§ 7 Soluble groups

Remember our plan for proving the insolubility of the quintic. The basic idea is the following. Suppose that a polynomial is soluble by radicals (we'll make this more precise later). This implies that all of its roots have a certain form, and thus that the splitting field extension has a certain structure. We will see that this implies that the corresponding Galois group has a similar sort of structure. By exhibiting explicit examples of quintics whose Galois groups do not have this structure, we will see that not every quintic is soluble by radicals. We first need a digression in group theory.

In this section we develop the group theory necessary for applications to Galois theory. We begin with a summary of the results from this section that we will need for applications to Galois theory.

Definition 7.1 A group G is *soluble* provided it has a chain of subgroups

$$G = G_0 > G_1 > \cdots > G_n = \{1\}$$

with each $G_{i+1} \lhd G_i$ and G_i/G_{i+1} abelian. ▲

We start by recalling the first isomorphism theorem for groups (we've already used it, in fact!):

Theorem 7.2 *Let $\varphi : G \longrightarrow H$ be a group homomorphism. Then $\ker \varphi$ is a normal subgroup of G and there is an isomorphism $G/\ker \varphi \to \operatorname{Im} \varphi$.*

As corollaries, we deduce the second and third isomorphism theorems. Let's start with the second.

If H is a subgroup of G, and $N \lhd G$, then write

$$HN = \{hn : h \in H, n \in N\}.$$

It is a subgroup of G.

Theorem 7.3 *Let H and N be subgroups of G with $N \lhd G$. Then $H \cap N \lhd H$ and*

$$H/H \cap N \cong HN/N.$$

PROOF. Define a map $\Phi : H \longrightarrow HN/N$ by $h \mapsto hN$. It is not hard to see that Φ is a surjective homomorphism with kernel $H \cap N$. The result follows from the first isomorphism theorem. ⊠

Next, we do the third isomorphism theorem.

Theorem 7.4 *Let H and N be normal subgroups of G with $H \supseteq N$. Then $H/N \lhd G/N$ and*

$$(G/N)/(H/N) \cong G/H.$$

PROOF. Define a map $\Psi : G/N \to G/H$ by $\Psi(gN) = gH$. It is easy to check that Ψ is a well-defined surjective homomorphism with kernel H/N. Now use the first isomorphism theorem. ⊠

Having proven these technical results, we can now return to the study of soluble groups.

Theorem 7.5 *Let G be a group and H, N subgroups of G with $N \lhd G$. Then*

1. *if G is soluble then H is soluble;*
2. *if G is soluble then G/N is soluble;*
3. *if N and G/N are soluble then G is soluble.*

PROOF. 1. By definition, G has a chain

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{1\}$$

with each G_i/G_{i+1} abelian. Set $H_i = G_i \cap H$. So we have

$$H = H_0 \rhd H_1 \rhd \cdots \rhd H_r = \{1\}$$

(where we have deleted any redundant terms).

Note that $H_{i+1} = G_{i+1} \cap H = (G_i \cap H) \cap G_{i+1}$. Thus, by the second isomorphism theorem (7.3),

$$H_i/H_{i+1} = (G_i \cap H)/((G_i \cap H) \cap G_{i+1}) \cong (G_i \cap H)G_{i+1}/G_{i+1}.$$

This last group is a subgroup of the abelian group G_i/G_{i+1} and so is abelian. This proves 1.

2. Again G has the chain of 1. Apply the canonical homomorphism $\pi : G \to G/N$ sending g to gN. Then we get

$$G/N = G_0N/N \rhd G_1N/N \rhd \cdots \rhd G_nN/N = \{1_{G/N}\}$$

(discarding redundant terms). Now,

$$(G_iN/N)/(G_{i+1}N/N) \cong G_iN/G_{i+1}N,$$

by the third isomorphism theorem (7.4). On the other hand, the latter group is

$$G_i(G_{i+1}N)/G_{i+1}N \cong G_i/G_i \cap (G_{i+1}N),$$

by the second isomorphism theorem. Finally, by the third isomorphism theorem, we have

$$G_i/G_i \cap G_{i+1}N \cong (G_i/G_{i+1})/((G_i \cap G_{i+1}N)/G_{i+1}))$$

which (being a quotient of the abelian group G_i/G_{i+1}) is abelian.

