Solvability by radicals

Rodney Coleman, Laurent Zwald

Solvability by radicals

Rodney Coleman, Laurent Zwald

December 10, 2020

Abstract

In this note we present one of the fundamental theorems of algebra, namely Galois's theorem concerning the solution of polynomial equations. We will begin with a study of cyclic extensions, before moving onto radical extensions.

1 Cyclic extensions

We say that a finite extension E of a field F is cyclic if the Galois group $Gal(E/F)$ is cyclic. In this section we aim to present some elementary properties of such extensions. We begin with a preliminary result known as *Hilbert's theorem 90*.

EXTSOLVcycth1

Theorem 1 *Let E/F be a finite cyclic Galois extension of degree n. We suppose that σ is a generator of the Galois group $Gal(E/F)$. If $\alpha \in E$, then $N_{E/F}(\alpha) = 1$ if and only if there exists $\beta \in E^*$ such that $\alpha = \frac{\beta}{\sigma(\beta)}$.*

PROOF If $\alpha = \frac{\beta}{\sigma(\beta)}$, then

$$N_{E/F}(\alpha) = \alpha\sigma(\alpha)\cdots\sigma^{n-1}(\alpha) = \frac{\beta\sigma(\beta)\sigma^2(\beta)\cdots\sigma^{n-1}(\beta)}{\sigma(\beta)\sigma^2(\beta)\cdots\sigma^{n-1}(\beta)\sigma^n(\beta)} = 1,$$

because $\sigma^n(\beta) = \beta$.

Now suppose that $N_{E/F}(\alpha) = 1$, i.e., $\alpha\sigma(\alpha)\cdots\sigma^{n-1}(\alpha) = 1$. We define a finite sequence $(\delta_i)_{i=0}^{n-1}$ as follows:

$$\delta_0 = \alpha, \delta_1 = \alpha\sigma(\alpha), \delta_2 = \alpha\sigma(\alpha)\sigma^2(\alpha), \ldots, \delta_{n-1} = \alpha\sigma(\alpha)\cdots\sigma^{n-1}(\alpha) = N_{E/F}(\alpha) = 1.$$

From Result REDUCdedcor1 the characters $1, \sigma, \ldots, \sigma^{n-1}$ form an independant set and so there exists $\gamma \in E$ such that

$$\delta_0\gamma + \delta_1\sigma(\gamma) + \cdots + \delta_{n-2}\sigma^{n-2}(\gamma) + \sigma^{n-1}(\gamma) \neq 0.$$

We note this sum β. Then

$$\begin{aligned}\sigma(\beta) &= \sigma(\delta_0)\sigma(\gamma) + \sigma(\delta_1)\sigma^2(\gamma) + \cdots + \sigma(\delta_{n-2})\sigma^{n-1}(\gamma) + \sigma^n(\gamma)\\ &= \alpha^{-1}\left(\delta_1\sigma(\gamma) + \delta_2\sigma^2(\gamma) + \cdots + \delta_{n-1}\sigma^{n-1}(\gamma)\right) + \sigma^n(\gamma),\end{aligned}$$

because $\alpha^{-1}\delta_i = \sigma(\delta_{i-1})$. As $\sigma^n = \mathrm{id}_E$, we have

$$\sigma^n(\gamma) = \gamma = \alpha^{-1}\delta_0\gamma,$$

hence $\sigma(\beta) = \alpha^{-1}\beta$. □

The theorem which we have just proved is often refered to as the 'multiplicative' version of Hilbert's theorem 90 to distinguish from the 'additive' version, which we will now present.

EXTSOLVcycth2

Theorem 2 *If E/F is a finite cyclic Galois extension of degree n, then $T_{E/F}(\alpha) = 0$ if and only if there exists $\beta \in E$ such that $\alpha = \beta - \sigma(\beta)$.*

PROOF Let σ be a generator of the Galois group $G = Gal(E/F)$, so that $\sigma^n = \mathrm{id}_n$.

If $\alpha = \beta - \sigma(\beta)$, then

$$T_{E/F}(\alpha) = \sum_{k=0}^{n-1} \sigma^k(\alpha) = \sum_{k=0}^{n-1} \sigma^k(\beta) - \sum_{k=1}^{n} \sigma^k(\beta) = 0,$$

because $\sigma^n(\beta) = \beta$.

Conversely, suppose that $T_{E/F}(\alpha) = 0$. As $T_{E/F} \neq 0$, we may find an element x such that $T_{E/F}(x) \neq 0$. Let

$$w = \alpha\sigma(x) + (\alpha + \sigma(\alpha))\,\sigma^2(x) + \cdots + \left(\alpha + \sigma(\alpha) + \cdots + \sigma^{n-2}(\alpha)\right)\sigma^{n-1}(x).$$

Then

$$\sigma(w) = \sigma(\alpha)\sigma^2(x) + \left(\sigma(\alpha) + \sigma^2(\alpha)\right)\sigma^3(x) + \cdots + \left(\sigma(\alpha) + \sigma^2(\alpha) + \cdots + \sigma^{n-1}(\alpha)\right)\sigma^n(x).$$

Since $T_{E/F}(\alpha) = 0$, we have

$$-\alpha = \sigma(\alpha) + \cdots + \sigma^{n-1}(\alpha),$$

so the last summand in the expression for $\sigma(w)$ is $-\alpha x$, hence

$$w - \sigma(w) = \alpha\left(x + \sigma(x) + \sigma^2(x) + \cdots + \sigma^{n-1}(x)\right) = \alpha T_{E/F}(x).$$

Setting $\beta = \frac{w}{T_{E/F(x)}}$, we obtain

$$\beta - \sigma(\beta) = \frac{w}{T_{E/F}(x)} - \frac{\sigma(w)}{\sigma(T_{E/F}(x))} = \frac{w - \sigma(w)}{T_{E/F}(x)},$$

because $T_{E/F}(x) \in F$. Therefore

$$\beta - \sigma(\beta) = \frac{\alpha T_{E/F}(x)}{T_{E/F}(x)} = \alpha,$$

as required. □

In the following we consider extensions E/F of a particular sort, namely where the field F contains a primitive nth root of unity, for some positive integer n.

