5 Normal subgroups and stability

Keywords: Algebraic extensions; finite extensions; finitely generated; normal subgroup; stable intermediate field.

5.1 Algebraic field extensions

Definition 84. A field extension $K \subset L$ is said to be **algebraic** if every element of L is algebraic over K. A field extension $K \subset L$ is called **finite** if its degree $[L : K]$ is finite.

Proposition 85. Every finite field extension is an algebraic extension.

Proof. Let L/K be a finite extension, say, of degree n. Let $\alpha \in L$. We must prove that α is algebraic over K. Now $1, \alpha, \alpha^2, \ldots, \alpha^n$ are $n+1$ elements in the n-dimensional vector space L over K and are therefore independent. That is, we have $\sum_{i=0}^{n} c_i \alpha^i = 0$ for some $c_i \in K$, not all zero. Write $f = \sum_{i=0}^{n} c_i X^i \in K[X]$. Then $f(\alpha) = 0$ and f is nonzero. This proves that α is algebraic over K as required. □

Proposition 86. Let M/K be fields. Let L be the set of elements of M that are algebraic over K. Then L is a subfield of M.

Proof. Let $\alpha, \beta \in L$. We must prove $K(\alpha, \beta) \subset L$. As α is algebraic over K, we have $[K(\alpha), K] < \infty$ by proposition 56e. Since β is algebraic over K it certainly is over $K(\alpha)$ and it follows that $[K(\alpha, \beta) : K(\alpha)]$ is finite. By the tower law, $[K(\alpha, \beta) : K]$ is finite as well. By proposition 85, $K(\alpha, \beta)$ is algebraic over K. This implies $K(\alpha, \beta) \subset L$ as promised. □

5.2 Exercises

(5.1) Let $\alpha \in \mathbb{C}$ be a root of $X^3 + \sqrt{3}\,X + \sqrt{5}$. Which of our theorems guarantee(s) that α is algebraic over $\mathbb{Q}$? Find a nonzero $f \in \mathbb{Q}[X]$ explicitly such that $f(\alpha) = 0$.

(5.2) Let K be a field and let α be an element of a larger field. Prove that α is algebraic over K if and only if $[K(\alpha) : K] < \infty$.

(5.3) Give an example of an infinite algebraic extension.

(5.4) Prove that a field extension is finite if and only if it is algebraic and finitely generated. (A field extension is said to be **finitely generated** if it is of the form $K \subset K(\alpha_1, \ldots, \alpha_n)$).

(5.5) Let $K \subset L \subset M$ be fields. Let $\alpha \in M$ and suppose that L/K is algebraic. Prove: if α is algebraic over L then it is algebraic over K.

5.3 Normal subgroups and stability

Let $K \subset M$ be fields and $f \in K[X]$. We say that f **factors completely over M** or **splits into linear factors over M** if all monic irreducible divisors of f in $M[X]$ have degree 1. Equivalently, f is of the form $c(X-a_1)\cdots(X-a_k)$ for some $c \in K^\times$ and $a_i \in M$.

If in addition to this $a_i \neq a_j$ whenever $i \neq j$ then we say that f **splits into distinct linear factors over M.**

Proposition 87. Suppose that M/K is Galois and f is a monic irreducible polynomial over K having a root u in M. Then f splits into distinct linear factors over M.

Proof. Let $u_1, \ldots, u_r$ be the distinct elements of $\{\phi(u) \mid \phi \in \mathrm{Gal}(M/K)\}$. Each u_i is a root of f and so we have $r \leq \deg f$. Write $g = (X-u_1)\cdots(X-u_r)$. In order to show that $g \in K[X]$, observe that any automorphism of M/K merely permutes the u_i. It follows that any coefficient of g is fixed by all automorphisms of M/K, hence is in K because M/K is Galois. By ** it follows that f divides g. Since also $\deg g \leq \deg f$ we deduce $f = g$. By construction, g factors over M into distinct linear factors; hence so does f. □

Recall that a subgroup H of a group G is called **normal** if $gHg^{-1} = H$ for all $g \in G$. If H is a normal subgroup of G then G/H is a group.

Definition 88. Let $K \subset L \subset M$ be fields. We say that L is **stable (relative to K and M)** if $\phi(L) \subset L$ for all $\phi \in \mathrm{Aut}(M/K)$.

Although for stable L the definition only gives $\phi(L) \subset L$ it is even true that $\phi(L) = L$ because also $\phi^{-1}(L) \subset L$.

Theorem 89. Let $K \subset L \subset M$ be fields. Suppose that M/K is finite and Galois and write $G = \mathrm{Gal}(M/K)$. Then the following are equivalent.

(a) L^* is a normal subgroup of G.

(b) L is stable (relative to K and M).

(c) L is Galois over K.

If these are true then G/L^* is isomorphic to $\mathrm{Gal}(L/K)$.

Proof. Proof of (b) $\Rightarrow$ (a). We must show that if $s \in G$ and $t \in L^*$ then $s^{-1}ts \in L^*$. That is, given $x \in L$ we must prove $s^{-1}ts(x) = x$ or its equivalent $ts(x) = s(x)$. But this is true since $x \in L$ and L is stable, whence $s(x) \in L$.

Proof of (a) $\Rightarrow$ (b). The proof is essentially the above read backwards. Given any $x \in L$ and $s \in G$ we must prove $s(x) \in L$. That is, we must show $ts(x) = s(x)$ for all $t \in H$ or its equivalent $s^{-1}ts(x) = x$. But this is true because $x \in L$ and $s^{-1}ts \in L^*$.

