5.3 Solvability by Radicals

04/23/20

We are interested in studying polynomials whose roots can be expressed in terms of radicals over the ground field K. Such is the case for any polynomial of degree 2, using the quadratic equation (provided $\text{char}(K) \neq 2$). Similarly, there is a cubic radical formula for any polynomial of degree 3, in characteristic $\neq 2, 3$. Roots of polynomials of degree 4 can be found using the cubic formula.

We are going to need a result on linear independence of characters.

Definition 5.6 A *linear character* of a group G with values in a field K is a group homomorphism $\chi : G \to K^\times$ from G to the multiplicative group of K.

Theorem 5.18 *Let G be a group and K a field. The set $\text{Hom}(G, K^\times)$, as a subset of the vector space K^G, is linearly independent. In other words, any family $(\chi_i | i \in I)$ of distinct characters of G with values in K is linearly independent over K.*

Proof. Suppose otherwise, and let $\chi_1, \ldots, \chi_m$ be a minimal dependent set with dependence relation

$$a_1\chi_1 + \cdots + a_m\chi_m = 0.$$

By minimality, we must have $a_i \neq 0$ for $i = 1, \ldots, m$. For any $g \in G$ we have

$$a_1\chi_1(g) + \cdots + a_m\chi_m(g) = 0 \tag{5.2}$$

and since each $\chi_i(g) \neq 0$ we must also have $m > 1$. Let $g_0 \in G$ be such that $\chi_1(g_0) \neq \chi_2(g_0)$. Then

$$a_1\chi_1(g_0g) + \cdots + a_m\chi_m(g_0g) = 0$$

which yields

$$a_1\chi_1(g_0)\chi_1(g) + \cdots + a_m\chi_m(g_0)\chi_m(g) = 0 \tag{5.3}$$

Multiplying (5.2) by $\chi_1(g_0)$ and subtracting from (5.3) yields a dependence relation on $\chi_2, \ldots, \chi_m$ with the coefficient of χ_2 equal to $a_2(\chi_2(g_0) - \chi_1(g_0)) \neq 0$, contradicting the minimality of $\chi_1, \ldots, \chi_m$. ∎

Corollary 5.19 *Let K and L be fields. The set* $\mathrm{Hom}(K, L)$ *of all homomorphisms from K to L, is linearly independent over L. In particular* $\mathrm{Aut}(K)$ *is linearly independent over K.*

Exercise 5.3.1 Prove Corollary 5.19.

5.3.1 Radical Extensions

Definition 5.7 An extension $K(\sqrt[n]{a})/K$ with $a \in K$ and $n \geq 1$, is called a *radical extension*. Note that the expression $\sqrt[n]{a}$ is ambiguous, as the polynomial $x^n - a$ may have several distinct roots. However, when K contains n-th roots of unity, the expression $K(\sqrt[n]{a})$ is unambiguous, as it contains all the roots of $x^n - a$, and is generated by any one of them.
A field tower $K = K_0 \leq K_1 \leq \cdots \leq K_l$ with each K_i/K_{i-1} a radical extension is called a *radical tower*. We say that K_l/K is a *root extension* and that the elements of K_l can be *expressed by radicals* over K. We say that a polynomial $f(x) \in K[x]$ is *solvable by radicals*, if all its roots can be expressed by radicals over K.

Definition 5.8 A Galois extension F/K usually adopts as part of its name, properties of the Galois group $\mathrm{Gal}(F/K)$. Thus, a *cyclic extension* is a Galois extension whose Galois group is cyclic. Similarly, an *abelian extension* is a Galois extension whose Galois group is abelian.

The following proposition can be stated, as: *an extension F/K is a radical extension iff it is a cyclic extension.* This is not quite correct, without some extra assumptions. More precisely,

Proposition 5.20 *Let $n \in \mathbb{N}$ and K a field such that* $\mathrm{char}K \not| n$ *and it contains n-th roots of unity.*

1. *For $a \in K$, let $F = K(\sqrt[n]{a})$. The extension F/K is cyclic of degree d, a divisor of n.*

2. *Conversely, if F/K is cyclic of degree n, then $F = K(\sqrt[n]{a})$ for some $a \in K$.*

The case when n is a multiple of char$K$ needs a somewhat different treatment. We avoid that case here.