EXTSOLVcycth3

Theorem 3 *Let E/F be a cyclic Galois extension of degree n, where F contains a primitive nth root of unity ζ. Then there exists an irreducible polynomial $f(X) = -\alpha + X^n \in F[X]$ such that E is a splitting field of f.*

PROOF Let σ be a generator of the Galois group $Gal(E/F)$. Since $\zeta \in F$, we have $N_{E/F}(\zeta) = \zeta^n = 1$ and so, by Hilbert's theorem 90 (multiplicative version), there is an element $\beta \in E^*$ such that $\zeta = \frac{\beta}{\sigma(\beta)}$. Then

$$\begin{aligned}
\sigma(\beta) &= \zeta^{-1}\beta \\
\sigma^2(\beta) &= \sigma(\zeta)^{-1}\sigma(\beta) = \zeta^{-1}(\zeta^{-1}\beta) = \zeta^{-2}\beta \\
\sigma^3(\beta) &= \sigma(\zeta)^{-2}\sigma(\beta) = \zeta^{-2}(\zeta^{-1}\beta) = \zeta^{-3}\beta
\end{aligned}$$

and generally $\sigma^m(\beta) = \zeta^{-m}\beta$, for all $m \in \mathbf{N}^*$. As the elements $\sigma^i(\beta)$, for $0 \leq m < n$ are distinct, the automomorphisms $\mathrm{id}_{|F(\beta)}, \sigma_{|F(\beta)}, \ldots, \sigma^{n-1}_{|F(\beta)}$ form a set of n distinct elements of the Galois group $Gal(F(\beta)/F)$. Then $[F(\beta) : F] \geq n$ and

$$n = |Gal(E/F)| = [E : F] = [E : F(\beta)][F(\beta) : F] \Longrightarrow [F(\beta) : F] \leq n.$$

Therefore $[F(\beta) : F] = n$, which implies that $E = F(\beta)$.

We claim that $\beta^n \in F$. Now

$$\sigma(\beta^n) = \sigma(\beta)^n = \zeta^{-n}\beta^n = \beta^n,$$

and it follows that β^n belongs to the fixed field of $Gal(E/F)$, i.e., F. Thus there exists $\alpha \in F$ such that $\beta^n = \alpha$. We have shown that $E = F(\beta)$, where β is a root of the polynomial $f(X) = -\alpha + X^n$. The roots of f have the form $\zeta^i\beta$, for $0 \leq i < n$ and $\zeta \in F$ by hypothesis, so E contains all the roots of f and hence is a splitting field of the polynomial f. Since $[F(\beta) : F] = n$, the degree of the minimal polynomial $m(\beta, F)$ is n, hence $f = m(\beta, F)$; it follows that f is irreducible. □

The theorem which we have just proved has a converse.

EXTSOLVcycth4

Theorem 4 *Let F be a field containing an nth primitive root of unity ζ and E a splitting field of the polynomial $f(X) = -\alpha + X^n \in F[X]$, with $\alpha \neq 0$. Then $E = F(\beta)$, where β is a root of f, and the Galois group $G = Gal(E/F)$ is cyclic of order dividing n. The order of G is equal to n if and only if f is irreducible.*

PROOF If β is root of f, then the roots of f have the form $\zeta^i\beta$, for $0 \leq i < n$. As $\zeta \in F$, all the roots of f lie in $F(\beta)$, so $F(\beta)$ is a splitting field of f and so $E = f(\beta)$.

Let $\sigma \in G = Gal(E/F)$. As σ permutes the roots of f, we may write $\sigma(\beta) = \zeta^{k(\sigma)}\beta$, where $k(\sigma)$ is uniquely determined modulo n. We thus obtain a mapping

$$\phi : G \longrightarrow (\mathbf{Z}_n, +), \sigma \longmapsto [k(\sigma)],$$

which is clearly a group homomorphism. If $\phi(\sigma) = [0]$, then $\sigma(\beta) = \beta$, which implies that σ is the identity on $F(\beta)$ and so ϕ is a monomorphism. Since G is isomorphic to a subgroup of the cyclic group $(\mathbf{Z}_n, +)$, G is cyclic of order dividing n.

If f is irreducible, then G acts transitively on the roots of f (Result 4). Thus there exists $\sigma \in G$ such that $\sigma(\beta) = \zeta^i\beta$, for $0 \leq i < n$. It follows that ϕ is surjective, so G is isomorphic to $(\mathbf{Z}_n, +)$.