3. Let $\overline{G}$ denote the quotient G/N. Suppose

$$\overline{G} \triangleright \overline{G}_1 \triangleright \cdots \triangleright \overline{G}_n = \{1\}$$

and

$$N \triangleright N_1 \triangleright \cdots \triangleright N_m = \{1\}$$

with all successive quotients being abelian. Let

$$G_i = \{g \in G \mid gN \in \overline{G}_i\}.$$

Firstly, we see that G_i is a subgroup of G. For this, we use the subgroup criterion. Clearly $1 \in G_i$. Let g_1, $g_2 \in G_i$. Consider $g_1 g_2^{-1}$. Then

$$(g_1 g_2^{-1})N = (g_1 N)(g_2 N)^{-1} \in \overline{G}_i$$

as $\overline{G}_i$ is a group. It follows that $g_1 g_2^{-1} \in G_i$, and, by the subgroup criterion, G_i is a group.

Next we check that $G_i/N = \overline{G}_i$. The quotient G_i/N consists of all cosets gN with $g \in G_i$ – but the defining property of this group is that these cosets all lie in $\overline{G}_i$. It follows that $G_i/N \subseteq \overline{G}_i$. Conversely, every element of $\overline{G}_i$ is some coset gN, and then the corresponding g must lie in G_i, whereupon the inclusion $G_i/N \longrightarrow \overline{G}_i$ is surjective.

Lastly, we claim that $G_{i+1} \lhd G_i$. Let $g \in G_{i+1}$, and $\gamma \in G_i$. Then we want to show that $\gamma^{-1} g \gamma \in G_{i+1}$. But

$$(\gamma^{-1} g \gamma)N = (\gamma N)^{-1}(gN)(\gamma N) \in \overline{G}_{i+1}$$

because $\overline{G}_{i+1} \lhd \overline{G}_i$. It follows that $\gamma^{-1} g \gamma \in G_{i+1}$, as required. By the third isomorphism theorem, we also see that

$$\frac{\overline{G}_i}{\overline{G}_{i+1}} = \frac{G_i/N}{G_{i+1}/N} \cong \frac{G_i}{G_{i+1}},$$

so that each quotient G_i/G_{i+1} is abelian. Then the sequence

$$G \triangleright G_1 \triangleright \cdots \triangleright G_n = N \triangleright N_1 \triangleright \cdots \triangleright N_m = \{1\}$$

is a series whose successive quotients are all abelian. Thus G is soluble. ⊠

Remark 7.6 1. Abelian groups are soluble (consider the series $G \triangleright \{1\}$).

2. S_3 is soluble. A suitable chain is given by:

$$S_3 \triangleright \langle (123) \rangle \triangleright \{1\}.$$

3. S_4 is soluble. Here, a suitable chain is given by:

$$S_4 \triangleright A_4 \triangleright V_4 \triangleright \{1\},$$

where $V_4 = \{1, (12)(34), (13)(24), (14)(23)\}$.

4. D_4 is soluble. (It is a subgroup of S_4.)

5. A group G is called $simple$ if it is non-trivial and it has no normal subgroups besides $\{1\}$ and G. A group which is soluble and simple is easily seen to be cyclic of prime order.

6. If $n \geq 5$ then A_n is simple and so A_n is not soluble, for $n \geq 5$.

7. If $n \geq 5$, it follows that S_n is not soluble (if S_n were to be soluble, then its subgroup A_n would be soluble, and it isn't).

The crucial result is that S_1, S_2, S_3 and S_4 are soluble groups, but S_5 is not. This will reflect the fact that polynomials of degree up to 4 are soluble by radicals, but that quintics are not in general.

§ 8 Solubility of polynomials

Let's start by making the (now obvious) definition of the Galois group of a polynomial.

Definition 8.1 Let K be a field, and let $f \in K[x]$. Let L be the splitting field of f over K. Define the *Galois group of* f to be $\mathrm{Gal}(L/K)$. (Note that L/K is Galois as L is a splitting field (Theorem 5.8).) We will denote this group $\mathrm{Gal}(f/K)$. ▲

We will explain that many of the properties of f will be reflected in properties of its Galois group. Most importantly, we will see that if the polynomial is soluble in radicals then its Galois group is a soluble group. In fact, the converse is also true, and is proven in Appendix C. As we have produced examples of non-soluble groups, this may indicate that not every polynomial is soluble by radicals. To confirm this, we will give an explicit quintic whose Galois group is S_5.

Let's first recall some earlier results, Lemma 4.10 and Lemma 4.11.