Proof. 1. The statement hold trivially for $a = 0$, so assume $a \neq 0$. Since K contains the n-th roots of unity, F is the splitting field of $x^n - a$ over K. Since char$K \not| n$, there are n distinct n-th roots of unity, so the polynomial $x^n - a$ has n distinct roots $\sqrt[n]{a}\,\xi^i$, $i = 0, \ldots, n-1$ where ξ is a primitive n-root of unity. Therefore $x^n - a$ is separable and F/K is Galois. Each $\sigma \in \mathrm{Gal}(F/K)$ is completely determined by $\sigma(\sqrt[n]{a})$, which must be equal to $\sqrt[n]{a}\,\xi^{i_\sigma}$. Consider the map

$$\begin{array}{rcl} \mathrm{Gal}(F/K) & \to & \mathbb{Z}_n \\ \sigma & \mapsto & i_\sigma \end{array}$$

Clearly, this map is injective, and it is easy to check that it is a homomorphism, as $\tau\sigma(\sqrt[n]{a}) = \tau(\sqrt[n]{a}\,\xi^{i_\sigma}) = \sqrt[n]{a}\,\xi^{i_\tau}\xi^{i_\sigma} = \sqrt[n]{a}\,\xi^{i_\tau + i_\sigma}$.

2. Let $\mathrm{Gal}(F/K) = \langle\sigma\rangle$ be cyclic of order n. For $\alpha \in F$ and ξ a primitive n-th root of unity, define the *Lagrange resolvent* by

$$(\alpha, \xi) := \alpha + \xi\sigma(\alpha) + \xi^2\sigma^2(\alpha) + \cdots + \xi^{n-1}\sigma^{n-1}(\alpha). \qquad (5.4)$$

By Corollary 5.19, $1, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ are linearly independent over F, so, we have

$$1 + \xi\sigma + \xi^2\sigma^2 + \cdots + \xi^{n-1}\sigma^{n-1} \neq 0,$$

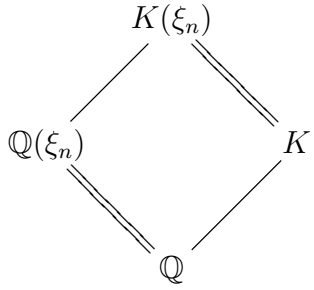
so there is $\alpha \in F$ such that $(\alpha, \xi) \neq 0$. Let $\rho := (\alpha, \xi)$. Since $\xi \in K$ we have $\sigma(\rho) = \xi^{-1}\rho$, and $\sigma(\rho^n) = \xi^{-n}\rho^n = \rho^n$, so $\rho^n \in F_{\langle\sigma\rangle} = K$. Moreover, for any $0 < i < n$, $\sigma^i(\rho) = \xi^{-i}\rho \neq \rho$, so $\sigma^i \notin \mathrm{Aut}_{K(\rho)}F$, i.e. $\mathrm{Aut}_{K(\rho)}F = \{1\} = \mathrm{Aut}_F F$,

$$\begin{array}{c} F \\ | \\ K(\rho) \\ | \\ K \end{array}$$

so $F = K(\rho) = K(\sqrt[n]{a})$, where $a = \rho^n \in K$. ∎

Proposition 5.21 *Let K be a field of characteristic 0, and ξ_n a primitive n-th root of unity. $K(\xi_n)/K$ is Galois with Galois group contained in U_n, hence Abelian.*

Proof. Follows at once from Corollary 4.16 and Proposition 4.32 by considering the following diagram:



■

Lemma 5.22 *Let K be a field of characteristic 0.*

1. *If F and E are radical extensions of K then so are FE/F and FE/E, so that $K \leq F \leq FE$ and $K \leq E \leq FE$ are radical towers.*
2. *If F and E are root extensions of K then so is FE.*
3. *If F is a root extension K then so is the normal closure L of F over K.*

Proof. 1. If $E = K(\sqrt[n]{a})$, then $FE = F(\sqrt[n]{a})$.