Now suppose that f is reducible. As f has no multiple roots, f has two distinct irreducible factors, so G does not act transitively on the roots of f (Result 5). Thus there exist roots $\zeta^i\beta$ and $\zeta^j\beta$, with $j > i$, for which there exists no element $\sigma \in G$ such that $\sigma(\zeta^i\beta) = \zeta^j\beta$, i.e., $\sigma(\beta) = \zeta^{j-i}\beta$. It follows that ϕ is not surjective and so $|G| < n$. □

Corollary 1 *Let p be prime, F a field containing a primitive pth root of unity and E a splitting field of the polynomial $f(X) = -\alpha + X^p \in F[X]$, with $\alpha \neq 0$. Then either f is irreducible and $Gal(E/F) \simeq \mathbf{Z}_p$ or f splits in F and $GalE/F) = \{\mathrm{id}_F\}$.*

PROOF The order of $Gal(E/F) = p$ or 1. In the first case, from Theorem 4, f is irreducible and $Gal(E/F) \simeq \mathbf{Z}_p$, because $Gal(E/F)$ is cyclic. Suppose now that the order of $Gal(E/F)$ is 1. Then $[E : F] = 1$. There exists $\beta \in E$ such that $E = F(\beta)$, so $[F(\beta) : F] = 1$, which implies that $\beta \in F$. It now follows that f splits in F. □

2 Radical extensions

Suppose that E/F is a field extension such that $E = F(\alpha)$ for some $\alpha \in E$. If there exists $n \in \mathbf{N}^*$ such that $\alpha^n \in F$, then we say that E is a *pure extension* of type n. In this case α is a root of a polynomial of the form $f(X) = -c + X^n \in F[X]$. A chain of extensions

$$F = F_0 \subset F_1 \subset \cdots \subset F_r = E,$$

where each extension F_{i+1}/F_i is a pure extension is called a *radical chain* and we say that E/F is a *radical extension*. Using Result 2 and Result 3, we see that a radical extension is a finite algebraic extension.

EXTSOLVradprop1

Proposition 1

- **a.** *If E/F is a radical extension and Z an intermediate field, then E/Z is a radical extension.*
- **b.** *If E/F is a field extension and Z_1, Z_2 intermediate fields such that Z_1/F, Z_2/F are radical extensions, then Z_1Z_2/F is a radical extension.*

PROOF **a.** We have the radical chain

$$F \subset F(\alpha_1) \subset F(\alpha_1, \alpha_2) \subset \cdots \subset F(\alpha_1, \cdots, \alpha_r) = E,$$

with $\alpha_i^{n_i} \in F(\alpha_1, \cdots, \alpha_{i-1})$, for some $n_i \in \mathbf{N}^*$. Then

$$Z \subset Z(\alpha_1) \subset Z(\alpha_1, \alpha_2) \subset \cdots \subset Z(\alpha_1, \ldots, \alpha_r) = E$$

and

$$\alpha_i^{n_i} \in F(\alpha_1, \cdots, \alpha_{i-1}) \subset Z(\alpha_1, \cdots, \alpha_{i-1}).$$

It follows that E/Z is a radical extension.

b. We have the radical extensions

$$F \subset F(\alpha_1) \subset F(\alpha_1, \alpha_2) \subset \cdots \subset F(\alpha_1, \cdots, \alpha_r) = Z_1$$

and

$$F \subset F(\beta_1) \subset F(\beta_1, \beta_2) \subset \cdots \subset F(\beta_1, \cdots, \beta_s) = Z_2.$$

Then

$$F \subset F(\alpha_1) \subset \cdots \subset F(\alpha_1, \cdots, \alpha_r) \subset F(\alpha_1, \cdots, \alpha_r, \beta_1) \subset F(\alpha_1, \cdots, \alpha_r, \beta_1, \ldots, \beta_s) = Z_1Z_2.$$

The only possible difficulty in seeing that we have a radical chain is in finding a power of β_1 in $F(\alpha_1, \cdots, \alpha_r)$. However, there exists $m_1 \in \mathbf{N}^*$ such that $\beta_1^{m_1} \in F \subset F(\alpha_1, \ldots, \alpha_r)$, so we indeed have a radical chain. □

Remark We may easily extend **b.** to any finite number of intermediate fields.

We now consider the normal closure of a radical extension.

EXTSOLVradprop2

Proposition 2 *If E/F is a radical extension and N the normal closure of E over F, then N/F is a radical extension.*

PROOF From Result GALGRPnormclosth1 12 the normal closure of E over F can be written as a compositum of fields $Z_1, \ldots, Z_r$ isomorphic to E contained in a field extension of F. As E is a radical extension of F, so are the Z_i. From the remark after Proposition EXTSOLVradprop1 1 the normal closure of E over F is a radical extension of F. □

We may insert fields into a radical chain so that each extension F_{i+1}/F_i is pure of type p_i, for some prime number p_i. Let us see why this is the case. Suppose that L/K is a pure extension of type n and $L = K(\alpha)$, where $\alpha \in L$ and $\alpha^n \in K$. If $n = p_1 \cdots p_s$ is the prime factorization of n, then

$$K \subset K(\alpha^{p_1 \cdots p_{s-1}}) \subset \cdots \subset K(\alpha^{p_1 p_2}) \subset K(\alpha^{p_1}) \subset K(\alpha) = L.$$

Then we have $\alpha^{p_1} \in K(\alpha^{p_1})$, $(\alpha^{p_1})^{p_2} \in K(\alpha^{p_1 p_2})$, and so on. This proves our claim. In this case we say that the radical extension is of prime type.

3 Solvability by radicals

Let F be a field and f a polynomial over F. We say that f is *solvable by radicals* if its splitting field L is contained in a radical extension E of F. In this section we aim first to show that under certain conditions solvability by radicals implies the solvability of the Galois group. (In an appendix we revise the notion of a solvable group.) Later we will prove the converse.

For certain results we need the presence of a primitive root of unity. We might be tempted to think that, for a given $n \in \mathbf{N}^*$, if a field does not contain a primitive nth root of unity, then we can simply add this root. However, this is not the case. Suppose that the field F has characteristic $p \neq 0$ and $p|n$, say $n = pm$. Let ζ be a primitive nth root of unity, then

$$0 = \zeta^n - 1 = (\zeta^m - 1)^p,$$

so $\zeta^m - 1 = 0$. This implies that the order of ζ is strictly less than n, a contradiction. So there is no primitive nth root of unity.

