(6) As in Example 3, the field $\mathbb{Q}(\sqrt[4]{2})$ is not Galois over $\mathbb{Q}$ since any automorphism is determined by where it sends $\sqrt[4]{2}$ and of the four possibilities $\{\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}\}$, only two are elements of the field (the two real roots).

Note that we have

$$\overbrace{\mathbb{Q} \underbrace{\subset \mathbb{Q}(\sqrt{2})}_{2} \subset \mathbb{Q}(\sqrt[4]{2})}^{4}$$

where $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ are both Galois extensions by Example 2 since both are quadratic extensions. This shows that a Galois extension of a Galois extension is not necessarily Galois.

(7) The extension of finite fields $\mathbb{F}_{p^n}/\mathbb{F}_p$ constructed after Proposition 13.37 is Galois by Corollary 6 since $\mathbb{F}_{p^n}$ is the splitting field over $\mathbb{F}_p$ of the separable polynomial $x^{p^n} - x$. It follows that the group of automorphisms for this extension is of order n. The injective homomorphism

$$\begin{aligned} \sigma : \mathbb{F}_{p^n} &\to \mathbb{F}_{p^n} \\ \alpha &\mapsto \alpha^p \end{aligned}$$

of Proposition 13.35 is surjective in this case since $\mathbb{F}_{p^n}$ is finite, hence is an isomorphism. This gives an automorphism of $\mathbb{F}_{p^n}$, called the *Frobenius* automorphism, which we shall denote by σ_p. Iterating σ_p we have $\sigma_p^2(\alpha) = \sigma_p(\sigma_p(\alpha)) = (\alpha^p)^p = \alpha^{p^2}$. Similarly we have

$$\sigma_p^i(\alpha) = \alpha^{p^i} \qquad i = 0, 1, 2, \ldots$$

Since $\alpha^{p^n} = \alpha$, we see that $\sigma_p^{p^n} = 1$ is the identity automorphism. No lower power of σ_p can be the identity, since this would imply $\alpha^{p^i} = \alpha$ for all $\alpha \in \mathbb{F}_{p^n}$ for some $i < n$, which is impossible since there are only p^i roots of this equation. It follows that σ_p is of order n in the Galois group, which means that $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is *cyclic* of order n, with the Frobenius automorphism σ_p as generator.

(8) The inseparable extension $\mathbb{F}_2(x)$ over $\mathbb{F}_2(t)$ where $x^2 - t = 0$ considered in Section 13.5 is not Galois. Any automorphism of this degree 2 extension is determined by its action on x, which must be sent to a root of the equation $x^2 - t$. We have already seen that there is only one root of this equation (with multiplicity 2) since we are in a field of characteristic 2. Hence the extension has only the trivial automorphism. Note that $\mathbb{F}_2(x)$ is the splitting field for $x^2 - t$ over $\mathbb{F}_2(t)$, so this example shows the separability condition in Corollary 6 is necessary.

EXERCISES

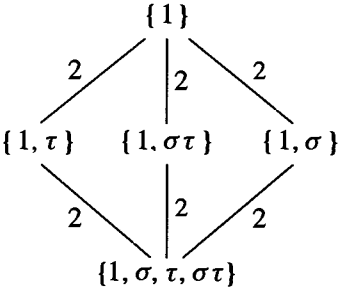
1. (a) Show that if the field K is generated over F by the elements $\alpha_1, \ldots, \alpha_n$ then an automorphism σ of K fixing F is uniquely determined by $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$. In particular show that an automorphism fixes K if and only if it fixes a set of generators for K.

(b) Let $G \leq \mathrm{Gal}(K/F)$ be a subgroup of the Galois group of the extension K/F and suppose $\sigma_1, \ldots, \sigma_k$ are generators for G. Show that the subfield E/F is fixed by G if and only if it is fixed by the generators $\sigma_1, \ldots, \sigma_k$.