Proof of (b) $\Rightarrow$ (c). Let $x \in L$. We must find $\phi \in \mathrm{Gal}(L/K)$ such that $\phi(x) \neq x$. As M/K is Galois, there exists $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(x) \neq x$. We have $\sigma(L) = L$ because L is stable. Define ϕ to be the restriction of σ to L. Then ϕ has the required properties.

Proof of (c) $\Rightarrow$ (b). Note that L/K is finite and therefore algebraic by proposition 85. Let $u \in L$ and $s \in \mathrm{Gal}(M/K)$. We know that u is algebraic over K; let f be its minimum polynomial over K. By proposition 87, f factors completely in L. Since $s(u)$ is a root of f, it must be in L.

Proof of the final statement. We shall define a group homomorphism $h\colon G = \mathrm{Gal}(M/K) \to \mathrm{Gal}(L/K)$. If $s \in G$ then $h(s)$ will be the restriction of s to L. It is clear that h is a group homomorphism. The kernel of h is L^* so by the first isomorphism theorem for groups, the image of h is isomorphic to G/L^*. Also, G/L^* and $\mathrm{Gal}(L/K)$ have equal (finite) cardinalities by theorem 78c and the result follows. □

5.4 Exercises

(5.6) Let $t \in \mathrm{Gal}(N/K)$. Let L, M be intermediate fields and $H, J \subset G$ be subgroups.

(a) If $M = t(L)$ then $L^* = t^{-1}M^*t$.

(b) If $t^{-1}Ht = J$ then $H^\dagger = t(J^\dagger)$.

(5.7) Let $G = \mathrm{Gal}(M/K)$ and L a closed intermediate field. Show

$$\{g \in G \mid g(L) = L\} = \{g \in G \mid gL^* = L^*g\}.$$

(5.8) Give an example of fields $K \subset L \subset M$ such that M/K is Galois, L is closed, L/K is Galois, yet L is not stable.

6 Splitting fields

Keywords: Splitting field; derivative; separable.

6.1 Splitting fields

Definition 90. Let $K \subset M$ be fields and let $f \in K[X]$. We say that M is a **splitting field** for f over K if f factors completely over M and M is generated by K and the roots of f in M.

This is the usual name though it would be more consistent to call it a *splitting extension.*

If there is no need to call attention to the polynomial we shall simply say that M is a splitting field over K.

Note that by exercise 5.4, any splitting field over K is of finite degree over K.

Example 91. Consider $f = X^3 - 2$. The complex roots of f are α, $\alpha\varepsilon$, $\alpha\varepsilon^2$ where $\alpha = \sqrt[3]{2} \in \mathbb{R}$ and $\varepsilon = \exp(2\pi i/3) \in \mathbb{C}$. It follows that $L := \mathbb{Q}(\alpha, \alpha\varepsilon, \alpha\varepsilon^2)$ is a splitting field for f over $\mathbb{Q}$. We only need two generators: $L = \mathbb{Q}(\alpha, \varepsilon)$. So far we have no method of proving that L is Galois over $\mathbb{Q}$; from the results in this chapter, it will follow almost immediately that it is.

Proposition 92: Existence and uniqueness of splitting fields.

(a) Let f be a polynomial over a field K. Then there exists a splitting field for f over K.

(b) For all $i \in \{1, 2\}$, let M_i/K_i be a splitting field for $f_i \in K_i[X]$ over K_i. Let $s\colon K_1[X] \to K_2[X]$ be an isomorphism such that $s(K_1) = K_2$, $s(X) = X$ and $s(f_1) = f_2$. Then the restriction of s to K_1 extends to an isomorphism $M_1 \to M_2$.

Proof. Proof of (a). Induction on the degree of f. If f is constant then $M = K$ will do. Suppose now that the degree of f is positive. Let g be an irreducible factor of f. By proposition 60 there exists an extension $K(\alpha)/K$ such that $g(\alpha) = 0$. There exists a polynomial h with coefficients in $K(\alpha)$ such that $f = (X - \alpha) \cdot h$. By the induction hypothesis, there exists a splitting field L for h over $K(\alpha)$. We claim that L is a splitting field for f over K. Indeed, f factors completely over L because h does. Moreover, L is generated by $K(\alpha)$ and the roots of h; it follows that L is generated by the roots of f. This proves that our claim that L is a splitting field for f over K.

Proof of (b). Induction on $d = [M_1 : K_1]$. If $d = 1$ then f_1 factors completely over K_1. Therefore so does f_2 over K_2 and $M_2 = K_2$.

Let now $d > 1$. We may assume that f_1 has an irreducible factor g_1 of degree greater than 1. Write $g_2 = s(g_1)$. For all $i \in \{1, 2\}$, let α_i be a root of g_i in M_i. By proposition 60 the isomorphism $s\colon K_1 \to K_2$ can be extended to an isomorphism $K_1(\alpha_1) \to K_2(\alpha_2)$. Then M_i is a splitting field for f_i over $K(\alpha_i)$ for all $i \in \{1, 2\}$ (exercise). Since $[M_1 : K_1(\alpha_1)] < [M_1 : K_1]$

the induction hypothesis implies that our isomorphism $K_1(\alpha_1) \to K_2(\alpha_2)$ extends to an isomorphism $M_1 \to M_2$. □

Definition 93. The **derivative** of a polynomial $f \in K[X]$ in one variable is defined as follows: writing $f = \sum_{\geq 0} a_n X^n$ we put $f' = \sum_{\geq 1} n\, a_n X^{n-1}$.

Exercise (6.1) Let $f, g \in K[X]$, $a, b \in K$. Prove that $(af + bg)' = af' + bg'$ and $(fg)' = f'g + fg'$.