On the other hand, if the characteristic of F does not divide n, this problem does not occur. If $f(X) = -1 + X^n$, then

$$f'(X) = nX^{n-1} \neq 0 \Longrightarrow \gcd(f, f') = 1,$$

so f has no multiple roots (f is strongly separable). Therefore there are n distinct nth roots of unity. As the group of nth roots of unity is cyclic, it has a generator, namely a primitive nth root of unity. To be certain that we can find primitive nth roots of unity, we may suppoe that the characteristic of a field is 0. This also ensures that all extensions are separable.

Our next step is to establish a preliminary result, which will play an important role in the following. To do this we need a lemma.

EXTSOLVsolvlem1 **Lemma 1** *Let $F \subset K \subset E$ be a chain of fields, with K the splitting field of a polynomial $f \in F[X]$. If $\sigma \in Gal(E/F)$, then $\sigma_{|_K} \in Gal(K/F)$.*

PROOF It is sufficient to show that $\sigma(K) = K$. If $\alpha_1, \ldots, \alpha_n$ are the distinct roots of f, then $K = F(\alpha_1, \ldots, \alpha_n)$. For each α_i, the element $\sigma(\alpha_i)$ is a root of f, so

$$\sigma(K) = \sigma(F(\alpha_1, \ldots, \alpha_n)) = F(\sigma(\alpha_1), \ldots, \sigma(\alpha_n)) = K,$$

as required. □

EXTSOLVsolvth1

Theorem 5 *Let $F \subset K \subset E$ be a chain of fields, with K the splitting field of a polynomial $f \in F[X]$ and E the splitting field of a polynomial $g \in F[X]$. Then $Gal(E/K)$ is a normal subgroup of $Gal(E/F)$ and*

$$Gal(E/F)/Gal(E/K) \simeq Gal(K/F).$$

PROOF We define a mapping $\phi : Gal(E/F) \longrightarrow Gal(K/F)$ by $\phi(\sigma) = \sigma_{|_K}$. (From Lemma EXTSOLVsolvlem1 1 we know that $\sigma_{|_K} \in Gal(K/F)$.) Clearly ϕ is a homomorphism. As $\phi(\sigma) = \mathrm{id}_K$ if and only if σ fixes all the elements of K, the kernel of ϕ is the Galois group $Gal(E/K)$. Therefore $Gal(E/K)$ is a normal subgroup of $Gal(E/F)$.

We claim that ϕ is surjective. Let $\tau \in Gal(K/F)$. As $F \subset K$, the polynomial f belongs to $K[X]$. Using Result thSPLIT2 7, with $K' = K$ and $f^* = f$, we obtain an automorphism $\tilde{\tau}$ of E extending τ. Thus $\phi(\tilde{\tau}) = \tau$. It follows that ϕ is surjective and

$$Gal(E/F)/Gal(E/K) \simeq Gal(K/F),$$

by the first isomorphism theorem. □

We now consider polynomials which are solvable by radicals. Let F be a field and $f \in F[X]$ solvable by radicals. We will suppose that the characteristic of F is 0. The reason for doing so is twofold: 1. Extensions of F are separable; 2. Roots of unity of any order may be found in some extension. By hypothesis there is a radical chain

$$F = F_0 \subset F_1 \subset \cdots \subset F_r = E$$

such that the splitting field L of f is included in E. From Proposition EXTSOLVradprop2 2 we may suppose that E is a Galois extension of F, hence the splitting field of a polynomial $g \in F[X]$. We have also seen at the end of the previous section that we may suppose that each extension F_{i+1}/F_i may be taken to be pure of prime type, for some prime p_i. In the next proposition we will suppose that the field F contains a primitive p_ith root of unity, for all the primes p_i. This is not in general the case. However, we will show further on that we may replace the radical chain by another for which this is the case.

EXTSOLVprop1

Proposition 3 *If F contains a primitive p_ith root of unity for all i, then the Galois group of f is solvable.*

PROOF We set

$$G_i = Gal(F_r/F_i),$$

for $i = 0, \ldots, r$. We consider $[F_i : F_{i-1}]$. As α_i is a root of the polynomial $f_i(X) = -\alpha_i^{p_i} + X^{p_i} \in F_{i-1}[X]$, the degree of the minimal polynomial $m(\alpha_i, F_{i-1})$ must be 1 or p_i. We can exclude the first case, because this would imply that $F_i = F_{i-1}$. Now

$$[F_{i-1}(\alpha_i) : F_{i-1}] = \deg m(\alpha_i, F_{i-1}) \Longrightarrow [F_{i-1}(\alpha_i) : F_{i-1}] = p_i.$$

As F_i is a Galois extension of F_{i-1}, we have $|Gal(F_i/F_{i-1})| = p_i$ and so the extension F_i/F_{i-1} is cyclic of degree p_i. We may apply Theorem EXTSOLVcycth3 3: As $F \subset F_{i-1}$, F_{i-1} contains a p_ith primitive root of unity and it follows that F_i is the splitting field of a polynomial f_i over F_{i-1}. (Thus F_i is a Galois extension of F_{i-1}.)

We now consider the sequence

$$G_0 \supset G_1 \supset \cdots \supset G_r = \{\mathrm{id}\}.$$

We claim this sequence is normal, i.e., $G_{i-1} \rhd G_i$, for all i. We have $F_{i-1} \subset F_i \subset F_r$. Since F_r is a normal extension of F, F_r is the splitting field of a polynomial $g \in F[X]$. Given that $F \subset F_r$, we have $g \in F_{i-1}[X]$ and we may apply Theorem 5, which ensures us that $G_{i-1} \rhd G_i$. Hence the sequence is normal. From Theorem 5 again, the quotient group G_{i-1}/G_i is isomorphic to $Gal(F_i/F_{i-1})$, which is cyclic. We have shown that the Galois group $Gal(F_r/F_0)$ is a solvable.