Lemma 4.10. *Let $n \geq 1$ be an integer, and let L be the splitting field over K of $x^n - 1$. Then $\mathrm{Gal}(L/K)$ is abelian.*

Lemma 4.11. *Let K be a field containing the nth roots of unity. Let $a \in K$. If L denotes the splitting field of $x^n - a$ over K, then $\mathrm{Gal}(L/K)$ is cyclic (of order dividing n).*

If the conditions of Lemma 4.11 hold, we call L/K a *Kummer* extension.

Now we turn to solubility by radicals.

Definition 8.2 Let K be a field, and let $f \in K[x]$. The equation $f(x) = 0$ is said to be *soluble by radicals over* K if there is an extension field M of K such that

1. M splits f
2. M has a chain of subfields

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_m = M$$

such that, for each i, $K_{i+1} = K_i(d_i)$ with $d_i^{n_i} \in K_i$ for some positive integer n_i.

▲

Remark 8.3 Then f is soluble by radicals if and only if the roots of f are given by expressions involving elements of K and $+$, $-$, $\times$, $/$, and nth roots.

Now we can prove the theorem which will imply the insolubility of the general quintic.

Theorem 8.4 *If a polynomial $f \in K[x]$ is soluble by radicals, then $\mathrm{Gal}(f/K)$ is a soluble group.*

PROOF. We first find a Galois extension $\widetilde{L}$ of K with $\mathrm{Gal}(\widetilde{L}/K)$ soluble and such that $\widetilde{L}$ splits f.

This suffices to show that $\mathrm{Gal}(f/K)$ is soluble, because if L is the splitting field of f, we have $K \subseteq L \subseteq \widetilde{L}$, and then by Theorem 5.15, $\mathrm{Gal}(f/K) = \mathrm{Gal}(L/K)$ is a quotient of $\mathrm{Gal}(\widetilde{L}/K)$ – and quotients of soluble groups by normal subgroups are again soluble (by Theorem 7.5 (2)).

We are given that f splits in an extension $M = K_m$ of K with the following property: $K_m = K(d_1, \ldots, d_m)$ and, for all i, there exists a positive integer n_i such that $d_i^{n_i} \in K(d_1, \ldots, d_{i-1})$. As before, let ζ denote a primitive nth root of unity, where $n = \prod_i n_i$.

Let $\widetilde{L}$ be the smallest Galois extension of K which contains $K_m(\zeta)$. Then certainly $\widetilde{L}$ splits f (as it contains K_m).

Suppose $\mathrm{Gal}(\widetilde{L}/K) = \{\theta_1 = \mathrm{id}, \theta_2, \ldots, \theta_r\}$. Then each $\theta_i(\zeta)$ (necessarily a power of ζ by APR 3.10) and each $\theta_i(d_j)$ necessarily also lies in $\widetilde{L}$. Conversely, $\widetilde{L}$ is generated by these elements.

Adjoining the generating elements

$$\zeta, d_1, d_2, \ldots, d_m, \theta_2(d_1), \theta_2(d_2), \ldots, \theta_r(d_m)$$

one at a time, we get a sequence of fields

$$K \subseteq K(\zeta) \subseteq K(\zeta, d_1) \subseteq K(\zeta, d_1, d_2) \subseteq \cdots \subseteq \widetilde{L}$$

in which the first extension is Galois and abelian (by Lemma 4.10) and each subsequent non-trivial extension is Galois with cyclic Galois group (by Lemma 4.11).

This corresponds to the chain of subgroups

$$\mathrm{Gal}(\widetilde{L}/K) \triangleright \mathrm{Gal}(\widetilde{L}/K(\zeta)) \triangleright \mathrm{Gal}(\widetilde{L}/K(\zeta, d_1)) \triangleright \cdots \triangleright \mathrm{Gal}(\widetilde{L}/\widetilde{L}) = \{1\}$$

shows that $\mathrm{Gal}(\widetilde{L}/K)$ is soluble, as each successive non-trivial quotient after the first (which is abelian) is cyclic (using Theorem 5.15). ⊠

The converse theorem

The converse of this theorem is also true. Hence a polynomial is soluble by radicals if and only if its Galois group is soluble. To prove this fact, we will some auxiliary lemmas.

Lemma 8.5 Let G be a finite abelian group. Then there exists a chain of subgroups (each necessarily normal in G)

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = \{1\}$$

with each G_i/G_{i+1} cyclic of prime order.