(This is a straightforward calculation. You shouldn't and needn't use anything you may have learned in analysis about differentiation.)

Proposition 94. Let K be a field, $a \in K$ and $f \in K[X]$. Then $(X-a)^2$ divides f in $K[X]$ if and only if $X - a$ divides both f and f'.

Proof. Proof of $\Rightarrow$. If $f = (X-a)^2 g$ then $f' = (X-a)\big(2g + (X-a)g'\big)$, which is divisible by $X - a$ and of course so is f.

Proof of $\Leftarrow$. Suppose that $X - a$ divides both f and f'. By theorem 2 there are $q, r \in K[X]$ such that $f = (X-a)^2 q + r$ and $\deg r < 2$. Since $X - a \mid f$ we have $r = (X-a)c$ for some constant $c \in K$. Differentiation gives $f' = (X-a)\big(2g + (X-a)g'\big) + c$. Since $X - a \mid f'$ we find $c = 0$. It follows that $f = (X-a)^2 q$ as required. □

Proposition 95. Let K be a field let $f \in K[X]$ be irreducible. Then the following are equivalent.

(1) Let a be an element of a larger field L. Then f is not divisible by $(X-a)^2$ in $L[X]$. In words: f has no multiple root in any larger field.
(2) In some splitting field of f over K, f factors into distinct linear factors.
(3) $f' \neq 0$.

Proof. (1) $\Rightarrow$ (2) is clear.

Proof of (2) $\Rightarrow$ (3). Suppose on the contrary that $f' = 0$. Let L/K be a splitting field for f. As f is not constant, it has a root $a \in L$. Therefore $X - a$ divides both f and f' in $L[X]$. By proposition 94, $(X-a)^2$ divides f, a contradiction.

Proof of (3) $\Rightarrow$ (1). Since f is irreducible over K it generates a maximal ideal $(f) \subset K[X]$ by proposition 33. We have $f' \notin (f)$ by the assumption that $f' \neq 0$. Therefore there are $p, q \in K[X]$ such that $pf + qf' = 1$. It follows that in $L[X]$, f, f' have no common factor of the form $X - a$. By proposition 94, $(X-a)^2$ does not divide f. □

Definition 96. An irreducible polynomial $f \in K[X]$ is called **separable** if it satisfies the equivalent conditions of proposition 95. An element α, algebraic over K, is said to be **separable** over K if its minimum polynomial is separable over K. An algebraic field extension L/K is said to be **separable** if all elements of L are separable over K. To avoid ambiguity we shall not define separability over K of a polynomial unless it is irreducible over K.

Example 97. Here is the simplest example of a nonseparable extension.

Let p be a prime number and F a field of characteristic p. Let $L = F(T)$, the field of rational functions in a variable T. Put $K = F(T^p)$. Write $g = X^p - T^p \in K[X]$. We shall prove that g is irreducible over K and not separable.

In order to prove that g is irreducible over K, it is helpful to write U instead of T^p. We get $g = X^p - U$ which is Eisenstein at U in $F[U] = F[T^p]$ and is therefore irreducible over K.

On the other hand, $g = (X - T)^p$ so g has multiple roots in its splitting field. Therefore, g is not separable.

Notice also that L is a splitting field for g over K. The Galois group for L/K is trivial because if $s \in \mathrm{Gal}(L/K)$ then s takes the root T of g to a root of g; the only possibility is $s(T) = T$.

Exercise (6.2) Let $f \in K[X]$ be irreducible.

(a) Suppose that the characteristic of K is 0. Then f is separable.

(b) Suppose that the characteristic of K is a prime number p. Then f is separable if and only if there exists a polynomial g such that $f = g(X^p)$.

The following is the second most important result in our course. The implications [2 $\Rightarrow$ 1] and [3 $\Rightarrow$ 1] are often used in applications.

Theorem 98. Let M/K be a finite field extension. The following are equivalent:

(1) M/K is Galois.

(2) M/K is separable and a splitting field.

(3) M/K is a splitting field for a polynomial f whose irreducible factors are separable.

Proof. Proof of (1) $\Rightarrow$ (2). Let u be an element of M and f its minimum polynomial over K. By proposition 87, f factors over M into distinct linear factors. Therefore u is separable over K. As this is true for every $u \in M$, the extension M/K is separable.

Let $v_1, \ldots, v_r$ be a K-basis of M, let f_i be the minimum polynomial of v_i over K, and write $g = f_1 \cdots f_r$. By proposition 87 again, each f_i factors completely in M and hence so does g. This shows that M is a splitting field of g over K.

Proof of (2) $\Rightarrow$ (3). Suppose that M is a splitting field of f over K. Let $f = f_1 \cdots f_r$ be the factorisation of f into irreducible factors over K. Each f_i is the minimum polynomial for an element in M which is by assumption separable over K. Hence each f_i is separable over K.

Proof of (3) $\Rightarrow$ (1). Suppose that M is a splitting field over K of a polynomial f whose irreducible factors are separable. Let $G = \mathrm{Gal}(M/K)$. By exercise 4.10, in order to prove that M/K is Galois, it suffices to prove that $\#G \geq [M : K]$. We shall show this by induction on $d = [M : K]$. If $d = 1$ there is nothing to prove.

