9 Radical extensions

Keywords: Normal closure, solvable group, commutator, radical extension, solvable extension.

9.1 Normal closures

Definition 116. Let $K \subset L \subset M$ be fields with L/K finite. We say that M is a **normal closure** of L/K if:

- The field M is a splitting field over K.
- No field other than M between L and M is a splitting field over K.

Proposition 117. Let L/K be a finite extension. Then there exists a normal closure M of L/K. If L/K is separable then M/K is Galois. Any two normal closures of L/K are L-isomorphic.

Proof. Let $v_1, \ldots, v_r$ be a K-basis of L. Let $f_i = \mathrm{mp}_K(v_i)$ and $f = f_1 \cdots f_r$.

Existence. Let M be a splitting field for f over L. Then M is also a splitting field for f over K (exercise). If L/K is separable then f_i is separable over K whence M/K is Galois by theorem 97. Any splitting field M' of L/K in between L and M must split each f_i for they each acquire a root in L. This shows that $M = M'$ and thus that M is a normal closure of L/K.

Uniqueness. Let M_i be a normal closure of L/K for all $i \in \{1, 2\}$. Then M_i is a splitting field over L of f. By uniqueness of splitting fields (proposition 91) M_1 and M_2 are L-isomorphic. □

9.2 Solvable groups

Definition 118. Let G be a group. We say that G is **solvable** if there are subgroups $G = A_0 \supset A_1 \supset \cdots \supset A_r = 1$ such that for all i, A_{i+1} is normal in A_i and A_i/A_{i+1} is abelian.

If G is solvable and finite, then by inserting more A_i we can arrange for A_i/A_{i+1} to be cyclic and such that its order is a prime number.

Proposition 119. Let G be a group and $H \subset G$ a subgroup.

(a) If G is solvable then so is H.

(b) If G is solvable and H is a normal subgroup of G then G/H is solvable.

(c) If H is normal in G and H and G/H are solvable then G is solvable.

(d) Every abelian group is solvable.

Proof. Proof of (a). Let $G = A_0 \supset A_1 \supset \cdots \supset A_r = 1$ be such that for all i, A_{i+1} is normal in A_i and A_i/A_{i+1} is abelian. Set $B_i = H \cap A_i$. Then $H = B_0 \supset B_1 \supset \cdots \supset B_r = 1$ and B_{i+1} is normal in B_i and B_i/B_{i+1} is a subgroup of an abelian group A_i/A_{i+1} and thereby abelian itself. This shows that H is solvable.

Part (b) is similar. Parts (c) and (d) are easy. □

For elements a, b of a group we write $[a, b] = aba^{-1}b^{-1}$. Such elements are called **commutators**.

Lemma 120. Every element of the alternating group A_5 is a commutator.

Proof. Every element of A_5 is of the form (ijk), $(ij)(k\ell)$ or $(ijk\ell m)$ where $i, j, k, \ell, m \in \{1, 2, 3, 4, 5\}$ are distinct. The following calculations finish the proof:

$$\begin{aligned}
&[(ij\ell), (ikm)] = (ij\ell)(ikm)(i\ell j)(imk) = (ijk),\\
&[(ijk), (ij\ell)] = (ijk)(ij\ell)(ikj)(i\ell j) = (ij)(k\ell),\\
&[(ij)(km), (im\ell)] = (ij)(km)(im\ell)(ij)km(i\ell m) = (ijk\ell m).
\end{aligned}$$ □

Proposition 121. The symmetric group S_5 and the alternating group A_5 are not solvable.

Proof. By proposition 119 it is enough to prove that A_5 is not solvable. Suppose that it is: $A_5 = B_0 \supset B_1 \supset \cdots \supset B_r = 1$ with B_{i+1} normal in B_i and B_i/B_{i+1} abelian. Let $f\colon B_0 \to B_0/B_1$ denote the natural homomorphism. As B_0/B_1 is abelian we have for all $a, b \in B_0$

$$1 = f(a)f(b)f(a)^{-1}f(b)^{-1} = f(aba^{-1}b^{-1}) = f([a, b])$$

so $[a, b] \in B_1$. But all elements of A_5 are commutators by lemma 120 so $B_1 = B_0$. Continuing this way we find $A_5 = B_i$ for all i, a contradiction. □

Lemma 122. Let p be a prime number. Let $H \subset S_p$ be a subgroup containing a p-cycle and at least one transposition (ij). Then $H = S_p$.

Proof. Exercise. □

9.3 Radical extensions

Definition 123. An extension L/K is a **radical extension** if L has the form $K(u_1, \ldots, u_m)$ where for all i there exists $\ell_i > 0$ such that

$$u_i^{\ell_i} \in K(u_1, \ldots, u_{i-1}).$$

It is clear that a radical extension is of finite degree. By inserting further u's if necessary we can arrange that the ℓ_i are prime numbers.

Definition 124. An extension L/K is a **solvable extension** if there exists a radical extension M/K with $L \subset M$.

The main result on solvable extensions is the following.

Theorem 125. Let L/K be a solvable extension of characteristic 0. Then $\mathrm{Gal}(L/K)$ is a solvable group.

Our proof of theorem 125 depends on three lemmas which don't assume the characteristic to be 0.

Lemma 126. Let $K \subset L \subset M$ be fields. Suppose that L/K is a radical extension and M is the normal closure of L/K. Then M/K is a radical extension.

Proof. This is easy using exercise 6.5. □

Lemma 127. Let p be a prime number and L a splitting field of $X^p - 1$ over K. Then $\mathrm{Gal}(L/K)$ is abelian.