2. Follows from repeated application of Part (1).

3. A root extension F/K is a finite extension. By Exercise 5.3.2 below, its normal closure is also a finite extension, hence F/K has finitely many conjugates in $\overline{K}$, each of which is isomorphic to F/K and also a root extension. The normal closure is the composite of these finitely many root extension, so, by part (2), it is also a root extension. ■

Exercise 5.3.2 Let F/K be a finite extension, and L/K its normal closure. Show that L/K is also a finite extension. Hint: if you write $E = K(\alpha_1, \ldots, \alpha_n)$, and let $f_i(x) = \min_K(\alpha_i)$, show that L is the splitting field of the set $A = \{f_1(x), \ldots, f_n(x)\}$.

5.3.2 Solvable Groups

04/28/20 We need to recall the following definitions and facts on solvable groups from Group Theory, Section 1.1.4.

Definition 5.9 The *commutator series* or *derived series* of a group G, denoted by $(G^{(n)}|n \geq 0)$, is defined recursevely by

$$G^{(0)} := G, \quad \text{and} \quad G^{(n+1)} := \left(G^{(n)}\right)'.$$

The group G is *solvable* if there is a k such that $G^{(k)} = 1$. The smallest such k is called the *derived length* or *solvable length* of G, and is denoted $l(G)$.

The only group of solvable length zero is the trivial group. Groups of solvable length 1 are precisely the non-trivial abelian groups. It is common practice by some authors to say "*solvable of length* n" meaning "*solvable of length* $\leq n$"; that way, one would say that abelian groups are precisely the groups of solvable length 1. Solvable groups of length ≤ 2 are also called *metabelian*.

Proposition 5.23 *Let G be a group, $H \leq G$ and $N \trianglelefteq G$.*

1. *If G is solvable, then H is also solvable, and*

$$l(H) \leq l(G).$$

2. *G is solvable iff N and G/N are both solvable. In this case*

$$l(G) \leq l(N) + l(G/N).$$

Definition 5.10 A *normal series* of a group G is a series

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_{n-1} \trianglelefteq H_n = G$$

Theorem 5.24 *A group is solvable iff it has a normal series*

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_{n-1} \trianglelefteq H_n = G \tag{5.5}$$

with abelian factors, i.e. such that each H_{i+1}/H_i is Abelian.

The sequence (5.5) is called an *Abelian series* for G and n is called the length of the series.

Examples 5.3.1

1. As already mentioned, every Abelian group is solvable, of length ≤ 1, and conversely.
2. Every cyclic-by-Abelian group is metabelian, i.e. solvable of length ≤ 2. In particular the Galois group of the splitting field of $x^n - a$ over a field of characteristic zero is solvable.
3. The group A_5 is not solvable. In fact, any non-Abelian simple group is non-solvable. It can be shown that A_5 is in fact the smallest non-solvable group, i.e. any group of order less than or equal to 59 is solvable.

For finite groups we have a stronger condition for solvability.

Proposition 5.25 *A finite group G is solvable iff there is a normal series*

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_{n-1} \trianglelefteq H_n = G$$

with cyclic factors, i.e. such that each H_{i+1}/H_i is cyclic.

In other words, for finite groups, we can replace Abelian with cyclic in the definition of solvable.

Exercise 5.3.3

1. Prove Proposition 5.25.
2. Show, with a counterexample, that for infinite groups the two conditions are not be equivalent.

The class of solvable groups has been extensively studied. One can refer to Proposition 5.23 above, by saying that the class of solvable groups is closed under subgroups, quotients and extensions. In particular,

Corollary 5.26 *If G and H are solvable groups then so is their direct product $G \times H$.*

Hence, the class of solvable groups is closed under finite products.

Exercise 5.3.4

1. Prove Corollary 5.26.
2. Show that the class of solvable groups is not closed under arbitrary products.

Using the fact that A_n is non-abelian simple for $n \geq 5$, and computing the derived series of S_n for $n \leq 4$, one gets the following.