Suppose now that $d > 1$. Let g be an irreducible factor of f of degree greater than 1; such a g exists because $d > 1$. Let $u \in M$ be a root of g. Let $u_1, \ldots, u_r$ be the roots of g in M (say, $u = u_1$), and let i be such that $1 \leq i \leq r$. By proposition 60 (uniqueness of primitive extensions) there exists a

K-isomorphism $h_i\colon K(u) \to K(u_i)$ taking u to u_i. Now $[M : K(u_i)] = d/r < d$ so by the induction hypothesis, there are at least d/r ways to extend h_i to a K-automorphism of M. As i varies this yields d distinct elements of G as required. □

6.2 Examples

Example 99. Let $n \geq 1$ and let $\varepsilon \in \mathbb{C}$ be a primitive n-th root of unity. Prove that $\mathbb{Q}(\varepsilon)/\mathbb{Q}$ is Galois.

Solution. Let $f = X^n - 1$. By (2) $\Rightarrow$ (1) in theorem 98 it suffices to prove that $\mathbb{Q}(\varepsilon)/\mathbb{Q}$ is separable and a splitting field of f.

We have the factorisation

$$f = \prod_{i=0}^{n-1} (X - \varepsilon^i).$$

To prove this, observe that $X - \varepsilon^i$ divides f in $\mathbb{C}[X]$. Therefore the least common multiple $\prod_{i=0}^{n-1}(X - \varepsilon^i)$ divides f. The argument is finished by looking at the leading terms.

But each root ε^i is in $\mathbb{Q}(\varepsilon)$. It follows that f factors completely over $\mathbb{Q}(\varepsilon)$. Also, $\mathbb{Q}(\varepsilon)$ is generated by $\mathbb{Q}$ and the roots $1, \varepsilon, \ldots, \varepsilon^{n-1}$ of f, thus proving that $\mathbb{Q}(\varepsilon)$ is a splitting field for f over $\mathbb{Q}$.

Moreover, $\mathbb{Q}(\varepsilon)/\mathbb{Q}$ is separable because the characteristic is 0. By (2) $\Rightarrow$ (1) in theorem 98, $\mathbb{Q}(\varepsilon)/\mathbb{Q}$ is Galois.

Alternatively, one can avoid the characteristic 0 argument because we have even proved that f splits into *distinct* linear factors over $\mathbb{Q}(\varepsilon)$ which again implies that $\mathbb{Q}(\varepsilon)/\mathbb{Q}$ is Galois by (3) $\Rightarrow$ (1) in theorem 98. □

The surprise in the above example is that all roots of $X^n - 1$ can be expressed in terms of just one of them.

Example 100. Put $L = \mathbb{Q}(\sqrt{2}, \sqrt{5}) \subset \mathbb{C}$.

(a) Prove that $L/\mathbb{Q}$ is Galois.

(b) Which standard group is isomorphic to the Galois group $G = \mathrm{Gal}(L/\mathbb{Q})$?

(c) List all subgroups of G (by generators) and the corresponding intermediate fields (also by generators).

Solution. (a). It is clear that L is a splitting field over $\mathbb{Q}$ of $(X^2 - 2)(X^2 - 5)$. Also, L is separable over $\mathbb{Q}$ because the characteristic is 0. By theorem 98, $L/\mathbb{Q}$ is Galois.

(b). Let $G, \mathcal{F}, \mathcal{G}, \dagger, *$ be as usual. Every element of G takes $\sqrt{2}$ into $\{-\sqrt{2}, \sqrt{2}\}$ and $\sqrt{5}$ into $\{-\sqrt{5}, \sqrt{5}\}$. Moreover, an element of G is determined by where it takes $\sqrt{2}$ and $\sqrt{5}$. Therefore, there are at most 4 elements of G, which we can already identify as follows, although we don't know yet

whether they exist.

$s \in G$	$s(\sqrt{2})$	$s(\sqrt{5})$
1	$\sqrt{2}$	$\sqrt{5}$
a	$\sqrt{2}$	$-\sqrt{5}$
b	$-\sqrt{2}$	$\sqrt{5}$
c	$-\sqrt{2}$	$-\sqrt{5}$

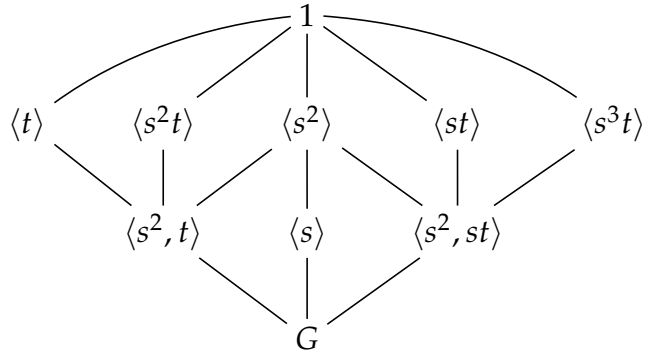
In example 64 we already showed that $[L : \mathbb{Q}] = 4$. By (a), $L/\mathbb{Q}$ is Galois, so by theorem 78 G has precisely 4 elements. Therefore, the elements in the table exist. From the table it is clear that $G \cong (\mathbb{Z}_2)^2$.

(c). Prove yourself that the answer is as follows.

subgroup	1	$\langle a \rangle$	$\langle b \rangle$	$\langle c \rangle$	G
field	L	$\mathbb{Q}(\sqrt{2})$	$\mathbb{Q}(\sqrt{5})$	$\mathbb{Q}(\sqrt{10})$	$\mathbb{Q}$

□

Example 101: Subgroups of D_8. Let $n \geq 1$. The *dihedral group* D_{2n} of order $2n$ is the group of permutations of $\mathbb{Z}/n$ of the form $x \mapsto a + x$ or $x \mapsto a - x$ (with $a \in \mathbb{Z}/n$). We will freely use the following properties of D_8. It is generated by s, t defined by $s(x) = x + 1$, $t(x) = -x$. The subgroups of D_8 are the following.



