^3 + x_2^3x_3^3 = p^3 + 3q^2.$$

Let us look again at the discriminant
$(x_1 - x_2)^2(x_2 - x_3)^2(x_1 - x_3)^2 = (x_3^2 - 4x_1x_2)(x_1^2 - 4x_2x_3)(x_2^2 - 4x_1x_3) =$
$-63x_1^2x_2^2x_3^2 - 4(x_2^3x_3^3 + x_1^3x_2^3 + x_1^3x_3^3) + 16x_1x_2x_3(x_1^3 + x_2^3 + x_3^3) =$
$-63q^2 - 4(p^3 + 3q^2) + 48q^2 = -27q^2 - 4p^3.$

Cubic equations

Therefore,

$$\sqrt{D} = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3) = \sqrt{-27q^2 - 4p^3}.$$

This expression is invariant under $A_3 \cong \mathbb{Z}_3$. Recall that $\mathbb{Q}(p, q) \subset \mathbb{Q}(x_1, x_2, x_3)$ has S_3 as the Galois group. A_3 corresponds to an intermediate field $\mathbb{Q}(p, q) \subset F \subset \mathbb{Q}(x_1, x_2, x_3)$. We have $[F : \mathbb{Q}(p, q)] = [S_3 : A_3] = 2$, therefore $F = \mathbb{Q}(p, q)(\sqrt{D})$. We also have $[\mathbb{Q}(x_1, x_2, x_3) : F] = |A_3| = 3$. If $u \in \mathbb{Q}(x_1, x_2, x_3)$ does not belong to F, then its irreducible polynomial over F has degree 3, so that $\mathbb{Q}(x_1, x_2, x_3) = F(u)$. We can simplify formulas by taking more than one element to generate $\mathbb{Q}(x_1, x_2, x_3)$

Cubic equations

Let $\zeta = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. Then $u = (x_1 + \zeta x_2 + \zeta^2 x_3)/3$ and $v = (x_1 + \zeta^2 x_2 + \zeta x_3)/3$ are multiplied by ζ and ζ^2 if we permute $x_1 \mapsto x_2 \mapsto x_3$. Consequently, u^3 and v^3 are invariant under A_3, hence they belong to $F = \mathbb{Q}(p, q)(\sqrt{D})$. But $u, v \notin F$. Note that the permutation $x_2 \leftrightarrow x_3$ interchanges u and v. The system

$$\begin{cases} x_1 + \zeta x_2 + \zeta^2 x_3 = 3u \\ x_1 + \zeta^2 x_2 + \zeta x_3 = 3v \\ x_1 + x_2 + x_3 = 0 \end{cases}$$

has unique solution:

$$x_1 = u + v, \qquad x_2 = \zeta^2 u + \zeta v, \qquad x_3 = \zeta u + \zeta^2 v$$

(use $1 + \zeta + \zeta^2 = 0$).

Cubic equations

In fact, a direct check shows that u^3 and v^3 satisfy the equation

$$y^2 + qy - \left(\frac{p}{3}\right)^3 = 0,$$

hence they are equal to $-\frac{q}{2} \pm \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}$, which gives the formulas

$$\begin{aligned}
x_1 &= \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}, \\
x_2 &= \zeta^2\sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \zeta\sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}, \\
x_3 &= \zeta\sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \zeta^2\sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}
\end{aligned}$$

Cubic equation: overview

The goal was to understand the splitting field $\mathbb{Q}(x_1, x_2, x_3)$ of the polynomial $x^3 + px + q$ over $\mathbb{Q}(p, q)$. The Galois group is the symmetric group S_3 permuting the roots x_1, x_2, x_3. We have a chain of subgroups $\{1\} < A_3 < S_3$. Therefore, we will have a chain of subfields $\mathbb{Q}(p, q) \subset F \subset \mathbb{Q}(x_1, x_2, x_3)$. Since the indices are $[S_3 : A_3] = 2$, $[A_3 : \{1\}] = 3$, the degrees are $[F : \mathbb{Q}(p, q)] = 2$ and $[\mathbb{Q}(x_1, x_2, x_3) : F] = 3$. We check that $u^3 = (x_1 + \zeta x_2 + \zeta^2 x_3)^3$ is fixed under A_3, but u is not. It follows that $u^3 \in F$ but u is not in F, so $\mathbb{Q}(x_1, x_2, x_3) = F(u)$. We also check that $D = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1)$ is fixed by A_3 and not by S_3, hence $D \in F$ but not in $\mathbb{Q}(p, q)$. We also see that D^2 is fixed by S_3, so $D^2 \in \mathbb{Q}(p, q)$. It follows that D is a square root of a function in p and q. $u^3 \in F$, so u^3 can be expressed using D and p, q. Consequently, u is a cube root of an expression involving p, q, D. Since $x_1, x_2, x_3 \in F(u)$, all roots can be expressed using p, q, D, u.

We see that the main idea was to find a tower of fields $\mathbb{Q}(p, q) \subset F \subset \mathbb{Q}(x_1, x_2, x_3)$ such that each extension $F_1 \subset F_2$ in the tower can be written as $F_2 = F_1(\alpha)$ for some α such that $\alpha^n \in F_1$ for some n, i.e., α is a root of $x^n - a$ for some $a \in F_1$. Such extensions are called *radical*. An equation can be solved in radicals if its splitting field can be constructed using a tower of consecutive radical extensions.

