# Solving polynomial equations by radicals

**Question:** Can every algebraic number be expressed using algebraic operations $(+, -, *, \div)$ and radicals $\sqrt[n]{\ }$, starting from rational numbers?
**Answer:** Yes for algebraic numbers of degree $\leq 4$ (See §8.1 of Howie).
No in general for algebraic numbers of degree $\geq 5$.

---

**Definition.** Let $K$ be a field. An extension $L \supseteq K$ is called a **radical extension** if there exists a chain of subfields

$$K = L_0 \subset L_1 \subset \cdots \subset L_m = L$$

such that for each $j = 0, 1, \ldots, m-1$, $L_{j+1} = L_j(\alpha_j)$ where $\alpha_j^{n_j} \in L_j$ for some integer $n_j \geq 2$.
We say that an element $\alpha$ is **expressable by radicals** over $K$ if it is contained in a radical extension of $K$.
We say that a polynomial over $K$ is **solvable (or soluble) by radical** if every root is experessable by radicals (i.e. its splitting field is contained in a radical extension).

---

**Definition.** A finite group $G$ is called **solvable (or soluble)** if there exists a chain of subgroups

$$\{1\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_m = G$$

such that each for each $i = 0, 1, \ldots, m = 1$, $G_i$ is a normal subgroup of $G_{i+1}$ (denoted $G_i \triangleleft G_{i+1}$) and $G_{i+1}/G_i$ is cyclic.

---

We will prove the following in the next few classes.

**Theorem 1.** (Galois) Let $K$ be a field of characteristic 0. A polynomial $f(x) \in K[x]$ is solvable by radicals if and only if its Galois group is solvable.

**Theorem 2.** For every integer $n \geq 1$ there exists a field $K$ of characteristic 0 and a polynomial $f(x) \in K[x]$ of degree $n$ such that the Galois group of $f$ over $K$ is isomorphic to $S_n$. (Note: The symmetric group $S_n$ is unsolvable for $n \geq 5$.)

**Theorem 3.** For every integer $n \geq 1$ there exists a polynomial $f(x) \in \mathbb{Q}[x]$ of degree $n$ such that the Galois group of $f$ over $\mathbb{Q}$ is isomorphic to the symmetric group $S_n$.
(We will only prove this for prime $n$.)

---

Exercises: (more on the back)

1. Let $K$ be a field of characteristic 0, let $a \in K - \{0\}$, and let $L$ be the splitting field of $x^n - a$ over $K$. Prove that $L$ contains all $n^{th}$ roots of unity.

2. Let $K$ be a field of characteristic 0 containing all $n^{th}$ roots of unity and let $L = K(\alpha)$ where $\alpha^n \in K$. Prove that $\mathrm{Gal}(L : K)$ is a cyclic group. (Hint: consider the map $\varphi : \mathrm{Gal}(L : K) \to K^*$ defined by $\sigma \mapsto \sigma(\alpha) \cdot \alpha^{-1}$. Show that it is an injective homomorphism.)

3. Prove that finite abelian groups are solvable.

4. Prove that $S_3$ and $S_4$ are solvable.

5. Prove that the symmetric group $S_n$ is unsolvable for $n \geq 5$.

6. Prove that a subgroup of a solvable group is solvable.

7. Prove that the quotient of a solvable group by a normal subgroup is solvable.

8. Prove that if a group $G$ has a normal subgroup $N$ such that both $N$ and $G/N$ are solvable, then $G$ is also solvable.