(102)

Example 103: Biquadratic equation. Let L/K be a splitting field of

$$f = (X^2 - p)^2 - q.$$

Let $G = \mathrm{Gal}(L/K)$ and suppose $\#G \geq 8$. Let $\beta \in L$ be such that $\beta^2 = q$. Let $\alpha_1, \alpha_2 \in L$ be such that $\alpha_1^2 = p + \beta$, $\alpha_2^2 = p - \beta$.

(a) Prove that $f = (X - \alpha_1)(X + \alpha_1)(X - \alpha_2)(X + \alpha_2)$ and that f has 4 distinct roots.

(b) Let Γ be the graph whose vertices are the roots of f in L and such that θ_1, θ_2 are adjacent whenever $\theta_1 + \theta_2 \neq 0$.

Prove that G acts faithfully on Γ. Draw Γ. You may now assume that the automorphism group of Γ is isomorphic D_8. Prove that $G = \mathrm{Aut}(\Gamma)$.

(c) Prove that there are unique $s, t \in G$ such that

$$s(\alpha_1) = \alpha_2, \qquad s(\alpha_2) = -\alpha_1, \qquad t(\alpha_1) = \alpha_1, \qquad t(\alpha_2) = -\alpha_2.$$

(d) Define $\gamma = \alpha_1\alpha_2$, $\delta_1 = \alpha_1 + \alpha_2$, $\delta_2 = \alpha_1 - \alpha_2$. For each $H \in \mathcal{G}$ define $H^0 \in \mathcal{F}$ to be the field in the corresponding slot in figure 2. Prove that $H^\dagger \supset H^0$ for all $H \in \mathcal{G}$.

(e) Prove that if $H_1 \subset H_2 \subset G$ are groups and $[H_2 : H_1] = 2$ then $[H_1^0 : H_2^0] \leq 2$.

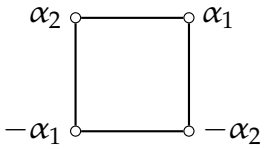
(f) Prove that $H^\dagger = H^0$ for all $H \in \mathcal{G}$.

Solution. (a). The factorisation of f follows from

$$\begin{aligned}(X-\alpha_1)(X+\alpha_1)(X-\alpha_2)(X+\alpha_2) &= (X^2-\alpha_1^2)(X^2-\alpha_2^2)\\ &= (X^2-(p+\beta))(X^2-(p-\beta)) = (X^2-p)^2-\beta^2\\ &= (X^2-p)^2-q = f.\end{aligned}$$

Suppose that f has precisely r distinct roots. So $r \leq 4$. As G consists of K-automorphisms and $f \in K[X]$ we have that G acts on the set of roots of f. This action is faithful because L is generated by the roots of f. Thus we have an injective homomorphism $G \to S_4$. So $8 = \#G \leq \#S_r = r!$ so $r \geq 4$.

(b).



The graph Γ.

Let $g \in G$. We have seen in (a) that g permutes the roots in L of f, that is, the vertices of Γ. In order to prove that it takes edges to edges, let θ_1, θ_2 be vertices of Γ, that is, roots of f. Then

$$\begin{aligned}g(\theta_1), g(\theta_2) \text{ are adjacent} &\iff g(\theta_1)+g(\theta_2) = 0\\ &\iff g(\theta_1+\theta_2) = 0\\ &\iff \theta_1+\theta_2 = 0\\ &\iff \theta_1, \theta_2 \text{ are adjacent.}\end{aligned}$$

This proves that G acts on Γ. The action is faithful by the same argument as in (a).

In other words, we have an injective homomorphism $G \to \mathrm{Aut}(\Gamma)$. We may assume that $\mathrm{Aut}(\Gamma)$ is isomorphic to D_8, in particular, has 8 elements. We know that G has at least 8 elements. Therefore G has precisely 8 elements and $G = \mathrm{Aut}(\Gamma)$.

(c). In (b), we already identified G with D_8. One easily checks that the elements of G corresponding to what we called s and t in example 101 act precisely on the roots of f the way specified.

(d). Note that $s(p+\beta) = s(\alpha_1^2) = \alpha_2^2 = p-\beta$ so $s(\beta) = -\beta$. Similarly, we have $t(p+\beta) = t(\alpha_1^2) = \alpha_1^2 = p+\beta$ so $t(\beta) = \beta$. So

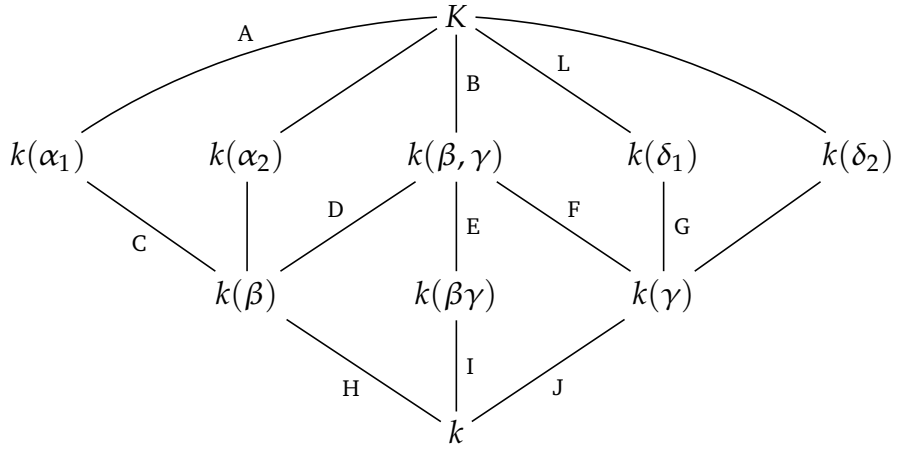
$$s(\beta) = -\beta, \qquad s(\gamma) = -\gamma, \qquad t(\beta) = \beta, \qquad t(\gamma) = -\gamma.$$

The required inclusion $H^\dagger \supset H^0$ follows easily except for $K(\delta_i)$ which we handle as follows: $st(\delta_1) = st(\alpha_1+\alpha_2) = s(\alpha_1-\alpha_2) = \alpha_2-(-\alpha_1) = \alpha_2+\alpha_1 = \delta_1$ and similarly for $K(\delta_2)$.