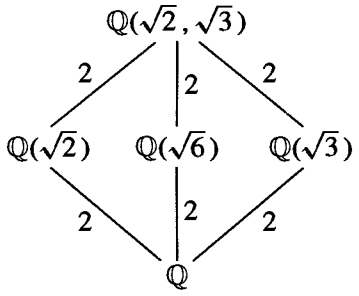
2. Let τ be the map $\tau : \mathbb{C} \to \mathbb{C}$ defined by $\tau(a+bi) = a-bi$ (*complex conjugation*). Prove that τ is an automorphism of $\mathbb{C}$.
3. Determine the fixed field of complex conjugation on $\mathbb{C}$.
4. Prove that $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are not isomorphic.
5. Determine the automorphisms of the extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ explicitly.
6. Let k be a field,
   (a) Show that the mapping $\varphi : k[t] \to k[t]$ defined by $\varphi(f(t)) = f(at+b)$ for fixed $a, b \in k$, $a \neq 0$ is an automorphism of $k[t]$ which is the identity on k.
   (b) Conversely, let φ be an automorphism of $k[t]$ which is the identity on k. Prove that there exist $a, b \in k$ with $a \neq 0$ such that $\varphi(f(t)) = f(at+b)$ as in (a).
7. This exercise determines $\mathrm{Aut}(\mathbb{R}/\mathbb{Q})$.
   (a) Prove that any $\sigma \in \mathrm{Aut}(\mathbb{R}/\mathbb{Q})$ takes squares to squares and takes positive reals to positive reals. Conclude that $a < b$ implies $\sigma a < \sigma b$ for every $a, b \in \mathbb{R}$.
   (b) Prove that $-\frac{1}{m} < a-b < \frac{1}{m}$ implies $-\frac{1}{m} < \sigma a - \sigma b < \frac{1}{m}$ for every positive integer m. Conclude that σ is a continuous map on $\mathbb{R}$.
   (c) Prove that any continuous map on $\mathbb{R}$ which is the identity on $\mathbb{Q}$ is the identity map, hence $\mathrm{Aut}(\mathbb{R}/\mathbb{Q}) = 1$.
8. Prove that the automorphisms of the rational function field $k(t)$ which fix k are precisely the *fractional linear transformations* determined by $t \mapsto \dfrac{at+b}{ct+d}$ for $a, b, c, d \in k, ad-bc \neq 0$ (so $f(t) \in k(t)$ maps to $f(\dfrac{at+b}{ct+d})$) (cf. Exercise 18 of Section 13.2).
9. Determine the fixed field of the automorphism $t \mapsto t+1$ of $k(t)$.
10. Let K be an extension of the field F. Let $\varphi : K \to K'$ be an isomorphism of K with a field K' which maps F to the subfield F' of K'. Prove that the map $\sigma \mapsto \varphi\sigma\varphi^{-1}$ defines a group isomorphism $\mathrm{Aut}(K/F) \xrightarrow{\sim} \mathrm{Aut}(K'/F')$.

14.2 THE FUNDAMENTAL THEOREM OF GALOIS THEORY

In the Galois extension $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ considered in the previous section, there was a strong similarity between the diagram of subgroups of the Galois group:



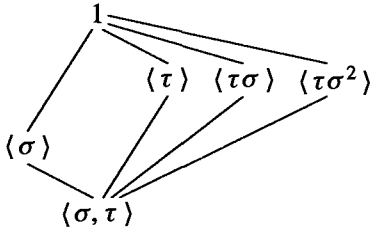
and the diagram of corresponding fixed fields



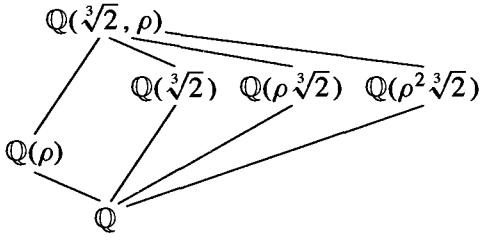
(we have inverted the lattice of subgroups because of the inclusion-reversing nature of the correspondence).

Note that this is also the diagram of *all* known subfields of the extension and that in this case each of the subfields is also a Galois extension of $\mathbb{Q}$.

