1 Insolvable quintic equations

Let G be a finite group. The following result is usually covered in a first course on group theory:

Theorem (Sylow)**.** Suppose that $|G| = p^n \cdot a$ where $\gcd(a, p) = 1$ with p prime and $n \geq 0$.
Then there is a subgroup $H \subseteq G$ such that $|H| = p^n$.
Furthermore, if $H, H' \subseteq G$ are two subgroups with $|H| = |H'| = p^n$ then $g^{-1}Hg = H'$ for some $g \in G$.

A subgroup $H \subseteq G$ as in the theorem is called a *p-Sylow subgroup* of G.
According to the theorem, any two p-Sylow subgroups of G are conjugate.

Corollary (Cauchy)**.** If p is prime that divides $|G|$, then there is an element of order p in G.

Proof. We know that G has a p-Sylow subgroup H. This is a p-group so has nontrivial center.
Take any non-identity element of the center.
The order of this element is a nontrivial power of p as the cyclic group it generates has size dividing p^n.
An appropriate power of this element has order p. □

Let $n, k \geq 0$. Let $\sigma \in S_n$ and write $\langle g \rangle$ for the subgroup of S_n generated by σ.
Recall that σ is is said to be a *k-cycle* if

- $\langle g \rangle$ has one orbit of cardinality k in $\{1, \ldots, n\}$; and
- all the other orbits of $\langle g \rangle$ have cardinality 1.

Note that an orbit of cardinality 1 is a subset of $\{1, \ldots, n\}$ consisting of a fixed point of σ.
Note also that a k-cycle necessarily has order k.
A *transposition* is a 2-cycle.

Lemma. Let p be a prime number and let $\sigma \in S_p$. Suppose that the order of σ is p. Then σ is a p-cycle.

Proof. Let $a \in \{1, \ldots, p\}$. Then we have $|\mathrm{Orb}(\langle \sigma \rangle, a)| \cdot |\mathrm{Stab}(\langle \sigma \rangle, a)| = p$.
Since the only subgroups of $\langle \sigma \rangle$ are $\langle \sigma \rangle$ and $\{1\}$, we conclude that $|\mathrm{Orb}(\langle \sigma \rangle, a)|$ is equal to either p or 1.

Let A be the number of orbits with cardinality p and let B be the number of fixed points of σ.
We then have $pA + B = p$ and $B = 0$ and $A = 1$.
Thus $\langle \sigma \rangle$ has exactly one orbit, and it has cardinality p. In particular, σ is a p-cycle. □

Proposition. Let p be a prime number.
Let $\sigma, \tau \in S_p$ and suppose that σ is a transposition and that τ is a p-cycle. Then σ and τ generate S_p.

Proof. By conjugating σ by τ^k, we get $p-1$ transpositions (a_i, a_{i+1}) where $\{a_1, a_2, \ldots, a_p\} = \{1, 2, \ldots, p\}$.
These elements generate S_p. □

Proposition. Let p be a prime number and let $P(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree p. Suppose that $P(x)$ has precisely $p-2$ real roots in $\mathbb{C}$. Then $\mathrm{Gal}(P) \cong S_p$.

Proof. Let $L \mid \mathbb{Q}$ be a splitting field for $P(x)$.
We identify L with the field generated over $\mathbb{Q}$ by the roots of $P(x)$ in $\mathbb{C}$.
The roots of $P(x)$ are distinct since $P(x)$ is separable.

Choosing a labelling of the roots of $P(x)$ in L, we may view $\mathrm{Gal}(L \mid K)$ as a subgroup of S_p.
Since $P(x)$ is irreducible, the ring $\mathbb{Q}[x]/(P(x))$ is a field and there is a homomorphism of $\mathbb{Q}$-extensions

$$\mathbb{Q}[x]/(P(x)) \hookrightarrow L$$

and so p divides $[L : K]$.
Since $|\mathrm{Gal}(L \mid K)| = [L : K]$, we see that p divides $|\mathrm{Gal}(L \mid K)|$.
We can thus conclude from Cauchy's theorem that there is an element σ of order p in $\mathrm{Gal}(L \mid K)$.