Example 8.6 If $G = \langle a \rangle$ is cyclic of order 30 then one gets such a chain by

$$\langle a \rangle \triangleright \langle a^2 \rangle \triangleright \langle a^6 \rangle \triangleright \{1\}.$$

Here, the factors are C_2, C_3 and C_5. ⊠

PROOF. If G is trivial or cyclic of prime order then the result holds trivially. Otherwise G has a non-trivial, proper subgroup G_1. Choose G_1 to be maximal (i.e., there is no subgroup N with $G \triangleright N > G_1$). By induction on the order of G, the subgroup G_1 has an appropriate chain of subgroups

$$G_1 \triangleright G_2 \triangleright \cdots \triangleright G_n = \{1\}.$$

Furthermore, G/G_1 has no non-trivial, proper subgroups and so is cyclic of prime order. The result follows. ⊠

As a result of this lemma, we can give an alternative characterisation of when groups are soluble.

Corollary 8.7 A finite group G is soluble if and only if there is a chain of subgroups

$$G = G_0 > G_1 > \cdots > G_n = \{1\}$$

with each $G_{i+1} \lhd G_i$ and G_i/G_{i+1} cyclic of prime order.

PROOF. ($\Longleftarrow$) is clear.

($\Longrightarrow$) Let G be finite and soluble. Take a series

$$G \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_n = \{1\}.$$

The successive quotients are abelian. In particular, the quotient $\overline{G} = G/G_1$ is abelian. By the previous lemma, there is a sequence

$$\overline{G} \triangleright \overline{G}_1 \triangleright \cdots \triangleright \overline{G}_m = \{1\}$$

in which each quotient is a cyclic group of prime order. By the same technique as Theorem 7.5 (3), we can lift this to a series

$$G \triangleright G_{11} \triangleright \cdots \triangleright G_{1m} = G_1$$

and all successive quotients are cyclic of prime order. Similarly, between G_1 and G_2 we can construct a sequence

$$G_1 \triangleright G_{21} \triangleright \cdots \triangleright G_{2r} = G_2,$$

and so on between each pair of terms. Stringing these together gives a sequence of the desired type. ⊠

Our next result gives a converse to Lemma 4.11.

Lemma 8.8 (Kummer Theory) Let ζ be a primitive n^{th} root of unity, and let $K \subseteq \mathbb{C}$ be a field such that $K \supset \mathbb{Q}(\zeta)$. Suppose that L/K is a Galois extension with Galois group C_n. Then L/K is a Kummer extension—i.e. there exists $\alpha \in K$ such that

$$L = K(\sqrt[n]{\alpha}).$$

PROOF. Write $\mathrm{Gal}(L/K) = \langle\varphi\rangle$ for a choice of generator $\varphi \in \mathrm{Gal}(L/K)$.

Suppose that we could find an element $\beta \in L^\times$ such that $\varphi(\beta) = \zeta\beta$. Then:

- The elements $\varphi^i(\beta) = \zeta^i\beta$ would give n distinct elements of K. Moreover, by Theorem 3.10 (APR), these elements are roots of the minimal polynomial of β. It follows that $[K(\beta) : K] \geq n$. Since $[L : K] = n$, it follows that $L = K(\beta)$.
- We have $\varphi(\beta^n) = \varphi(\beta)^n = \beta^n$, so that $\beta^n \in L^{\{\varphi\}} = L^{\mathrm{Gal}(L/K)} = K$.

Writing $\alpha = \beta^n$, we would therefore be able to deduce that $L = K(\sqrt[n]{\alpha})$.

Hence, it is sufficient to prove that there is an element $\beta \in L^\times$ such that $\varphi(\beta) = \zeta\beta$. Equivalently, viewing φ as a K-linear map $L \to L$, it is sufficient to prove that φ has ζ as an eigenvalue.

Write μ_n for the multiplicative group of n^{th} roots of 1. Let Λ denote the set of eigenvalues of φ. It's clear that $\Lambda \subset \mu_n$. Indeed, if $\lambda \in \Lambda$ has eigenvector $\beta \in L^\times$, then

$$\beta = \varphi^n(\beta) = \lambda^n\beta,$$

from which it follows that $\lambda^n = 1$.

Moreover, Λ is a group under multiplication: if $\lambda_1, \lambda_2 \in \Lambda$, and λ_i has eigenvector β_i, then because φ is also a field homomorphism,

$$\varphi(\beta_1\beta_2^{-1}) = \varphi(\beta_1)\varphi(\beta_2)^{-1} = \lambda_1\lambda_2^{-1}(\beta_1\beta_2^{-1}),$$

so that $\lambda_1\lambda_2^{-1} \in \Lambda$.