To conclude we consider the chain of fields

$$F \subset L \subset F_r,$$

where L is the splitting field of f. Using Theorem 5 again, we obtain the isomomorphism

$$Gal(L/F) \simeq Gal(F_r/F)/Gal(F_r/L).$$

As $Gal(L/F)$ is isomorphic to a quotient of a solvable group, $Gal(L/F)$ is itself solvable. □

We now eliminate the hypothesis concerning the existence of p_ith primitive roots of unity in the field F. Our aim is to replace the initial radical chain by another satisfying the conditions of Proposition 3.

EXTSOLVsolvth1a

Theorem 6 *Let F be a field of characteristic 0 and $f \in F[X]$ solvable by radicals. If L is a splitting field of f, then $Gal(L/F)$ is a solvable group.*

PROOF By hypothesis there is a radical chain

$$F = F_0 \subset F_1 \subset \cdots \subset F_r = E,$$

with $L \subset F_r$. We may assume that F_r is the splitting field of some polynomial $g \in F[X]$ and that F_i/F_{i-1} is a pure extension of prime type p_i. In addition, each extension F_i/F_{i-1} is a Galois extension of degree p_i, because $F \subset F_{i-1}$ implies that $g \in F_{i-1}[X]$.

Let m be the lcm of the p_i and ζ an mth primitive root of unity. We construct a new chain by adding ζ to each element of our first chain:

$$F = F_0 \subset F_0(\zeta) \subset F_1(\zeta) \subset \cdots \subset F_r(\zeta).$$

We notice that $F_0(\zeta)$ contains all the p_ith primitive roots of unity. For example, if $m = p_1 \cdots p_s$, then $\zeta^{p_2 \cdots p_s}$ is a primitive p_1th root of unity. To simplify the notation, let us write F'_i for $F_i(\zeta)$, for $i = 0, \ldots, r$.

We consider the extensions F'_i/F'_{i-1}. From Result 10, we have $[F_iF'_{i-1} : F'_{i-1}] | [F_i : F_{i-1}]$. However,

$$F_i = F_{i-1}(\alpha_i) \Longrightarrow F_iF_{i-1}(\zeta) = F_{i-1}(\alpha_i, \zeta) = F_i(\zeta) = F'_i,$$

so $[F'_i : F'_{i-1}] | [F_i : F_{i_1}]$, which implies that $[F'_i : F'_{i-1}]$ has the value 1 or p_i. In the first case, we can eliminate F'_i (or F'_{i-1}), so we can assume that $[F'_i : F'_{i-1}] = p_i$. Since F_i and F'_{i-1} are extensions of F_{i-1} and F_i is a finite Galois extension of F_{i-1}, by Result 9, the compositum $F_iF'_{i-1}$ is a Galois extension of F'_{i-1}, i.e., F'_i is a Galois extension of F'_{i-1}. We now may apply Theorem 3: There exists an irreducible polynomial $f_{i-1}(X) = -c_{i-1} + X^{p_i} \in F'_{i-1}[X]$ such that F'_i is a splitting field of f_{i-1}. Let α'_i be a root of f_{i-1}. Then f_{i-1} splits in $F'_{i-1}(\alpha'_i)$, because F'_{i-1} contains a primitive p_ith root of unity. This implies that $F'_i \subset F'_{i-1}(\alpha'_i)$. As the reverse inclusion is clear, we have $F'_i = F'_{i-1}(\alpha'_i)$. We have shown that there exists $\alpha'_i \in F'_i$ such that $F'_i = F'_{i-1}(\alpha'_i)$, with $\alpha'^{p_i}_i \in F'_{i-1}$. Hence the extension F'_r/F'_0 is radical of prime type.

Our next step is to show that $Gal(F'_r/F'_0)$ is solvable. Since F'_r is the splitting field of the polynomial $h(X) = (-1 + X^m)g(X) \in F'_0[X]$, F'_r is a Galois extension of F'_0 and $Gal(F'_r/F'_0)$ is the Galois group of h. From Proposition 3 we deduce that $Gal(F'_r/F'_0)$ is solvable.

We now show that $Gal(F'_r/F)$ is solvable. We consider the chain of fields

$$F_0 \subset F'_0 \subset F'_r.$$

Since F'_0 and F'_r are each the splitting field of a polynomial in $F_0[X]$, from Theorem 5, $Gal(F'_r/F'_0)$ is a normal subgroup of $Gal(F'_r/F_0)$ and

$$Gal(F'_r/F_0)/Gal(F'_r/F'_0) \simeq Gal(F'_0/F_0).$$

From Result 6, $Gal(F'_0/F_0)$ is abelian, hence solvable. Therefore the quotient group $Gal(F'_r/F_0)/Gal(F'_r/F'_0)$ is solvable. However, we have also seen that the subroup $Gal(F'_r/F'_0)$ is solvable. It follows that $Gal(F'_r/F_0)$ is solvable, i.e., $Gal(F'_r/F)$ is solvable.

Let L be a splitting field in F'_r. (All the roots of f lie in F'_r, so a splitting field of f is contained in F'_r.) We are now in a position to show that $Gal(L/F)$ is solvable. Once again we use Theorem 5. We consider the chain of fields

$$F \subset L \subset F'_r.$$

L and F'_r are both splitting fields of polynomials over F, hence $Gal(F'_r/L)$ is a normal subgroup of $Gal(F'_r/F)$ and

$$Gal(F'_r/F)/Gal(F'_r/L) \simeq Gal(L/F).$$

The left hand side of the expression is a quotient of a solvable group, hence solvable. Therefore the Galois group $Gal(L/F)$ is solvable, as required. □

Example The Galois group of the polynomial $f(X) = -1 - 4X + X^5 \in \mathbf{Q}[X]$ is the symmetric group S_5, which is not solvable, hence f is not solvable by radicals.