In a similar way there is a strong similarity between the diagram



of subgroups of the Galois group and the diagram of known subfields for the splitting field of $x^3 - 2$:



where the subfields in the second diagram are precisely the fixed fields of the subgroups in the first diagram.

Note in this pair of diagrams only the subgroup $\langle\sigma\rangle$ generated by σ is normal in S_3 and that the subfield $\mathbb{Q}(\rho)$ is the only subfield Galois over $\mathbb{Q}$.

The Fundamental Theorem of Galois Theory states that the relations observed in the two examples above are not coincidental and hold for any Galois extension. Before proving this we first develop some preliminary results on *group characters*, of which field automorphisms give particular examples.

Definition. A *character*[1] χ of a group G with values in a field L is a homomorphism from G to the multiplicative group of L:

$$\chi : G \to L^\times$$

i.e., $\chi(g_1g_2) = \chi(g_1)\chi(g_2)$ for all $g_1, g_2 \in G$ and $\chi(g)$ is a nonzero element of L for all $g \in G$.

Definition. The characters $\chi_1, \chi_2, \ldots, \chi_n$ of G are said to be *linearly independent* over L if they are linearly independent as functions on G, i.e., if there is no nontrivial relation

$$a_1\chi_1 + a_2\chi_2 + \cdots + a_n\chi_n = 0 \qquad (a_1, \ldots, a_n \in L \text{ not all } 0) \tag{14.2}$$

as a function on G (that is, $a_1\chi_1(g) + a_2\chi_2(g) + \cdots + a_n\chi_n(g) = 0$ for all $g \in G$).

Theorem 7. *(Linear Independence of Characters)* If $\chi_1, \chi_2, \ldots, \chi_n$ are distinct characters of G with values in L then they are linearly independent over L.

Proof: Suppose the characters were linearly dependent. Among all the linear dependence relations (2) above, choose one with the minimal number m of nonzero coefficients a_i. We may suppose (by renumbering, if necessary) that the m nonzero coefficients are $a_1, a_2, \ldots, a_m$:

$$a_1\chi_1 + a_2\chi_2 + \cdots + a_m\chi_m = 0.$$

Then for any $g \in G$ we have

$$a_1\chi_1(g) + a_2\chi_2(g) + \cdots + a_m\chi_m(g) = 0. \tag{14.3}$$

Let g_0 be an element with $\chi_1(g_0) \neq \chi_m(g_0)$ (which exists, since $\chi_1 \neq \chi_m$). Since (3) holds for every element of G, in particular we have

$$a_1\chi_1(g_0g) + a_2\chi_2(g_0g) + \cdots + a_m\chi_m(g_0g) = 0$$

i.e.,

$$a_1\chi_1(g_0)\chi_1(g) + a_2\chi_2(g_0)\chi_2(g) + \cdots + a_m\chi_m(g_0)\chi_m(g) = 0. \tag{14.4}$$

Multiplying equation (3) by $\chi_m(g_0)$ and subtracting from equation (4) we obtain

$$[\chi_m(g_0) - \chi_1(g_0)]a_1\chi_1(g) + [\chi_m(g_0) - \chi_2(g_0)]a_2\chi_2(g) + \cdots + [\chi_m(g_0) - \chi_{m-1}(g_0)]a_{m-1}\chi_{m-1}(g) = 0,$$

which holds for all $g \in G$. But the first coefficient is nonzero and this is a relation with fewer nonzero coefficients, a contradiction.

Consider now an injective homomorphism σ of a field K into a field L, called an *embedding* of K into L. Then in particular σ is a homomorphism of the multiplicative group $G = K^\times$ into the multiplicative group $L^\times$, so σ may be viewed as a character of $K^\times$ with values in L. Note also that this character contains all of the useful information about the values of σ viewed simply as a *function* on K, since the only point of K not considered in $K^\times$ is 0, and we know σ maps 0 to 0.

[1]This is the definition of a *linear* character. More general characters will be studied in Chapter 18.