(e). We do this case by case. In general, one proves that $[L(\theta) : L] \leq 2$ by writing down a quadratic equation over L satisfied by θ.

In case B we have $[K(\alpha_1) : K(\beta)] \leq 2$ by the equation $\alpha_1^2 = p+\beta$ (the cases are indicated next to the edges in figure 2). The same equation handles the cases A, B, C.

Figure 2.



(104)

The equation $\beta^2 = q$ settles cases E, F, H. We have $\gamma^2 = \alpha_1^2\alpha_2^2 = (p+\beta)(p-\beta) = p^2 - q$ which handles J, D. We get $(\beta\gamma)^2 = q(p^2-q)$ which settles case I.

Consider next case G. We have $\delta_1^2 = (\alpha_1+\alpha_2)^2 = \alpha_1^2 + 2\alpha_1\alpha_2 + \alpha_2^2 = (p+\beta) + 2\gamma + (p-\beta) = 2(p+\gamma)$. The equation

$$\delta_1^2 = 2(p+\gamma) \tag{105}$$

shows that δ_1 is of degree at most 2 over $K(\gamma)$.

Finally, we consider case L of $L/K(\delta_1)$. The characteristic is not 2 by part (a). So (105) implies that $\gamma \in K(\delta_1)$. Therefore $(X-\alpha_1)(X-\alpha_2) = X^2 - (\alpha_1+\alpha_2)X + \alpha_1\alpha_2 = X^2 - \delta_1 X + \gamma \in K(\delta_1)[X]$. This handles the case L.

The remaining cases are similar to the ones we have done.

(f). Let $H \in \mathcal{G}$. Then there is a chain of groups $1 = H_0 \subset H_1 \subset H_2 \subset H_3 = G$ such that $\#H_k = 2^k$ for all k and such that H is one of the H_i. By (e) we have $[H_i^0 : H_{i+1}^0] \leq 2$. Multiplying over all $i \in \{0,1,2\}$ and the tower law yields

$$8 = [L:K] = [H_0^0 : H_3^0] = \prod_{i=0}^{2} [H_i^0 : H_{i+1}^0] \leq 2^3 = 8.$$

So equality holds throughout. The same is true for $H_i^\dagger$ so $H_i^\dagger = H_i^0$ for all i. In particular, $H^\dagger = H^0$. □

Example 106. Let ε be a complex primitive fifth root of unity. Put $L = \mathbb{Q}(\varepsilon)$ and $G = \mathrm{Gal}(L/\mathbb{Q})$.

(a) Prove that there exists a unique $s \in G$ such that $s(\varepsilon) = \varepsilon^2$.

(b) Prove that G is generated by s, and write down all subgroups of G by generators.

(c) Prove that $\mathbb{Q}(\varepsilon) = \mathbb{Q}(\alpha)$ where $\alpha = \varepsilon + \varepsilon^2$.

Solution. (a). Uniqueness. The extension $L/\mathbb{Q}$ is generated by ε so any element of G is determined by what it does with ε. This proves uniqueness of σ.

Existence. Both ε and ε^2 are roots of the irreducible polynomial $\phi_5 \in \mathbb{Q}[X]$. By uniqueness of primitive extensions (proposition 60b) there exists a $\mathbb{Q}$-isomorphism s: $\mathbb{Q}(\varepsilon) \to \mathbb{Q}(\varepsilon^2)$ taking ε to ε^2. Then $s^2(\varepsilon) = s(\varepsilon^2) = \varepsilon^4$ and $s^4(\varepsilon) = (\varepsilon^4)^4 = \varepsilon^{16} = \varepsilon$. Therefore s is bijective and $s \in G$.

(b). In part (a) we already saw that $s^4 = 1$ and $s^2 \neq 1$, so s is of order 4. In example 99 we proved that $L/\mathbb{Q}$ is Galois. By theorem 78, the main theorem of Galois theory, it follows that $\#G = [L : \mathbb{Q}] = 4$. Therefore $G = \langle s \rangle$. The subgroups are 1, G and $\langle s^2 \rangle$.

(c). We know that $L/\mathbb{Q}$ is Galois. In particular, $\mathbb{Q}(\alpha) = \mathbb{Q}(\varepsilon)$ would be equivalent to $\mathbb{Q}(\alpha)^* = \mathbb{Q}(\varepsilon)^*$, that is, to $H = 1$ where we define $H = \mathbb{Q}(\alpha)^*$. Suppose that to the contrary $H \neq 1$. Then $s^2 \in H$ so $\varepsilon + \varepsilon^2 = \alpha = s^2(\alpha) = s^2(\varepsilon + \varepsilon^2) = \varepsilon^4 + \varepsilon^8 = \varepsilon^4 + \varepsilon^3$ whence $\varepsilon + \varepsilon^2 - \varepsilon^3 - \varepsilon^4 = 0$, a contradiction as the minimum polynomial of ε is $X^4 + X^3 + \cdots + 1$. This proves $H = 1$ as required.