Proof. If the characteristic is p then $X^p - 1 = (X-1)^p$ and $L = K$. Suppose now that the characteristic is not p. Let ε be a root of $X^p - 1$ different from 1. Then $X^p - 1$ has p distinct roots $1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{p-1}$. Therefore $L = K(\varepsilon)$. An automorphism of L/K is determined by what it does to ε. Say $s, t \in \mathrm{Gal}(L/K)$ take ε to ε^i, respectively, ε^j. Then st and ts both take ε to ε^{ij}. Thus $st = ts$ and $\mathrm{Gal}(L/K)$ is abelian. □

Lemma 128. Let K be a field in which $X^n - 1$ factors completely. Let $a \in K$ and let L be a splitting field for $X^n - 1$ over K. Then $\mathrm{Gal}(L/K)$ is abelian.

Proof. Let u be a root in L of $X^n - a$. Then $L = K(u)$ because the other roots of $X^n - a$ are of the form $u\alpha$ where α is a root of $X^n - 1$ and is hence in K. Thus, an element of $\mathrm{Gal}(L/K)$ is determined by what it does to u. Let $s, t \in \mathrm{Gal}(L/K)$ and write $s(u) = \alpha u$, $t(u) = \beta u$ where α, β are roots in K of $X^p - 1$. Then st and ts both take u to $\alpha\beta u$. Thus $\mathrm{Gal}(L/K)$ is abelian. □

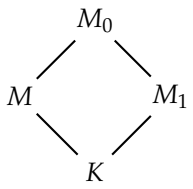
Proof of theorem 125. Let M/K be a radical extension such that $L \subset M$.

If K_0 denotes the closure $K^{*\dagger}$ with respect to L/K nothing in the problem is changed if we replace K by K_0. Hence we may assume that $K = K_0$, that is, L is Galois over K.

If N denotes a normal closure of M/K then N is a radical extension of K by lemma 126. Thus, changing notation again, we may assume that M is Galois over K (by theorem 97 and because the characteristic is 0).

Since $\mathrm{Gal}(L/K)$ is a quotient of $\mathrm{Gal}(M/K)$ and quotients of solvable groups are solvable by proposition 119, we have only to show that $\mathrm{Gal}(M/K)$ is solvable. Thus we may henceforth forget about L.

As M/K is radical, we may suppose that $M = K(u_1, \ldots, u_n)$ where for all i there exists a prime number p_i such that $u_i^{p_i} \in K(u_1, \ldots, u_{i-1})$. We argue by induction on n. Write $p = p_1$, $u = u_1$; then $u^p \in K$. Let M_0 be a splitting field for $X^p - 1$ over M. Let M_1 be the subfield of M_0 generated by K and the roots of $X^p - 1$.



If we show that $\mathrm{Gal}(M_0/K)$ is solvable, it will follow that $\mathrm{Gal}(M/K)$ is, again because a quotient of a solvable group is solvable. Now M_1 is a Galois ex-

tension of K with an abelian Galois group by lemma 127. Hence it will sufice to show that $\mathrm{Gal}(M_0/M_1)$ is solvable, for a group is solvable if a normal subgroup and its quotient group are solvable (proposition 119c). Now $M_0 = M_1(u_1, \ldots, u_n)$ for M_0 is generated over K by the u's and the roots of $X^p - 1$ and the latter are already in M_1. Write $G = \mathrm{Gal}(M_0/M_1)$ and let $H = M_1(u)^* \subset G$ be the subgroup corresponding to $M_1(u)$. Since $X^p - 1$ factors completely in M_1, $M_1(u)$ is a splitting field for $X^p - u_1^p$ over M_1 and hence is Galois with abelian Galois group by lemma 128. Thus G/H is abelian. To prove that G is solvable it remains finally to show that H is solvable. This follows from our inductive assumption, for M_0 is a radical extension of M_1 generated by a chain $u_2, \ldots, u_n$ as before with $n - 1$ elements. This completes the proof of theorem 125. □

Using theorem 125 we can easily construct an unsolvable field extension L/K. Let S_5 act on $L = \mathbb{Q}(X_1, \ldots, X_5)$ by permuting the variables and put $K = L^{S_5}$. Then $\mathrm{Gal}(L/K) \cong S_5$ hence is an unsolvable group; therefore L/K is an unsolvable extension.

We shall give a more satisfying example with $K = \mathbb{Q}$ with the help of the following lemma.

Lemma 129. Let p be a prime number and let $f \in \mathbb{Q}[X]$ be an irreducible polynomial of degree p and with precisely two nonreal complex roots. Let $L/\mathbb{Q}$ be the complex splitting field of f. Then $\mathrm{Gal}(L/K) \cong S_p$.

Proof. Let $H = \mathrm{Gal}(L/K)$. Then H acts faithfully on the set of complex roots of f. Thus $H \subset S_p$. Also $[L : K]$ is divisible by p because if $\alpha \in L$ is a root of f then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = p$. But $\#H = [L : K]$ so H contains a p-cycle. Complex conjugation restricts to an element of $\mathrm{Gal}(L/K) = H \subset S_p$ which is a transposition. Lemma 122 now implies that $H = S_p$. □

We claim that $f = x^5 - 6x + 3$ is not solvable. It is irreducible over $\mathbb{Q}$ by Eisenstein's criterion and a crude inspection of its graph reveals that it has exactly two nonreal roots. Hence its splitting field over $\mathbb{Q}$ has Galois group S_5 by lemma 129. Therefore f is not solvable by theorem 125.