From the lemmas, we conclude that σ is a p-cycle of S_p.
On the other hand, complex conjugation is a field automorphism of $\mathbb{C}$.
Since $L \mid \mathbb{Q}$ is a Galois extension, we see that the image of L under complex conjugation is again L.
Hence it restricts to an element $\kappa \in \mathrm{Gal}(L \mid \mathbb{Q})$.

We have $\kappa \neq \mathrm{id}_L$ since $P(x)$ has non-real roots by assumption.
Let $\alpha, \beta \in L$ be the two non-real roots of $P(x)$.
Then we must have $\kappa(\alpha) = \beta$, since κ fixes all the other roots of $P(x)$ by assumption and $\kappa \neq \mathrm{id}_L$.
In particular, κ is a transposition in S_p.
By the previous proposition, the elements κ and σ generate S_p and thus $\mathrm{Gal}(L \mid K) = S_p$. □

Corollary. The polynomial $x^5 - 6x + 3 \in \mathbb{Q}[x]$ is not solvable by radicals.

Proof. $P(x) := x^5 - 6x + 3$ is irreducible by *Eisenstein's criterion* (for $p = 3$; see the lecture notes).
Furthermore, we compute $P(-1) = 8 > 0$ and $P(1) = -2 < 0$.
Also $\lim_{x\to\infty} P(x) = \infty$ and $\lim_{x\to-\infty} = -\infty$.

Hence $P(x)$ has roots in $(-\infty, -1)$, $(-1, 1)$ and $(1, \infty)$ by the intermediate value theorem.
In particular, $P(x)$ has at least three roots in $\mathbb{R}$. Finally, we compute

$$\frac{d}{dx}P(x) = 5x^4 - 6$$

and the real roots of $\frac{d}{dx}P(x)$ are $\pm\sqrt[4]{6}$.

If $P(x)$ had more than three roots in $\mathbb{R}$, then $\frac{d}{dx}P(x)$ would have at least three roots in $\mathbb{R}$ by the mean value theorem, which is not possible.

We conclude that $P(x)$ has precisely $3 = 5 - 2$ roots in $\mathbb{R}$.

Thus by the previous proposition $\mathrm{Gal}(P) \cong S_5$.
Since S_5 is not solvable, we conclude that $P(x)$ is not solvable by radicals. □

2 The fundamental theorem of algebra via Galois theory

We will now prove that $\mathbb{C}$ is algebraically closed using Galois theory and basic real analysis.
We need the following fact.

Lemma. Let $P(x) \in \mathbb{R}[x]$ be a monic polynomial of odd degree. Then $P(x)$ has a root in $\mathbb{R}$.

Proof. Let $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. When $x \neq 0$, we have

$$P(x) = x^n(1 + a_{n-1}/x + a_{n-2}/x^2 + \cdots + a_0/x^n).$$

Since

$$\lim_{x \to \pm\infty} 1 + a_{n-1}/x + a_{n-2}/x^2 + \cdots + a_0/x^n) = 1$$

there is a real number $x_1 > 0$ such that $1 + a_{n-1}/x_1 + a_{n-2}/x_1^2 + \cdots + a_0/x_1^n > 0$.

Similarly, there is a real number $x_0 < 0$ such that $1 + a_{n-1}/x_0 + a_{n-2}/x_0^2 + \cdots + a_0/x_0^n > 0$.
On the other hand, $x_0^n < 0$ and $x_1^n > 0$ so $P(x_0) < 0$ and $P(x_1) > 0$.
We conclude from the intermediate value theorem that $P(x)$ has a root in the interval $[x_0, x_1]$. □

Theorem. The field $\mathbb{C}$ is algebraically closed.

In the following proof, if

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{C}[x]$$

then we shall write $\overline{P}(x)$ for the polynomial

$$\overline{P}(x) = \overline{a_n}x^n + \overline{a_{n-1}}x^{n-1} + \cdots + \overline{a_0} \in \mathbb{C}[x]$$

where $\overline{a}$ is the complex conjugate of $a \in \mathbb{C}$.

