SOLVING POLYNOMIALS BY RADICALS

DEFINITION: Let F be a field, and $f \in F[x]$. We say that f is **solvable by radicals** if every root of f can be obtained from elements of F by $+$, $-$, $\times$, $\div$, and taking nth roots (for any $n > 1$).

(1) Let F be a field of characteristic $\neq 2$. Show that[1] any quadratic polynomial

$$f(x) = ax^2 + bx + c \in F[x]$$

with $a \neq 0$ is solvable by radicals.

We can rewrite as $x^2 + \frac{b}{a}x + \frac{c}{a} = 0$. Then this is the same as $(x + \frac{b}{2a})^2 + \frac{c}{a} - \frac{b^2}{4a^2} = 0$. Then $x + \frac{b}{2a} = \pm\frac{\sqrt{b^2-4ac}}{2a}$ and $x = \frac{-b}{2a} \pm \frac{\sqrt{b^2-4ac}}{2a}$.

(2) Solving the cubic: Let $f(x) = x^3 - 3x^2 + 12x - 7 \in \mathbb{Q}[x]$.

(a) Find a $c \in \mathbb{Q}$ such that, setting $x = y + c$, we have $f(y) = y^3 + py + q$ with no y^2 term.

(b) Make the *Vieta substitution* $y = z - \frac{p}{3z}$, and rewrite the result as a quadratic in z^3.

(c) Without forgetting that any nonzero complex number has three cube roots, solve for z, and use this to solve for x.

(d) Discuss: what would you do with a general cubic? Explain why any cubic is solvable by radicals (over $\mathbb{Q}$).

(a) Take $c = 1$ to get $f(x) = (y+1)^3 - 3(y+1)^2 + 12(y+1) - 7 = y^3 + 9y + 3$.

(b) We have $f = (z - \frac{3}{z})^3 + 9(z - \frac{3}{z}) + 3(z - \frac{3}{z}) = z^3 + 3 - \frac{27}{z^3}$. Clearing denominators gives $(z^3)^2 + 3(z^3) - 27 = 0$.

(c) We have $z^3 = \frac{-3\pm\sqrt{9+108}}{2} = \frac{3}{2}(1 \pm \sqrt{13})$. Then the solutions are

$$z = \sqrt[3]{\frac{3}{2}(\sqrt{13}-1)},\ \omega\sqrt[3]{\frac{3}{2}(\sqrt{13}-1)},\ \omega^2\sqrt[3]{\frac{3}{2}(\sqrt{13}-1)},$$
$$\zeta\sqrt[3]{\frac{3}{2}(\sqrt{13}+1)},\ -\sqrt[3]{\frac{3}{2}(\sqrt{13}+1)},\ \zeta^5\sqrt[3]{\frac{3}{2}(\sqrt{13}+1)}$$

where $\omega = e^{2\pi i/3}$, $\zeta = e^{2\pi i/6}$ are primitive cube and sixth roots of 1. We can write $x = 1 + z - 9/z$ for each of these six values of z to get the three roots x (each appearing twice).

(d) It is the same process for any cubic, so this gives a formula in terms of radicals for the roots.

DEFINITION: Let G be a finite group. We say that G is **solvable** if there exist subgroups H_i such that

$$\{e\} = H_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \cdots \trianglelefteq H_n = G$$

where each consecutive quotient H_{i+1}/H_i is abelian.

[1] Hint: Complete the square!

THEOREM: Let F be a field of characteristic zero, and $f \in F[x]$ be a separable polynomial. If f is solvable by radicals, then the Galois group[2][3] of f is a solvable group.

LEMMA: Let G be a finite group.

(1) If $N \trianglelefteq G$, then G is solvable if and only if N and G/N are both solvable.
(2) If $\{e\} = H_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \cdots \trianglelefteq H_n = G$ and each consecutive quotient H_{i+1}/H_i is *solvable*, then G is solvable.

(3) Not solving the quintic: Let $f(x) = x^5 - 4x - 2 \in \mathbb{Q}[x]$.

(a) Show that f is irreducible and has five distinct complex roots, of which three are real[4].
(b) Show that[5] the Galois group of f is isomorphic to $\mathcal{S}_5$.
(c) Use the Theorem to show that f cannot be solved by radicals.

PROPOSITION: Let F be a field of characteristic zero.

(1) For any $m \geq 1$, the Galois group of $x^m - 1$ is abelian.
(2) If F contains all mth roots of 1 and $a \in F$, then the Galois group of $x^m - a$ is cyclic.

(4) Proof of Proposition $\Longrightarrow$ Theorem: Let F be a field of characteristic zero. Say that a sequence of fields

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n$$

is a **radical tower** if for all $i = 0, \ldots, n-1$, F_{i+1} is the splitting field of $x^{m_i} - a_i \in F_i[x]$ for some $m_i \geq 2$ and $a_i \in F_i$.

(a) Suppose that β can be obtained from elements of F by $+$, $-$, $\times$, $\div$, and taking nth roots. Explain why there exists a radical tower $F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n$ such that $\beta \in F_n$.
(b) Suppose that $\beta_1, \ldots, \beta_s$ can be obtained from elements of F by $+$, $-$, $\times$, $\div$, and taking nth roots. Explain why there exists a radical tower $F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n$ such that $\beta_1, \ldots, \beta_s \in F_n$.
FACT: In the setting of the previous part, one can also arrange that F_n/F *is Galois*.
(c) Suppose that K/F is the splitting field of $x^m - a$ for some $m \geq 2$ and $a \in F$. Show that $\mathrm{Gal}(K/F)$ is solvable.
(d) Let $F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n$ be a radical tower with F_n/F Galois. Show that $\mathrm{Gal}(F_n/F)$ is solvable.
(e) Complete the proof of the Theorem.

(5) Proof of Proposition (1):

(a) Let F be a field of characteristic zero, $m \geq 1$, and K be a splitting field of $x^m - 1$. Show that[6] the set $\mu_m \subseteq K$ of solutions of $x^m - 1$ in K is a cyclic subgroup of $K^\times$.
(b) Let ζ be a generator of μ_m. Show that $K = F(\zeta)$.

---

[2]Recall that we have defined the Galois group of a separable polynomial to be the Galois group of its splitting field.
[3]The converse is also true, but we won't prove it. Moreover, a version of the theorem is true in arbitrary characteristic.
[4]Hint: Calculus.
[5]Hint: Use Cauchy's Theorem and complex conjugation.
[6]Hint: Use a homework problem.

(c) Show that the map

$$\begin{array}{ccc} \mathrm{Gal}(K/F) & \longrightarrow & (\mathbb{Z}/m)^\times \\ \sigma & \mapsto & [i]_m \quad \text{s.t. } \sigma(\zeta) = \zeta^i \end{array}$$

is an injective group homomorphism and deduce part (1) of the Proposition.

(6) Proof of Proposition (2):

(a) Let F be a field of characteristic zero containing m distinct mth roots of 1, let $a \in F$, and let K be a splitting field for $x^m - a$. Let α be any root of $x^m - a$. Show that $K = F(\alpha)$.

(b) Let ζ be a generator for μ_m as in the previous problem. Show that the map

$$\begin{array}{ccc} \mathrm{Gal}(K/F) & \longrightarrow & \mathbb{Z}/m \\ \sigma & \mapsto & [i]_m \quad \text{s.t. } \sigma(\alpha) = \zeta^i \alpha \end{array}$$

is an injective group homomorphism and deduce part (2) of the Proposition.