Proposition 5.27 *The group S_n is solvable iff $n \leq 4$.*

5.3.3 Solvable by Radicals

We now go back to the main result of this section, the characterization of polynomials which are solvable by radicals. 04/30/20

Theorem 5.28 *Let K be a field of characteristic 0, and $f(x) \in K[x]$. Let F be the splitting field of $f(x)$. The polynomial $f(x)$ is solvable by radicals iff* $\mathrm{Gal}(F/K)$ *is a solvable group.*

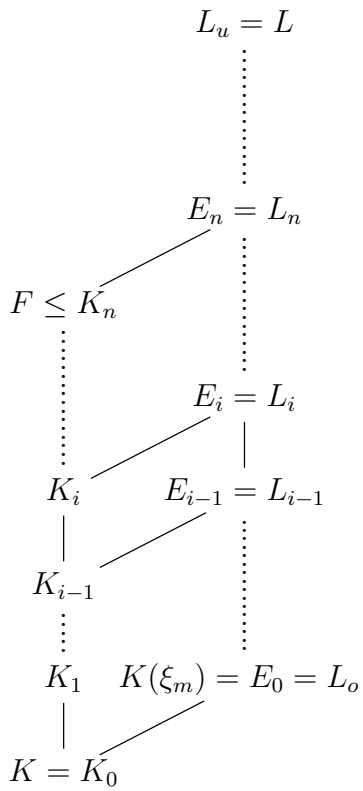
Proof. ($\Rightarrow$) Each root a of $f(x)$ is contained in a root extension, i.e. at the top of a radical tower. Taking the join of all those root extensions, yields a root extension by Lemma 5.22.2, which contains all the roots of $f(x)$. Write the radical tower for this root extension as

$$K = K_0 \leq K_1 \cdots \leq K_n$$

with $K_{i+1} = K_i(\sqrt[m_i]{a_i})$ for some $a_i \in K_i$, and we have $F \leq K_n$. Let $m = \text{l.c.m.}(m_1, \ldots, m_n)$, ξ_m a primitive m-th root of unity, $E_0 = K(\xi_m)$, and $E_{i+1} = E_i(\sqrt[m_i]{a_i})$. By Proposition 5.21, E_o/K_0 is an Abelian extension, and by Propostion 5.20, each E_{i+1}/E_i is a cyclic extension. Let L/K be the normal closure of E_n/K. L is the join of all conjugates of E_n over K, and by Lemma 5.22, L/K is a root extension, with a radical tower

$$K \leq K(\xi_m) = L_0 \leq \cdots \leq L_u = L$$

where each $L_{j+1} = L_j(\sqrt[m_j]{a_j})$ and all $m_j \mid m$, for $0 \leq j < u$. L/K is a Galois extension that contains all the roots of $f(x)$, hence $F \leq L$.



L_0/K is an Abelian extension, and each L_{j+1}/L_j is a cyclic extension. Let $G = \mathrm{Gal}(L/K)$ and $G_j = \mathrm{Gal}(L/L_j)$. We have

$$G \geq G_0 \geq G_1 \geq \cdots \geq G_u = 1,$$

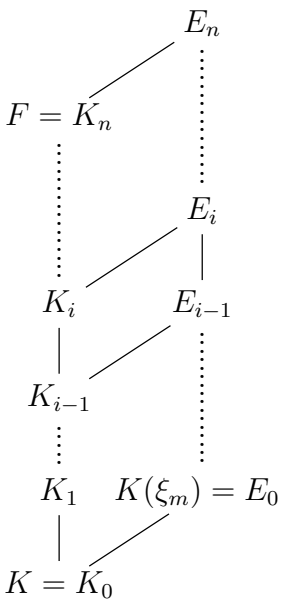
and since L_{j+1}/L_j is Galois we get $G_{j+1} \trianglelefteq G_j$ and

$$G_j/G_{j+1} = \mathrm{Gal}(L/L_j)/\mathrm{Gal}(L/L_{j+1}) \approx \mathrm{Gal}(L_{j+1}/L_j)$$

is Abelian. It follows that G is solvable. The splitting field F of $f(x)$ over K is contained in L, so

$$\mathrm{Gal}(F/K) \approx \mathrm{Gal}(L/K)/\mathrm{Gal}(L/F)$$

is also solvable.