We now prove the converse of Theorem 5. We need a preliminary result.

EXTSOLVsolvlem2

Lemma 2 *Let F be a field, $f \in F[X]$ and E a splitting field of f. If F^* is an extension of F, then $f \in F^*[X]$. If E^* is an extension of F^* and E^* is a splitting field of f containing E and $\sigma \in Gal(E^*/F^*)$, then $\sigma_{|_E} \in Gal(E/F)$ and the mapping*

$$\phi : Gal(E^*/F^*) \longrightarrow Gal(E/F), \sigma \longmapsto \sigma_{|_E}$$

is a monomorphism.

PROOF By hypothesis we have

$$E = F(\alpha_1, \ldots, \alpha_n) \qquad \text{and} \qquad E^* = F^*(\alpha_1, \ldots, \alpha_n),$$

where the α_i are the roots of f. If $\sigma \in Gal(E^*/F^*)$, then σ permutes the roots of f and fixes F^*, hence F; therefore $\sigma_{|_E} \in Gal(E/F)$. Clearly ϕ is a homomorphism. If $\sigma_{|_E} = \mathrm{id}_E$, then $\sigma_{|_E}(\alpha_i) = \alpha_i$, for all i. Thus $\sigma(\alpha_i) = \alpha_i$, for all i, which implies that $\sigma = \mathrm{id}_{E^*}$. It follows that ϕ is injective. □

Now for the theorem.

Theorem 7 *Let F be a field of characteristic 0 and E a finite Galois extension of F. If the Galois group $Gal(E/F)$ is solvable, then E can be embedded in a radical extension.*

PROOF From Corollary 3 there is a normal subgroup H of prime index, say p, in G. Let ζ be a primitive pth root of unity, which exists in some extension of F, because F has characteristic 0.

We will first suppose that $\zeta \in F$ and prove the theorem by induction on $n = [E : F]$. If $n = 1$, then $E = F$ and there is nothing to prove. (It is sufficient to take any radical extension of F, for example $F(\alpha)$, where α is a root of the polynomial $f(X) = -c + X^p \in F[X]$.)

Now let us suppose that the result is true up to $n - 1$. From Result 8 we know that the extension E/E^H is normal, (E^H is the subfield of E fixed by the elements of H), hence Galois, because the extension is also separable. Now $Gal(E/E^H)$ is a solvable group, being a subgroup of the Galois group $Gal(E/F)$, which we note G, and $[E : E^H] < n$. By the induction hypothesis there is a radical chain

$$E^H \subset F_1 \subset \cdots \subset F_s, \tag{1}$$

where $E \subset F_s$.

Next we observe that E^H/F is a Galois extension, because H is a normal subgroup of G, and $[E^H : F] = [G : H] = p$ (Result 11). From the proof of Theorem 3 there exists $\beta \in E^H$ such that $E^H = F(\beta)$ and $\beta^p \in F$, i.e., E^H is a pure extension of E and we may lengthen the chain (1) by adding the prefix $F \subset E^H$. We thus obtain the radical extension F_s/F (and $E \subset F_s$).

We now consider the general case. We set $F^* = F(\zeta)$ and $E^* = E(\zeta)$. As E is a normal extension of F, E is the splitting field of a polynomial $f \in F[X]$. It is not difficult to see that E^* is the splitting field of the polynomial $g(X) = (-1 + X^p)f(X) \in F[X]$. The polynomial g belongs to $F^*[X]$ and E^* is its splitting field. Thus E^* is a normal extension of F^*, hence a Galois extension. We set $G^* = Gal(E^*/F^*)$. From Lemma 2 there is a monomorphism from G^* into G, so we may consider that G^* is a subgroup of the solvable group G, hence is solvable. We may now apply the first part of the proof: there is a radical extension F_t^* of F^* containing E^*: we have the radical chain

$$F^* \subset F_1^* \subset \cdots \subset F_t^*,$$

with $E^* \subset F_t^*$. As $E \subset E^*$, we have $E \subset F_t^*$. Since $F^* = F(\zeta)$, F^* is a pure extension of F and we may lengthen the radical chain by adding the prefix $F \subset F^*$, providing us with the radical extension F_t^*/F (and $E \subset F_t^*$). □

Corollary 2 *If F is a field of characteristic 0 and $f \in F[X]$ whose Galois group is solvable, then f is solvable by radicals.*

Example The Galois group of $f(X) = -1 + X + X^3 \in \mathbf{Q}[X]$ is the symmtric group S_3, hence f is solvable by radicals.

Basic results from Galois theory

Result 1 *A set of distinct automorphisms $\{\sigma_1, \ldots, \sigma_n\}$ on a field F is independant, i.e., if $\lambda_1, \ldots, \lambda_n \in F$ and*

$$\lambda_1\sigma_1(x) + \cdots + \lambda_n\sigma_n(x) = 0,$$

for all $x \in F^*$, then $\lambda_1 = \cdots = \lambda_n = 0$.