Corollary 8. If $\sigma_1, \sigma_2, \ldots, \sigma_n$ are distinct embeddings of a field K into a field L, then they are linearly independent as functions on K. In particular distinct automorphisms of a field K are linearly independent as functions on K.

We now use Corollary 8 to prove the fundamental relation between the orders of subgroups of the automorphism group of a field K and the degrees of the extensions over their fixed fields.

Theorem 9. Let $G = \{\sigma_1 = 1, \sigma_2, \ldots, \sigma_n\}$ be a subgroup of automorphisms of a field K and let F be the fixed field. Then

$$[K : F] = n = |G|.$$

Proof: Suppose first that $n > [K : F]$ and let $\omega_1, \omega_2, \ldots, \omega_m$ be a basis for K over F ($m = [K : F]$). Then the system

$$\begin{aligned} \sigma_1(\omega_1)x_1 + \sigma_2(\omega_1)x_2 + \cdots + \sigma_n(\omega_1)x_n &= 0 \\ &\vdots \\ \sigma_1(\omega_m)x_1 + \sigma_2(\omega_m)x_2 + \cdots + \sigma_n(\omega_m)x_n &= 0 \end{aligned}$$

of m equations in n unknowns $x_1, x_2, \ldots, x_n$ has a nontrivial solution $\beta_1, \beta_2, \ldots, \beta_n$ in K since by assumption there are more unknowns than equations.

Let $a_1, a_2, \ldots, a_m$ be m arbitrary elements of F. The field F is by definition fixed by $\sigma_1, \ldots, \sigma_n$ so each of these elements is fixed by every σ_i, i.e., $\sigma_i(a_j) = a_j$, $i = 1, 2, \ldots, n$, $j = 1, 2, \ldots, m$. Multiplying the first equation above by a_1, the second by $a_2, \ldots$, the last by a_m then gives the system of equations

$$\begin{aligned} \sigma_1(a_1\omega_1)\beta_1 + \sigma_2(a_1\omega_1)\beta_2 + \cdots + \sigma_n(a_1\omega_1)\beta_n &= 0 \\ &\vdots \\ \sigma_1(a_m\omega_m)\beta_1 + \sigma_2(a_m\omega_m)\beta_2 + \cdots + \sigma_n(a_m\omega_m)\beta_n &= 0. \end{aligned}$$

Adding these equations we see that there are elements $\beta_1, \ldots, \beta_n$ in K, not all 0, satisfying

$$\sigma_1(a_1\omega_1 + a_2\omega_2 + \cdots + a_m\omega_m)\beta_1 + \cdots + \sigma_n(a_1\omega_1 + a_2\omega_2 + \cdots + a_m\omega_m)\beta_n = 0$$

for all choices of $a_1, \ldots, a_m$ in F. Since $\omega_1, \ldots, \omega_m$ is an F-basis for K, every $\alpha \in K$ is of the form $a_1\omega_1 + a_2\omega_2 + \cdots + a_m\omega_m$, so the previous equation means

$$\sigma_1(\alpha)\beta_1 + \cdots + \sigma_n(\alpha)\beta_n = 0$$

for all $\alpha \in K$. But this means the distinct automorphisms $\sigma_1, \ldots, \sigma_n$ are linearly dependent over K, contradicting Corollary 8.

We have proved $n \leq [K : F]$. Note that we have so far not used the fact that $\sigma_1, \sigma_2, \ldots, \sigma_n$ are the elements of a *group*.

Suppose now that $n < [K : F]$. Then there are more than n F-linearly independent elements of K, say $\alpha_1, \ldots, \alpha_{n+1}$. The system

$$\begin{aligned} \sigma_1(\alpha_1)x_1 + \sigma_1(\alpha_2)x_2 + \cdots + \sigma_1(\alpha_{n+1})x_{n+1} &= 0 \\ &\vdots \\ \sigma_n(\alpha_1)x_1 + \sigma_n(\alpha_2)x_2 + \cdots + \sigma_n(\alpha_{n+1})x_{n+1} &= 0 \end{aligned} \tag{14.5}$$