Degree 4 equations

A degree 4 equation can be also reduced to $x^4 + px^2 + qx + r = 0$ by a change of variable $x \mapsto y - a/4$. We can look at $x^4 + px^2 + qx + r$ as at a polynomial over $\mathbb{Q}(p, q, r)$. Let x_1, x_2, x_3, x_4 be its roots, so that the splitting field is $\mathbb{Q}(x_1, x_2, x_3, x_4)$. The Galois group of the polynomial is S_4. We have a composition series

$$\{1\} \leq \mathbb{Z}_2 \leq \mathbb{Z}_2 \oplus \mathbb{Z}_2 \leq A_4 \leq S_4$$

with factors $\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_2$. This will correspond to a tower of field extensions with degrees $2, 3, 2, 2$.

Degree 4 equations

The Klein's four-group $V \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ plays an important role here. Recall that it consists of the permutations
$(x_1, x_2)(x_3, x_4), (x_1, x_3)(x_2, x_4), (x_1, x_4)(x_3, x_2)$.
Let F be the corresponding fixed field. It is easy to see that the expressions $z_1 = \frac{1}{2}(x_1x_2 + x_3x_4)$, $z_2 = \frac{1}{2}(x_1x_3 + x_2x_4)$ and $z_3 = \frac{1}{2}(x_1x_4 + x_2x_3)$ are fixed by V, i.e., belong to F. The symmetric group S_4 permutes z_1, z_2, z_3, and elements of V are the only elements fixing each z_i. (BTW, this explicitly gives an epimorphism $S_4 \longrightarrow S_3$ with kernel V.)

Degree 4 equations

Since S_4 permutes z_1, z_2, z_3, the elements $z_1 + z_2 + z_3, z_1z_2 + z_1z_3 + z_2z_3, z_1z_2z_3$ are fixed by S_4, hence belong to $\mathbb{Q}(p, q, r)$. It follows that z_1, z_2, z_3 are roots of a cubic polynomial with coefficients in $\mathbb{Q}(p, q, r)$. In fact, they are roots of the *cubic resolvent*

$$z^3 - \frac{p}{2}z^2 - rz + \left(\frac{pr}{2} - \frac{q^2}{8}\right) = 0.$$

Degree 4 equations

We know how to solve it, so we will get expressions for z_1, z_2, z_3. We have $2z_1 = x_1x_2 + x_3x_4$ and $r = x_1x_2 \cdot x_3x_4$. It follows that x_1x_2 and x_3x_4 are roots of the polynomial $x^2 - 2z_1x + r$. We also have, $2(z_2 + z_3) = x_1x_3 + x_2x_4 + x_1x_4 + x_2x_3 = (x_1 + x_2)(x_3 + x_4)$ and $(x_1 + x_2) + (x_3 + x_4) = 0$. Consequently, $(x_1 + x_2)$ and $(x_3 + x_4)$ are roots of $x^2 + 2(z_2 + z_3)$. Solving these quadratic equations, we will find $x_1x_2, x_1 + x_2, x_3x_4, x_3 + x_4$. Then, solving the quadratic equations $x^2 - (x_1 + x_2)x + x_1x_2 = 0$ and $x^2 - (x_3 + x_4)x + x_3x_4 = 0$ we will find x_1, x_2, x_3, x_4.

General discussion

An extension $F \subset E$ is an *extension of F by radicals* if there is a sequences of extensions

$$F = F_0 \subset F_1 \subset F_2 \subset \ldots \subset F_m = E$$

such that for each $F_i \subset F_{i+1}$ there exist α_i and n_i such that $F_{i+1} = F_i(\alpha_i)$ and $\alpha_i^{n_i} \in F_i$.
We say that a polynomial $f(x) \in F[x]$ is *solvable by radicals* if its splitting field is contained in a radical extension of F. Solving a *general equation of degree n in radicals* corresponds to solvability of a general polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Q}(a_1, a_2, \ldots, a_{n-1})[x]$ in radicals. We have seen that general polynomials are solvable in radicals for $n = 1, 2, 3, 4$.

Some particular (non-general) equations of higher degree may be solvable in radicals. For example, $x^n - 1$ or $x^n - a$ are solvable for every n and a. Recall that a group G is called *solvable* if there exists a series

$$\{1\} = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_n = G$$

such that all factor groups G_{i+1}/G_i are abelian.

Theorem 1

A polynomial $f(x) \in F[x]$ is solvable in radicals (if and) only if its Galois group is solvable.

As a corollary, we get

Theorem 2

The general polynomial equation of degree n is solvable in radicals if and only if $n \geq 4$.

Namely, for $n \geq 5$ the subgroup $A_n < S_n$ is simple. (It is easier to show that the subgroup of A_n generated by the commutators $g^{-1}h^{-1}gh$ is the whole group A_n, so that any homomorphism to an abelian group from A_n has A_n as the kernel, so there are not subgroups $H \lhd A_n$ such that A_n/H is abelian.)