Result 2 *If K is a finite extension of F and E a finite extension of K, then E is a finite extension of F and*

$$[E : F] = [E : K][K : F],$$

where $[A : B]$ is the degree of A over B.

propFEalgext3 **Result 3** *If K is an algebraic extension of F, E an extension of K and $\alpha \in E$ is algebraic over K, then α is algebraic over F.*

thGALPOLYirred2 **Result 4** *Let f be a separable polynomial in $F[X]$ of degree n with Galois group $G = Gal(E/F)$. If f is irreducible, then*

- **a.** *n divides the order of G;*
- **b.** *the action of G on A, the set of roots of f, is transitive.*

ropGALPOLYirred1 **Result 5** *Let $f \in F[X]$, with $\deg f \geq 2$, and G be its Galois group. If f has two distinct irreducible factors, then the action of G on A, the set of roots of f, is not transitive.*

GALPOLYctomcor1a **Result 6** *If E is a cyclotomic extension of F, then the Galois group $G(E/F)$ is abelian.*

thSPLIT2 **Result 7** *Let F and F' be fields, $\sigma : F \longrightarrow F'$ an isomorphism, $f \in F[X]$ and $f' \in F'[X]$ the polynomial corresponding to f. If E is a splitting field of F and E' a splitting field of f', then there is an isomorphism $\tilde{\sigma} : E \longrightarrow E'$ extending σ.*

NORMprop2 **Result 8** *Suppose that K is an extension of F and E an extension of K, with E normal over F. Then E is normal over K.*

thGALGRPcomp1 **Result 9** *Let K and L be extensions of F in E, where K is a finite Galois extension of F. Then*

- **a.** *KL is a finite Galois extension of L;*
- **b.** *If $\sigma \in Gal(KL/L)$, then the restriction of σ to K belongs to $Gal(K/F)$ and the mapping*

$$\phi : Gal(KL/L) \longrightarrow Gal(K/F), \sigma \longmapsto \sigma_{|K}$$

is a monomorphism;

GALGRPcompex1 **Result 10** *If K and L are extensions of F, then $[KL : L]$ divides $[K : F]$.*

thGALGRPfund3b **Result 11** *Suppose that E is a finite Galois extension of F and G the associated Galois group. Then K is a normal extension of F if and only if $H = Gal(E/K)$ is a normal subgroup of G. In this case the Galois group $Gal(K/F)$ is isomorphic to the quotient group G/H.*

In addition, for any subgroup H (not necessarily normal),

$$[K : F] = [G : H] \qquad \text{and} \qquad [E : K] = |H|.$$

ALGRPnormclosth1 **Result 12** *Let E be a finite extension of F and N the normal closure of E over F in an algebraic closure C of F. Then*

$$N = \prod_{\sigma \in Gal(N/F)} \sigma(E).$$

4 Appendix: Solvable groups

In this appendix we revise the basic properties of solvable groups, which may or may not be known to the reader.

A *normal series* or *normal sequence* of a group G is a sequence of subgroups of the form

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_n = \{e\},$$

where e is the identity of G and G_{i+1} is a proper normal subgroup of G_i. We do not require the subgroups to be normal subgroups of G. The quotient groups G_i/G_{i+1} are called the factors of the normal series. A group is said to be *solvable* if it has a normal series with abelian factors. In this case we say that the normal series is solvable. An abelian group G is clearly solvable: we only need to take the sequence $G = G_0 \rhd \{e\}$.

Let G be a group. The *commutator* of two elements $x, y \in G$, which we note $[x, y]$, is the product $xyx^{-1}y^{-1}$. The *commutator subgroup* of G, written G', is the subgroup generated by the commutators. From the observation that

$$g[x, y]g^{-1} = [gxg^{-1}, gyg^{-1}]$$

for all $g \in G$, we deduce that G' is a normal subgroup of G. There is no difficulty in seeing that the quotient group G/G' is abelian.

APPSOLVprop1 **Proposition 4** *If H is a normal subgroup of G, then G/H is abelian if and only if $G' \subset H$.*

PROOF If G/H is abelian, then

$$xyH = xHyH = yHxH = yxH \Longrightarrow [x, y] \in H.$$

As all the commutators lie in H, we have $G' \subset H$.

On the other hand, if $G' \subset H$, then by the third isomorphism theorem

$$(G/G')/(H/G') \simeq G/H,$$

so G/H is isomorphic to the quotient group of an abelian group and is thus abelian. □

The *higher commutator subgroups* are defined by induction:

$$G^{(0)} = G \qquad \text{and} \qquad G^{(i+1)} = G^{(i)'},$$

i.e., $G^{(i+1)}$ is the commutator subgroup of $G^{(i)}$ and so is a normal subgroup of $G^{(i)}$.

APPSOLVprop2 **Proposition 5** *A group G is solvable if and only if there is a nonnegative integer n such that $G^{(n)} = \{e\}$.*

PROOF If $G^{(n)} = \{e\}$, then the series

$$G = G^{(0)} \rhd G^{(1)} \rhd G^{(2)} \rhd \cdots \rhd G^{(n)} = \{e\}$$

is solvable, so G is a solvable group.

If G is solvable, then there exists a solvable series

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_n = \{e\}$$

We prove, by induction on i, that $G_i \supset G^{(i)}$, for $i = 0, \ldots, n$. First, for $i = 0$, we have $G_0 = G = G^{(0)}$. Suppose now, that $G_i \supset G^{(i)}$. Then $G_i' \supset G^{(i)'} = G^{(i+1)}$. However, G_i/G_{i+1} is abelian, hence, from Proposition 4, we have $G_{i+1} \supset G_i'$ and so $G_{i+1} \supset G^{(i+1)}$. This finishes the induction step. It follows that $G^{(n)} = \{e\}$. □

APPSOLVprop1

Now we come to two fundamental results.