Note that if $Q(x) = P(x)\overline{P}(x)$, then $\overline{Q}(x) = Q(x)$, so that $Q(x) \in \mathbb{R}[x]$.

Proof. Let $P(x) \in \mathbb{C}[x]$. We need to show that $P(x)$ splits.
Replacing $P(x)$ by $P(x)\overline{P}(x)$, we may assume $P(x)$ has even degree and all coefficients in $\mathbb{R}$.

Let $L \mid \mathbb{R}$ be a splitting field of $P(x)$. Let $G = \mathrm{Gal}(L \mid \mathbb{R})$.
Let $G_2 \subseteq G$ be a 2-Sylow subgroup of G. Then let $M = \mathbb{C}^{G_2}$.
The degree $[M : \mathbb{R}]$ is odd by the definition of Sylow subgroups and the main theorem on Galois extensions.

Suppose that $M \mid \mathbb{R}$ is a nontrivial extension and let $\alpha \in M \backslash \mathbb{R}$.
Let $m_\alpha(x) \in \mathbb{R}[x]$ be the minimal polynomial of α.
Then $\deg(m_\alpha(x))$ must divide $[M : \mathbb{R}]$.
In particular $\deg(m_\alpha(x))$ is odd.

Thus, by the previous lemma, $m_\alpha(x)$ has a root in $\mathbb{R}$.
Since $m_\alpha(x)$ is irreducible, this means that $\deg(m_\alpha(x)) = 1$.
This contradicts the fact that $\alpha \in M \backslash \mathbb{R}$.

We conclude that $M \mid \mathbb{R}$ is the trivial extension.
In other words $G_2 = G$. In particular $|G| = 2^k$ for some $k \geq 0$.

We may suppose without loss of generality that $k > 0$ as otherwise $P(x)$ splits in $\mathbb{R}$.
The group is solvable since it is a p-group for $p = 2$.
Thus there is a finite filtration of G that has cyclic quotients of order 2.
This gives rise via the fundamental theorem of Galois extensions to a sequence of subfields

$$L = L_n \supseteq L_{n-1} \supseteq \cdots \supseteq L_0 = \mathbb{R}$$

such that L_{i+1} is Galois over L_i for all $i \in \{0, \ldots, n-1\}$, and $\mathrm{Gal}(L_{i+1} \mid L_i) \cong \mathbb{Z}/2\mathbb{Z}$.

By our results on Kummer extensions, there exists $\beta \in L_1$ with $\beta^2 \in L_0 = \mathbb{R}$ and $L_1 = \mathbb{R}(\beta)$.
Since any positive element of $\mathbb{R}$ has a square root in $\mathbb{R}$, we see that $\beta^2 < 0$ as $L_1 \mid L_0$ is nontrivial.
Now we may compute

$$(\beta/\sqrt{|\beta^2|})^2 = \beta^2/|\beta^2| = -1.$$

Thus the polynomial $x^2 + 1 \in \mathbb{R}[x]$ has a root in L_1.
In particular, $x^2 + 1$ splits in L_1.

Since $x^2 + 1$ has no roots in $\mathbb{R}$ and $[L_1 : L] = 2$, we conclude that L_1 is a splitting field for $x^2 + 1$.
In other words $L_1 \cong \mathbb{C}$ as an $\mathbb{R}$-extension.

Now suppose that $k > 1$.
By similar reasoning, there exists $\rho \in L_2$ such that $\rho^2 \in L_1 \cong \mathbb{C}$ and such that $L_2 = L_1(\rho)$.
Furthermore $L_2 \mid L_1$ is a nontrivial extension by assumption.
This is a contradiction, because any element of $L_1 \cong \mathbb{C}$ has a square root.
Explicitly, if $z = re^{i\theta}$ then $\sqrt{r}e^{i\theta/2}$ is a square root of z.

We conclude that $k = 1$ and thus $L = L_1 \cong \mathbb{C}$. In particular, $P(x)$ splits in $\mathbb{C}$. □