The subgroups of μ_n are exactly the groups μ_d for $d \mid n$. Suppose that $\Lambda = \mu_d$ for some $d \mid n$. Since $\varphi^n = 1$, φ is diagonalisable. And since $\Lambda = \mu_d$, then φ^d is a diagonalisable linear map with eigenvalues all 1. So $\varphi^d = 1$. Hence, we must have $d = n$. The result follows. ⊠

Theorem 8.9 *Let $f \in K[x]$. If $\mathrm{Gal}(f/K)$ is soluble, then f is soluble by radicals.*

PROOF. Write L for the splitting field of f. By the assumption that $\mathrm{Gal}(L/K)$ is soluble combined with Lemma 8.7, we can find

$$\mathrm{Gal}(L/K) = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{1\}$$

such that G_i/G_{i+1} is cyclic of order n_i. Applying the fundamental theorem of Galois theory, we can find

$$K = K_0 \subset K_1 \subset \cdots \subset K_n = L$$

such that $\mathrm{Gal}(K_{i+1}/K_i) = G_i/G_{i+1}$.

Let $K_i' = K_i(\zeta)$ with ζ is a primitive $\prod_i n_i$th root of 1. So we have

$$K \subset K(\zeta) \subset K_1(\zeta) \subset \cdots \subset K_n(\zeta) = L(\zeta).$$

Clearly $L(\zeta)$ splits f over K, so it remains to show that for each i, $K_{i+1}' = K_i'(\sqrt[n_i]{d_i})$ for some $d_i \in K_i'$. Now, for each i, the map

$$\mathrm{Gal}(K_{i+}'/K_i') \to \mathrm{Gal}(K_{i+1}/K_i)$$

given by $\varphi \mapsto \varphi|_{K_{i+1}}$ is an injection: by Theorem 2.5 (TPE), $K_{i+1} = K_i(\gamma)$ for some $\gamma \in K_i$, $K_{i+1}' = K_i'(\gamma)$ by definition, and hence, any $\varphi \in \mathrm{Gal}(K_{i+1}'/K_i')$ is determined by $\varphi(\gamma)$. Moreover, K_{i+1}'/K_i' is Galois, since it is the splitting field of the minimal polynomial of γ.

Hence, by Lemma 8.8, each K_{i+1}'/K_i' is a Kummer extension. The result follows. ⊠

§ 9 Polynomials again

Let $f \in K[x]$ be a polynomial of degree n and let L be its splitting field. We have already seen the following:

- The Galois group $\mathrm{Gal}(f/K) = \mathrm{Gal}(L/K)$ may be regarded as a subgroup of the symmetric group S_n (Lemma 3.16), simply by looking at the action of each automorphism on the n roots of f in L;
- f is soluble by radicals implies that $\mathrm{Gal}(f/K)$ is a soluble group (Theorem 8.4), and in Appendix C we prove the converse (Theorem 8.9);
- S_n is soluble for $n = 1, 2, 3, 4$ and is not soluble for $n \geq 5$ (Remark 7.6);
- Any subgroup of a soluble group is again soluble (Theorem 7.5(1)).

Together, these imply that any polynomial of degree up to 4 is soluble by radicals, which, of course, we saw in Chapter 1. We'll make a few remarks on the process for finding roots from a more Galois-theoretic point of view.

Later in the section, we will explain how to construct polynomials whose Galois group is S_5, and which are therefore not soluble by radicals.

Transitivity

Suppose that $f(x) \in K[x]$ is an irreducible polynomial of degree n. Then we know that $\mathrm{Gal}(f/K) \subset S_n$. But clearly, there are restrictions on what the Galois group of f can be! For example, if $\mathrm{Gal}(f/K)$ is the trivial group, then that means f must have been completely reducible. In this subsection, we will prove that the Galois group of an irreducible polynomial of degree n is a *transitive* subgroup of S_n. Roughly, this means that given any two roots of f, there is an element of the Galois group which maps the first root to the second root.

Definition 9.1 We say that a subgroup $G \subseteq S_n$ is *transitive* if for any pair i, $j \in \{1, \ldots, n\}$, there is a permutation $\rho \in G$ such that ρ maps i to j. ▲

Then we have

Proposition 9.2 Let $f \in K[x]$ have only simple roots. Then $f(x)$ is irreducible if and only if $\mathrm{Gal}(f/K)$ permutes the roots of f transitively.

PROOF. First suppose f is irreducible. Let L denote a splitting field for f over K. If α and β are any two roots in L of f, then there is a K-automorphism of L mapping α to β. It follows that $\mathrm{Gal}(f/K)$ acts transitively on the roots.