Theorem 8 *If G is a solvable group, then every subgroup and quotient group is solvable.*

PROOF Let H be a subgroup of the solvable group G. By induction it is easy to prove that $H^{(i)} \subset G^{(i)}$, for all i. There exists a nonnegative integer n such that $G^{(n)} = \{e\}$. It follows that $H^{(n)} = \{e\}$ and so, by Proposition 5, H is solvable. APPSOLVprop2

We now consider the case of a quotient group. We will prove a more general result: if G is a solvable group and $\phi : G \longrightarrow C$ is a surjective homomorphism, then C is solvable. To do so, we will show that $\phi(G^{(i)}) = C^{(i)}$, for all i. We will use an induction argument. For $i = 0$, the result is evident. As the image of a commutator is a commutator, $\phi(G') \subset C'$. On the other hand, if $u, v \in C$, then there exist $x, y \in G$ such that $\phi(x) = u$, $\phi(y) = v$ and we have $\phi[x, y] = [u, v]$; it follows that $\phi(G') = C'$. Thus the result is true for $i = 1$. Suppose now that $\phi(G^{(i)}) = C^{(i)}$. Then ϕ restricted to $G^{(i)}$ provides us with a surjective homomorphism of $G^{(i)}$ onto $C^{(i)}$. From the previous argument, we have $\phi(G^{(i)'}) = C^{(i)'}$, i.e., $\phi(G^{(i+1)}) = C^{(i+1)}$. This completes the induction step. To finish we notice that there is an n such that $G^{(n)} = \{e_G\}$. This implies that $C^{(n)} = \{e_C\}$ and so C is solvable. □

This theorem has a converse.

Theorem 9 *Let G be a group with a normal subgroup H. If H and G/H are solvable, then so is G.*

PROOF As G/H is solvable, there is a solvable series composed of subgroups of G/H:

$$G/H = G_0^* \rhd G_1^* \rhd \cdots \rhd G_s^* = \{H/H\},$$

where $G_i/H = G_i^*$. By the correspondance theorem, there is a normal series

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_s = H.$$

By the third isomorphism theorem, we have $G_i/G_{i+1} \simeq (G_i/H)/(G_{i+1}/H)$, so the factors G_i/G_{i+1} are abelian. As H is solvable, we have a solvable series composed of subgroups of H:

$$H = H_0 \rhd H_1 \rhd \cdots \rhd H_t = \{e_H\} = \{e_G\}.$$

Putting the two series together gives us a solvable series of G. □

We may refine the solvable series so as to obtain factor groups of prime order. To prove this we need a preliminary result. We recall that a group G is *simple* if $G \neq \{e\}$ and its only normal subgroups are $\{e\}$ and G itself.

APPSOLVlem1 **Lemma 3** *If G is a finite abelian simple group, then G is cyclic of prime order.*

PROOF If $x \in G$ and $x \neq e$, then $\langle x \rangle$ is a normal subgroup, because G is abelian. As $x \neq e$, we have $\langle x \rangle = G$, so G is cyclic.

If G is not of prime order and $|G| = n$, then G has a (unique) subgroup of order $\frac{n}{d}$, for every positive divisor d of n. As G is abelian, these subgroups are normal, so we have a contradiction to the simplicity of G. Thus G is of prime order. □

APPSOLVth3 **Theorem 10** *If G is a solvable group, then G has a solvable series whose factor groups are cyclic of prime order.*

PROOF As G is solvable, G has a solvable series

$$G = G_0 \rhd \cdots \rhd G_i \rhd G_{i+1} \rhd \cdots \rhd G_n = \{e\}.$$

If G_{i+1} is not a maximal normal subgroup of G_i, then we can insert a normal subgroup H between G_{i+1} and G_i. As the quotient group H/G_{i+1} is a subgroup of G_i/G_{i+1}, it is abelian. Continuing the process we obtain a solvable series such that G_{i+1} is always a maximal normal subgroup of G_i.

Now G_i/G_{i+1} is finite and abelian. If this factor group is not simple, then it has a proper nontrivial normal subgroup. By the correspondance theorem there exists a nontrivial subgroup, which is normal in G_i and lies strictly between G_{i+1} and G_i; thus G_i is not maximal, a contradiction. Therefore G_i/G_{i+1} is finite, abelian and simple. By Lemma APPSOLVlem1 3, G_i/G_{i+1} is cyclic of prime order. □

APPSOLVcor1 **Corollary 3** *A solvable group G has a normal subgroup of prime index.*

PROOF From Theorem APPSOLVth3 10 we may suppose that in the solvable series of G the index of G_1 in G_0 is a prime number p. As $G_0 = G$, we have the result. □

Solvability of the symmetric groups

The symmetric groups S_n are solvable if and only if $n \leq 4$. If $n = 1$ or $n = 2$, then S_n is abelian, hence solvable. For S_3 it is sufficient to consider the series

$$\langle e \rangle \subset A_3 \subset S_3.$$

For S_4 we may take the chain

$$\langle e \rangle \subset V \subset A_4 \subset S_4,$$

where

$$V = \{e, (12)(34), (13)(24), (14)(23)\}.$$

(The only possible difficulty here is in seeing that $V \lhd A_4$; however, it is sufficient to notice that conjugation preserves the cycle structure.)

For the next result we will suppose that it is known that, for $n \geq 5$, A_n is simple, i.e., has no normal subgroups other than $\{e\}$ or A_n itself.

Theorem 11 *For $n \geq 5$, S_n is not solvable.*

PROOF For $n \geq 5$, A_n is simple, therefore $A_n' = A_n$ or $A_n' = \{e\}$. However, the second case is not possible, because A_n is not abelian for $n \geq 4$. Thus $A_n' = A_n$, which implies that $A_n^{(k)} = A_n$, for all k. It follows that A_n is not solvable. As a subgroup of a solvable group is solvable, S_n cannot be solvable. □