Another solution to (c) would be to express ε explicitly in terms of α but that is likely to be more work. □

6.3 Exercises

(6.3) Give another solution to exercise 83 by using the results of this section. Namely, if K is a field of characteristic $\neq 2$ and L/K is an extension of degree 2 then L is Galois over K.

(6.4) Let $K(\alpha) = L$ be an algebraic extension of a field K and suppose that $\mathrm{mp}_K(\alpha)$ splits over L into distinct linear factors (that is, is a product of linear polynomials over L and has no multiple roots in L). Prove that $\#\,\mathrm{Gal}(L/K) = [L : K]$ two ways: (1) using no more than the results up to and including chapter 3; (2) using at least one theorem in the present chapter.

(6.5) Let $K \subset L \subset M$ be fields with L/K normal (possibly of infinite degree) and M/L a splitting field of a polynomial with coefficients in K whose irreducible factors over L are separable. Prove that M is Galois over K. [Hint: use exercise 4.17 and proposition 92b].

(6.6) Let K be a field and $f \in K[X]$ (not necessarily irreducible). Prove that f has a multiple root in some larger field if and only if f and f' have a common factor (of degree > 1).

(6.7) If $\alpha_1, \ldots, \alpha_r$ are separable over K, prove that $K(\alpha_1, \ldots, \alpha_r)$ is separable over K.

(6.8) Let $K = \mathbb{R}(T)$, the field of rational functions in one variable. Let $P \subset \mathbb{R}[T]$ be the ideal generated by t.

(a) Prove that P is a prime ideal.

(b) Prove that $f = X^4 - T \in \mathbb{R}[T][X]$ is Eisenstein at P.

(c) Let L be a splitting field for f over K. Prove that L contains a square

root i of -1. Prove $[L : K] = 8$.

(d) Let $\alpha \in L$ be a root of f. Prove that every $g \in G := \mathrm{Gal}(L/K)$ preserves $A = \{\alpha, \alpha i, \alpha i^2, \alpha i^3\}$. Prove that every $g \in G$ preserves the graph with vertex set A and (unoriented) edges $\{\alpha\, i^k, \alpha\, i^{k+1}\}$ where $k \in \{0, 1, 2, 3\}$. Deduce that $G \cong D_8$.

[Hint: you may assume that D_8 is the automorphism group of the above graph, and has 8 elements.]

(e) Give two generators of G and their values at i, α. List all subgroups of G (by group generators), and the corresponding intermediate fields (by field generators). Show either in inclusion diagrams as on page 73 of the printed notes. Give a full proof for just one of the most difficult subgroups (choose yourself) and no proofs for the others.

(6.9) Let $L \subset \mathbb{C}$ be the splitting field of $X^4 - 2$. Prove that $L = \mathbb{Q}(i + \sqrt[4]{2})$. [Hint: Find at least five elements of the $\mathrm{Gal}(L/\mathbb{Q})$-orbit of $i + \sqrt[4]{2}$.]

(6.10) Let M/K be a splitting field of a polynomial $f \in K[X]$ of degree n. Prove that $[M : K]$ divides $n!$.

(6.11) (a) Let $K \subset L \subset M$ be fields with L a splitting field over K. Prove that L is stable.

(b) Let M be a splitting field over K and L an intermediate field. Prove that L is a splitting field over K if and only if L is stable. Show also that $G/L^* \cong \mathrm{Gal}(L/K)$.

(6.12) Suppose that $f = X^4 - 2cX^2 + d^2 \in k[x]$ is irreducible with $c, d \in k$. Show that if $\alpha \in L$ is a root of f in some extension field L, then so is d/α, and deduce that $K = k(\alpha)$ is already a splitting field of f.

(6.13) Let K be a field. Suppose that $f = x^4 - a \in K[x]$ has no root in K but is reducible. Prove that there exists $r \in K$ such that $a = r^2$ or $a = -4\,r^4$.

(6.14) Suppose that $f = X^4 - 2aX^2 + b \in k[X]$ is irreducible, and let K be a splitting field for f over k; prove that $[K : k] = 4$ or 8.

(6.15) Let K be the splitting field of $X^{12} - 1$ over $\mathbb{Q}$. Calculate $[K : \mathbb{Q}]$ and find an explicit $\mathbb{Q}$-basis for K. Prove that K is also the splitting field of $(X^4 - 1)(X^3 - 1)$ over $\mathbb{Q}$.

(6.16) Let $f = X^6 + 3$, $\alpha \in \mathbb{C}$, $f(\alpha) = 0$, $K = \mathbb{Q}(\alpha)$, $g = X^6 + 2$, $M \subset \mathbb{C}$ a splitting field of g over $\mathbb{Q}$, $L = \mathbb{Q}(\sqrt{-2}, \sqrt{-3}) \subset \mathbb{C}$. Clearly, f and g are irreducible over $\mathbb{Q}$ by Eisenstein.

(a) Prove that K contains all 6-th roots of unity.

(b) Prove that K is a splitting field over $\mathbb{Q}$.

(c) Prove $L \subset M$.

(d) Prove $[L : \mathbb{Q}] = 4$.

(e) Prove $[M : \mathbb{Q}] = 12$.

(6.17) (a) Let $f = X^3 - 3\,X - 1$. Prove that f is irreducible in $\mathbb{Q}[x]$.

(b) Prove directly that if $\alpha \in \mathbb{C}$ is a root of f then so is $2 - \alpha^2$.

(c) Let $\alpha \in \mathbb{C}$ be a root of f and put $K = \mathbb{Q}(\alpha)$. Prove that $K/\mathbb{Q}$ is a Galois extension. [Hint: use theorem 98].