Conversely, if f is reducible, and α is a root of f, let g denote the minimal polynomial of α over K. As $f(\alpha) = 0$, we have that $g|f$; further $f \neq g$ as f is reducible and g is irreducible. So $f = gh$ with $\deg h \geq 1$. By APR (Theorem 3.10), automorphisms of L permute the roots of g. So automorphisms of L can only map α to other roots of g; if β is a root of h, there is no automorphism mapping α to β. ⊠

Example 9.3 We illustrate this with one of the earlier examples. Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. We saw earlier that $\mathrm{Gal}(L/K) = V_4$, and computed the action of the group of the roots of $(x^2 - 2)(x^2 - 3)$ and on the roots of $x^4 - 10x^2 + 1$, the minimal polynomial of $\sqrt{2} + \sqrt{3}$. We saw that in the first case, the action was not transitive, and corresponded to the subgroup generated by $(1\ 2)$ and $(3\ 4)$, whereas in the second case, it was transitive, and corresponded to the subgroup of S_4 generated by $(1\ 2)(3\ 4)$ and $(1\ 3)(2\ 4)$. ⊠

Polynomials of degree $\leqslant 4$

Degree 1

Note that when solving an equation of degree 1 over a field K, the root also lies in K. So the splitting field of a degree 1 polynomial over K is K itself. And indeed this also follows from the Galois-theoretic observation that the Galois group $\mathrm{Gal}(f/K)$ is a subgroup of the 1-element group S_1.

Degree 2

Since the solutions to

$$x^2 + ax + b = 0$$

are

$$x = \frac{-a \pm \sqrt{a^2 - 4b}}{2},$$

in general, the roots are contained in an extension of degree 2 over K, obtained by adjoining the root of the discriminant $a^2 - 4b$ to K. Again, this could have been expected from the Galois theory, as S_2 is a group with 2 elements. If the square root lies in K (equivalently, if the quadratic factors), then the splitting field is K itself, and the Galois group of the polynomial is trivial, otherwise, it has 2 elements, and is therefore cyclic.

Degree 3

Remember that we solved the cubic as follows. We started by completing the cube, replacing the variable x by $x + \frac{a}{3}$. Then

$$x^3 + ax^2 + bx + c = 0$$

may be put in the form

$$X^3 + BX + C = 0.$$

Then we wrote $X = u + v$, and derived a pair of equations

$$\begin{aligned} u^3 + v^3 + C &= 0, \\ 3uv + B &= 0. \end{aligned}$$

This led to a quadratic whose roots were u^3 and v^3:

$$y^2 + Cy - \frac{B^3}{27} = 0,$$

so u^3 and v^3 are

$$\frac{-C \pm \sqrt{C^2 + \frac{4B^3}{27}}}{2}.$$

Then u may be taken to be one of the three complex cube roots of

$$\frac{-C + \sqrt{C^2 + \frac{4B^3}{27}}}{2}$$

and the choice of v may be read off from the equation $3uv + B = 0$.

Now, suppose that we're given an irreducible polynomial $f(x) = x^3 + Bx + C \in K[x]$ of degree 3. Let's see how we can use Galois theory to rederive this method. Let L be the splitting field of f, and let $M = L(\omega)$, where ω is a primitive cubed root of 1. Then we have

$$K \subset K(\omega) \subset M.$$

We know that $\mathrm{Gal}(M/K(\omega))$ is a transitive subgroup of S_3, so is either $A_3 = \langle (123) \rangle$ or S_3. Either way, by the Galois correspondence, we can find an intermediate extension

$$K(\omega) \subset K_1 \subset M,$$

where K_1 is the fixed field M^{A_3}.

Now suppose that f has roots $\alpha_1, \alpha_2, \alpha_3 \in M$. Equating $x^3 + bx + C = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$, we find that

$$\begin{aligned} 0 &= \alpha_1 + \alpha_2 + \alpha_3 \\ B &= \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 \\ C &= -\alpha_1\alpha_2\alpha_3. \end{aligned}$$

We want to find a generator for $K_1/K(\omega)$. Since $K_1 = M^{(123)}$, and (123) acts on $\{\alpha_1, \alpha_2, \alpha_3\}$, we should look for combinations of $\alpha_1, \alpha_2, \alpha_3$ which are fixed by (123). Consider the elements

$$u = \frac{1}{3}(\alpha_1 + \omega\alpha_2 + \omega^2\alpha^3)$$

$$v = \frac{1}{3}(\alpha_1 + \omega^2\alpha_2 + \omega\alpha^3)$$

in M. We will make a few observations:

- We can recover $\alpha_1, \alpha_2, \alpha_3$ from u, v. Indeed,

$$\begin{aligned}\alpha_1 &= u + v\\ \alpha_2 &= \omega^2 u + \omega v = \omega^2(u + \omega^2 v)\\ \alpha_3 &= \omega u + \omega^2 v = \omega(u + \omega v).\end{aligned}$$

- We have $(123)u = \omega u$, so that $(123)u^3 = u^3$. Hence, $u^3 \in M^{(123)} = K_1$. Similarly, $v^3 \in K_1$.