($\Leftarrow$) Assume now that $\mathrm{Gal}(F/K)$ is solvable, with

$$1 = G_n \trianglelefteq G_{n-1} \trianglelefteq \cdots \trianglelefteq G_1 \trianglelefteq G_0 = \mathrm{Gal}(F/K)$$

and G_{i-1}/G_i cyclic of order m_i. Let $K_i = F_{G_i}$, so

$$K = K_0 \leq K_1 \leq \cdots \leq K_{n-1} \leq K_n = F$$

K_i/K_{i-1} is Galois with $\mathrm{Gal}(K_i/K_{i-1}) \approx G_i/G_{i-1}$. Let $m = \text{l.c.m.}(m_1, \ldots, m_n)$, $E_0 = K(\xi_m)$, $E_i = E_0K_i$. Then we have E_i/E_{i-1} is Galois with $\mathrm{Gal}(E_i/E_{i-1})$ isomorphic to a subgroup of $\mathrm{Gal}(K_i/K_{i-1})$, hence cyclic. Since E_0 has enough roots of unity, by Proposition 5.20 each E_i/E_{i-1} is a radical extension. Thus we have that $E = E_n$ is a root extension of K, that contains all the roots of $f(x)$, so $f(x)$ is solvable by radicals. ■

Example 5.3.2 Let E be the splitting field of $f(x) = x^5 - 20x + 6 \in \mathbb{Q}[x]$. We will try to determine the group $G = \mathrm{Gal}(E/\mathbb{Q})$. Note first that $f(x)$ is irreducible by Eisenstein's criterion with $p = 2$. By separability, it has no multiple roots. Let's name the roots $\alpha_1, \ldots, \alpha_5$. We can view G as a group of permutations of the roots $\alpha_1, \ldots, \alpha_5$, so that $G \leq S_5$. By irreducibility of $f(x)$ it follows that that $[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = 5$ and $[E : \mathbb{Q}]$ is divisible by 5. By Cauchy's Theorem, G has an element of order 5. But the only elements in S_5 of order 5 are the 5-cycles, so G contains a 5-cycle. From the first and second derivatives of $f(x)$

$$\begin{aligned} f'(x) &= 5x^4 - 20 \\ f''(x) &= 20x^3 \end{aligned}$$

we see that $f''(x)$ has a single real root, so by the Mean Value Theorem $f'(x)$ has at most two real roots, and $f(x)$ has at most three real roots. The table of values

x	-3	0	1	3
$f(x)$	-177	6	-13	189

and the Intermediate Value Theorem, tell us that $f(x)$ has three real roots. Therefore of the five roots of $f(x)$, three of them $\alpha_1, \alpha_2, \alpha_3$ are real, and the other two are non-real, complex conjugate of each other $\overline{\alpha_4} = \alpha_5$. Complex conjugation in $\mathbb{C}$ is a field automorphism, and its restriction to E yields an automorphism of E that, as a permutation of the roots of $f(x)$, is the transposition $(4\ 5)$. It follows from Exercise 5.3.5 below that $\mathrm{Gal}(E/\mathbb{Q}) = S_5$, and $[E : \mathbb{Q}] = 120$. Since S_5 is not solvable, it follows by Theorem 5.28 that the polynomial $f(x) = x^5 - 20x + 6 \in \mathbb{Q}[x]$ is not solvable by radicals.

Exercise 5.3.5 Let p be prime, and $G \leq S_p$. Show that if G contains a p-cycle and a transposition, the $G = S_p$.

We can now use Proposition 5.27, Example 5.3.2, and Theorem 5.28, to prove the following Theorem, due to Abel [1] in 1824.

Theorem 5.29 [Abel] *The general equation of degree n is not solvable by radicals for any $n \geq 5$.*

Proof. Since the Galois group of the polynomial $f(x) = x^5 - 20x + 6$ is S_5, then by Proposition 5.27, and Theorem 5.28, the roots of this polynomial cannot be expressed by radicals. Hence there is no formula to solve the general equation of degree 5 by radicals. For $n > 5$ the existence of a solution by radicals of the general polynomial of degree n yields a solution by radicals of the equation $f(x) \cdot x^{n-5} = 0$, contradicting the above. ■