(d) Choose yourself a nontrivial element of $G = \mathrm{Gal}(K/\mathbb{Q})$ and write down its matrix with respect to the $\mathbb{Q}$-basis $(1, \alpha, \alpha^2)$ of K.

(6.18) Let $\varepsilon = \exp(2\pi i/7) \in \mathbb{C}$. You may use the fact that ε has degree 6 over $\mathbb{Q}$. We put

$$\alpha = \varepsilon + \varepsilon^6, \quad \beta = \varepsilon^2 + \varepsilon^5, \quad \gamma = \varepsilon^3 + \varepsilon^4.$$

(a) Prove $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\varepsilon)$ and $[\mathbb{Q}(\varepsilon) : \mathbb{Q}(\alpha)] \in \{1, 2\}$ and use the Tower Law to deduce that α is of degree 3 or 6 over $\mathbb{Q}$.

(b) Compute the polynomial $f = (X - \alpha)(X - \beta)(X - \gamma)$ explicitly and hence prove that it is in $\mathbb{Z}[X]$.

(c) Prove that α is of degree 3 over $\mathbb{Q}$.

(d) Find explicitly an $r \in \mathbb{Z}[X]$ such that $r(\alpha) = \beta$.

(e) Prove that $\mathbb{Q}(\alpha)$ is Galois over $\mathbb{Q}$.

(6.19) In this exercise, you prove that $\mathbb{C}$ is algebraically closed (and more).

Let K be a field of characteristic 0 such that every polynomial of degree 2 or of odd degree has a root in K. Let $f \in K[X]$ be monic. Let $o_2(\deg f)$ denote the greatest $n \geq 0$ such that 2^n divides the degree on f. By induction on $r := o_2(\deg f)$ we prove that f has a root in K (and hence that K is algbraically closed).

(a) Let L be a splitting field for f over K. Let $f = \prod_{i=1}^{n}(X - a_i)$ with $a_i \in L$. For $c \in K$, define

$$g_c(X) = \prod_{1 \leq i < j \leq n} (X - a_i - a_j - c a_i a_j).$$

Compute $o_2(\deg g_c)$ and prove that $g_c \in K[X]$.

(b) Finish the proof.

(c) Deduce that $\mathbb{C}$ is algebraically closed.

(6.20) Let L/K be a finite field extension. Let $f \in K[x]$ be irreducible of degree p, a prime number. Suppose that f is reducible in $L[x]$. Prove that p divides $[L : K]$.

(6.21) Let K be a field and $f = X^4 + pX^2 + q \in K[X]$ a polynomial. Let $\alpha \in K$ be such that $X - \alpha \mid f$.

(a) Suppose that the characteristic of K is not 2. Prove that there exists $\beta \in K$ such that $(X - \alpha)(X - \beta) \mid f$.

(b) Suppose that the characteristic of K is 2. Prove again that there exists $\beta \in K$ such that $(X - \alpha)(X - \beta) \mid f$.

(6.22) For each of the following polynomials f, determine the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ where K is a splitting field of f over $\mathbb{Q}$, and all intermediate fields.

(a) $X^4 - 8X^2 + 8$.
(c) $X^4 - 22X^2 + 25$.
(b) $X^4 - 8X^2 + 4$.
(d) $X^6 + X^3 + 1$.

(6.23) In this exercise you generalise the results of this section to infinite families of polynomials, with an application to algebraic closures.

We say that L/K is a **splitting field** for an infinite set of polynomials $\{f_i \mid i \in I\} \subset K[X]$ if every f_i factors completely over L, and L is generated over K by the set of those $\alpha \in L$ for which $f_i(\alpha) = 0$ for some $i \in I$.

(a) Analogous to proposition 92, prove that a splitting field for $\{f_i \mid i \in I\}$ exists and is unique. (This involves a set theoretic difficulty; use Zorn's lemma. If you don't like set theory, simply assume that I is countable, say, $I = \mathbb{N}$. For uncountable I the Galois theoretic part of the proof is the same.)

(b) Let L/K be an algebraic extension. Analogous to theorem 98, prove that L/K is Galois if and only if L/K is a splitting field for a family of separable irreducible polynomials over K.

(c) We say that L is an **algebraic closure** of K if L/K is algebraic and L is algebraically closed. Prove that if L/K is a splitting field of all polynomials in $K[X]$, then L is algebraically closed. [Hint: use the result of exercise 5.5]. Deduce that every field has an algebraic closure and that it is unique (in what sense?).

(6.24) Let ε be a complex primitive 7th root of unity. Put $L = \mathbb{Q}(\varepsilon)$ and $G = \mathrm{Gal}(L/\mathbb{Q})$.

(a) Say why we already know that $L/\mathbb{Q}$ is Galois of degree 6.

(b) Prove that there exists a unique element $s \in G$ such that $s(\varepsilon) = \varepsilon^3$.

(c) Prove that s has order 6.

(d) Prove that $G = \langle s \rangle$.

(e) Give a generator for the group $\mathbb{Q}(\alpha)^* \subset G$ where $\alpha = \varepsilon + \varepsilon^{-1}$. Deduce that the degree of α over $\mathbb{Q}$ is 3.

(f) Compute the minimum polynomial over $\mathbb{Q}$ of α.

(g) Give all subgroups of G and the corresponding fields, both by generators. (You should prove your results but you don't have to say how you found them). Hint: if H is a subgroup of G, use the algorithm of example 81 to find elements of $H^\dagger$.

(h) Prove that $X^2 + 7$ factors completely over L.