- We have

$$\begin{aligned}u^3 + v^3 = (u + v)(u + \omega v)(u + \omega^2 v) &= \alpha_1\alpha_2\alpha_3 = -C\\ uv = \frac{1}{9}(\alpha_1^3 + \alpha_2^3 + \alpha - 3^3 + (\omega + \omega^2)(\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1)&\\ = \frac{1}{9}((\alpha_1 + \alpha_2 + \alpha_3)^3 - 3(\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1))&\\ = -\frac{1}{3}B.&\end{aligned}$$

  Hence u^3 and v^3 are roots of the polynomial

$$y^2 + Cy - \frac{B^3}{27} = 0.$$

We find that

$$K \subset K(\omega) \subset K(u^3) = K(\sqrt{C^2 + \frac{4B^3}{27}}) \subset K(u) = M.$$

This shows that f is soluble by radicals, as well as giving a method to solve f by finding u and v.

Degree 4

To solve the quartic we started by constructing the resolvent cubic:

$$X^4 + pX^2 + qX + r = 0,$$

we started by constructing the resolvent cubic:

$$Y^3 + 2pY^2 + (p^2 - 4r)Y - q^2 = 0.$$

The roots of this cubic were β^2, γ^2 and δ^2, where $\beta = \alpha_1 + \alpha_2$, $\gamma = \alpha_1 + \alpha_3$ and $\delta = \alpha_1 + \alpha_4$. The procedure to write down the roots of the quartic is as follows. Firstly, solve the resolvent cubic, which, as we saw above, means that we must first adjoin a square root, and then a cube root. This gives values of β^2, γ^2 and δ^2. To get the possible values of β and γ, we have to adjoin square roots of β^2 and γ^2. Then the value of δ can be read off, and the roots of the quartic can be recovered from just knowing β, γ and δ (and the fact that the sum of the roots, $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$).

Now let's see how we can rederive this from a Galois theoretic point of view. Suppose that f is irreducible. If M is the splitting field of f over K, then $\mathrm{Gal}(M/K)$ is a transitive subgroup of S_4. Moreover, S_4 is solvable, and

$$S_4 \rhd A_4 \rhd V_4 \rhd C_2 \rhd \{1\}.$$

In fact $V \lhd S_4$ and $S_4/V \cong S_3$. This suggests that we can solve f by combining the solutions of a cubic polynomial (to give the V to S_4 part) and two quadratic polynomials (to give the $\{1\}$ to C_2 to V_4 part).

Assume that K contains enough roots of unity (we need 12^{th} roots). If not, we can just add these roots to K as before. Then we can find subfields

$$K \subset M^{V_4} \subset M^{V_2} \subset M,$$

where each extension is obtained by adding an n^{th} root. Our goal is to find these generators. Note that these extensions may be trivial, depending on the Galois group of f.

Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ be the roots of f. As before, $\mathrm{Gal}(f/K)$ acts on the roots of f. In order to find M^{V_4}, we should look for elements of M that are fixed by $(12)(34), (13)(24), (14)(23) \in V_4$. Consider the elements

$$\begin{aligned}
\beta &= \alpha_1 + \alpha_2 = -\alpha_3 - \alpha_4 \\
\gamma &= \alpha_1 + \alpha_3 = -\alpha_2 - \alpha_4 \\
\delta &= \alpha_1 + \alpha_4 = -\alpha_2 - \alpha_3
\end{aligned}$$

As before, we can recover the α_i from β, γ, δ. For example,

$$\alpha_1 = \frac{1}{2}(\beta + \gamma + \delta).$$

In addition, for each $\varphi \in V_4$ we have $\varphi(\beta) = \pm\beta$, $\varphi(\gamma) = \pm\gamma$ and $\varphi(\delta) = \pm\delta$. Hence, $\beta^2, \gamma^2, \delta^2 \in M^{V_4}$. We can show computationally that $\beta^2, \gamma^2, \delta^2$ solve a cubic equation over K.

