14. Solvability by Radicals

Proposition 14.1. *Let L/K be the splitting field of the polynomial $x^n - a \in K[x]$, where n is coprime to the characteristic.*

Then the Galois group G is solvable.

Proof. Let $L/M/K$ be a splitting field for $x^n - 1$, and let H be the corresponding subgroup of G. Then H is the Galois group of L/M, H is normal in G and G/H is the Galois group of M/K. We have already seen that G/H is abelian. Thus it suffices to prove that H is solvable.

In particular we may assume that $x^n - 1$ splits in K. Suppose that $n = lm$. Let $L/M/K$ be a splitting field for $x^m - a$. Then M/K is normal, so that the corresponding subgroup H of G is normal as well. The extension L/M is a splitting field for $x^l - b$, where $b^m = a$. As

$$0 \longrightarrow H \longrightarrow G \longrightarrow G/H \longrightarrow 0,$$

is a short exact sequence, and the two extreme groups are the Galois groups for $x^l - b$ and $x^m - a$, we reduce to the case when n is prime.

Thus we may assume that $x^n - a$ is irreducible, in which case G is abelian. □

Definition 14.2. *Let $f(x) \in K[x]$ be a polynomial.*

We say that $f(x)$ is ***solvable by radicals*** *if there is a tower of extensions*

$$K = R_0 \subset R_1 \subset R_2 \subset R_n,$$

such that $R_i = R_{i-1}(\alpha_i)$, where $a_i = \alpha_i^{m_i} \in R_{i-1}$ for some m_i coprime to the characteristic and $f(x)$ splits in R_n.

Lemma 14.3. *Suppose that $f(x) \in K[x]$ is solvable by radicals.*

Then we may find a tower as in (14.2) such that R_m/K is Galois for all $1 \leq m \leq n$.

Proof. We have

$$K = S_0 \subset S_1 \subset S_2 \subset S_n,$$

such that $S_i = S_{i-1}(\alpha_i)$, where $a_i = \alpha_i^{m_i} \in S_{i-1}$ for some m_i coprime to the characteristic and $f(x)$ splits in S_n.

Let R_1 be a splitting field for $x^{m_1} - a_1$. Clearly S_1 is (isomorphic to) a subset of R_1. Then R_1 contains a splitting field for $x^n - 1$, M_1 and the two extensions R_1/M_1 and M_1/K are radical.

Now consider the polynomial $x^{m_2} - a_2$. Then $a_2 \in R_1$ but unfortunately not necessarily in K. On the other hand,

$$\prod_{\phi \in G} (x^{m_2} - \phi(a_2)),$$

is invariant under the action of the Galois group G of R_1/K and so lies in $K[x]$. Let R_2/R_1 be a splitting field extension. Then R_2/K is Galois and clearly R_2/K is a succession of radical extensions.

Continuing in this way, the result is clear by induction. □

Lemma 14.4. *Let L/K be a finite field extension and suppose that $L/M/K$ and $L/N/K$ are two intermediary fields such that L is the field generated by M and N. Suppose that M/K is Galois with Galois group G.*

Then L/N is Galois, with Galois group I isomorphic to

$$H = \operatorname{Gal}(M/M \cap N) \subset G.$$

Proof. Suppose that M/K is the splitting field of $f(x)$. Then so is L/N and $f(x)$ is separable. In particular L/N is Galois.

Suppose we are given an element σ of I. Then σ is an automorphism of L/K. As M/K is normal, $\sigma|_M$ is an automorphism of M/K. Thus there is a group homomorphism

$$\rho\colon I \longrightarrow G.$$

Let $\alpha_1, \alpha_2, \dots, \alpha_n$ be the roots of $f(x)$. Now $\rho(\sigma)$ is the identity map if and only if its action on the roots is the identity. But then σ is the identity as well. It follows that ρ is injective. Clearly $\rho(\sigma)$ fixes $M \cap N$, so that the image of ρ is a subgroup of H. On the other hand, if $\alpha \notin N$, then there is a σ that does not fix α. Thus the fixed field of the image is contained in $M \cap N$. □

Theorem 14.5. *Let $f(x) \in K[x]$ be a separable polynomial, whose Galois group G has order n, which is coprime to the characteristic.*

Then $f(x)$ is solvable by radicals if and only if the Galois group of $f(x)$ is solvable.

Proof. Suppose that the Galois groups is solvable. Let $\bar{K}$ be the algebraic closure of K. Let L'/K be a field extension obtained by adjoining nth roots of unity, and let N be the smallest subfield of $\bar{K}$ that contains both L and L'. Then L'/K is a radical extension and the extension N/L' is isomorphic to a subgroup of G.

So we may as well assume that $x^n - 1$ splits in K. As G is solvable, we may find a sequence of subgroups, each of which is normal in the next, with quotient a cyclic group of prime order. Thus we may find a sequence of extensions,

$$K = R_0 \subset R_1 \subset \dots R_n = L,$$

where R_i/R_{i-1} is an extension of degree $p = p_i$ a prime, such that $x^p - 1$ splits in K. We have already seen that then R_i/R_{i-1} is the splitting field for $x^p - a$, for some $a \in R_{i-1}$.

Now suppose that $f(x)$ is solvable by radicals. Let L/K be a splitting field for $f(x)$ and let N/L be an extension of K, which is a succesion of radical extensions, Galois over K. Then the Galois group of N/K is solvable and G is a quotient of a solvable group, whence it is itself solvable. □

Lemma 14.6. *Let $f(x)$ be a rational irreducible polynomial of prime degree p with exactly two roots that are not real.*

Then the Galois group G of $f(x)$ over $K = \mathbb{Q}$ is S_p, the full symmetric group.

Proof. The action of the Galois group is determined by its action on the roots. The only thing to check is that we get the whole of S_p. It suffices to prove that G contains a p-cycle and a transposition.

Let L/K be a splitting field for $f(x)$. Let α be a root of $f(x)$. Then $M = K(\alpha)/K$ has degree p. It follows, by the Tower Law, that the degree of the extension L/K is divisible by p. Thus the Galois group has order divisible by p and so by Sylow's Theorem G contains an element of order p. As $G \subset S_p$, and the only elements of S_p of order p are p-cycles, so in fact G contains a p-cycle.

On the other hand, as $f(x)$ is a real polynomial, complex conjugation acts on the roots of $f(x)$. As there are exactly two complex roots, complex conjugation corresponds to a transposition. □

Corollary 14.7. *The polynomial $x^5 - 6x + 3$ is not solvable by radicals.*

Proof. It suffices to check that $f(x)$ is irreducible and has three real roots.

Irreducibility follows from Eisenstein. $f(-2) < 0$, $f(0) = 3$, $f(1) < 0$ and $f(2) > 0$, so that by the IVT $f(x)$ has at least three real roots. On the other hand, the real zeroes of $f(x)$ are interspersed with the zeroes of the derivative $f(x) = 5x^4 - 6$, which has only two real roots. □