Hence, we can start by solving this cubic, to find the extension $K_1 = M^{V_4} = K(\beta^2, \gamma^2, \delta^2)$. In general this requires an extension of degree 6, and $\mathrm{Gal}(K_1/K) \cong S_3$. Having done this, we choose a square root β of β^2 and a square root γ of γ^2. So the field $M = K(\beta, \gamma, \delta)$, in which all the roots α_i lie, is obtained from M by adjoining two further square roots. The group $\mathrm{Gal}(M/K_1)$ is in general isomorphic to V_4. This fits in with the series

$$1 \lhd C_2 \lhd V_4 \lhd A_4 \lhd S_4;$$

solving the cubic corresponds to the group $S_4/V_4 \cong S_3$, and then the two further square roots corresponds to the group $V_4 = C_2 \times C_2$.

Insolubility of the general quintic

From the patterns emerging above, one might guess that the Galois group for the general quintic should be isomorphic to S_5, and therefore not be a soluble group. By the above, this would imply that the general quintic has no solution in terms of radicals. In fact, it is not too hard to show that the general polynomial of degree n has Galois group S_n. Here, however, we will give an explicit example of a polynomial not soluble by radicals.

We first use a group theoretical lemma.

Lemma 9.4 Let p be a prime number. Let G be a subgroup of S_p which is transitive and contains a transposition. Then $G = S_p$.

PROOF. Let $S = \{1, \ldots, p\}$, and define a relation $\sim$ on S by $i \sim j$ if and only if $i = j$ or $(i\ j) \in G$. $\sim$ is clearly reflexive and symmetric. Further, if $i \sim j$ and $j \sim k$, then either $i = j$, $i = k$ or $j = k$ (in which case it is easy to see that $i \sim k$) or $(i\ k) = (i\ j)(j\ k)(i\ j) \in G$. So $\sim$ is an equivalence relation.

If $a \in S$, denote its equivalence class by $\overline{a}$. Let $b \in S$. As G is transitive, there exists $\theta \in G$ with $\theta(a) = b$.

Let $c \in \overline{a}$. Either $c = a$ or $(a\ c) \in G$. Consider $\theta(c)$. Either $\theta(c) = \theta(a)$ or $(\theta(a)\ \theta(c)) = \theta(a\ c)\theta^{-1} \in G$.

In either case, $\theta(c) \sim b$. It follows that θ gives a bijection from the equivalence class of a to the equivalence class of b. So $|\overline{a}| = |\overline{b}|$. But S is partitioned into equivalence classes, and $|S| = p$, so either all classes have 1 element each, or there is only one class with p elements. The first case is ruled out because G contains a transposition. Thus all transpositions $(i\ j)$ lie in G. But S_p is generated by the transpositions. ⊠

Example 9.5 Let $f(x) = x^5 - 6x + 3 \in \mathbb{Q}[x]$. Then $f(x) = 0$ is not soluble by radicals over $\mathbb{Q}$. ⊠

PROOF. Note that $f'(x) = 5x^4 - 6$ and so has two real zeros. By Rolle's theorem, between any two real roots of f, there is a real root of f'. Thus f has at most three real zeros.

$f(-2) = -17$, $f(-1) = 8$, $f(1) = -2$ and $f(2) = 23$, so f has exactly three real roots.

Let $G = \mathrm{Gal}(f/\mathbb{Q})$. f is irreducible by Eisenstein ($p = 3$), so G acts transitively on the roots of f (by Proposition 9.2). Also, complex conjugation fixes the three real roots amd interchanges the other two, so G contains a transposition. By the lemma, $G = S_5$. Thus f is not soluble in radicals. ⊠

Note that the same argument shows the following: suppose $f(x) \in \mathbb{Q}[x]$ is a polynomial such that

- $\deg f = p$, a prime at least 5,
- f is irreducible over $\mathbb{Q}$,
- f has $p - 2$ real roots, and one pair of complex conjugate roots.

Then f is not soluble by radicals over $\mathbb{Q}$.

For this, the second and third hypotheses show that $\mathrm{Gal}(f/\mathbb{Q})$ is a transitive subgroup of S_p which contains a transposition. Given that p is prime, the lemma now implies that $\mathrm{Gal}(f/\mathbb{Q}) = S_p$. As $p \geq 5$, we know that S_p is not a soluble group, and we conclude that f is not soluble by radicals.

(Note that it is important that p be prime – the polynomial $x^4 - 2$ is irreducible over $\mathbb{Q}$, and has two real roots and one pair of complex conjugate roots, but its Galois group is D_4, not S_4.)