K to F to be

$$\mathrm{N}_{K/F}(\alpha)=\prod_{\sigma}\sigma(\alpha),$$

where the product is taken over all the embeddings of K into an algebraic closure of F (so over a set of coset representatives for H in $\mathrm{Gal}(L/F)$ by the Fundamental Theorem of Galois Theory). This is a product of Galois conjugates of α. In particular, if K/F is Galois this is $\prod_{\sigma\in\mathrm{Gal}(K/F)}\sigma(\alpha)$.

(a) Prove that $\mathrm{N}_{K/F}(\alpha)\in F$.

(b) Prove that $\mathrm{N}_{K/F}(\alpha\beta)=\mathrm{N}_{K/F}(\alpha)\mathrm{N}_{K/F}(\beta)$, so that the norm is a multiplicative map from K to F.

(c) Let $K=F(\sqrt{D})$ be a quadratic extension of F. Show that $\mathrm{N}_{K/F}(a+b\sqrt{D})=a^2-Db^2$.

(d) Let $m_\alpha(x)=x^d+a_{d-1}x^{d-1}+\cdots+a_1x+a_0\in F[x]$ be the minimal polynomial for $\alpha\in K$ over F. Let $n=[K:F]$. Prove that d divides n, that there are d distinct Galois conjugates of α which are all repeated n/d times in the product above and conclude that $\mathrm{N}_{K/F}(\alpha)=(-1)^n a_0^{n/d}$.

18. With notation as in the previous problem, define the *trace* of α from K to F to be

$$\mathrm{Tr}_{K/F}(\alpha)=\sum_{\sigma}\sigma(\alpha),$$

a sum of Galois conjugates of α.

(a) Prove that $\mathrm{Tr}_{K/F}(\alpha)\in F$.

(b) Prove that $\mathrm{Tr}_{K/F}(\alpha+\beta)=\mathrm{Tr}_{K/F}(\alpha)+\mathrm{Tr}_{K/F}(\beta)$, so that the trace is an additive map from K to F.

(c) Let $K=F(\sqrt{D})$ be a quadratic extension of F. Show that $\mathrm{Tr}_{K/F}(a+b\sqrt{D})=2a$.

(d) Let $m_\alpha(x)$ be as in the previous problem. Prove that $\mathrm{Tr}_{K/F}(\alpha)=-\dfrac{n}{d}a_{d-1}$.

19. With notation as in the previous problems show that $\mathrm{N}_{K/F}(a\alpha)=a^n\mathrm{N}_{K/F}(\alpha)$ and $\mathrm{Tr}_{K/F}(a\alpha)=a\mathrm{Tr}_{K/F}(\alpha)$ for all a in the base field F. In particular show that $\mathrm{N}_{K/F}(a)=a^n$ and $\mathrm{Tr}_{K/F}(a)=na$ for all $a\in F$.

20. With notation as in the previous problems show more generally that $\prod_\sigma(x-\sigma(\alpha))=(m_\alpha(x))^{n/d}$.

21. Use the linear independence of characters to show that for any Galois extension K of F there is an element $\alpha\in K$ with $\mathrm{Tr}_{K/F}(\alpha)\neq 0$.

22. Suppose K/F is a Galois extension and let σ be an element of the Galois group.

(a) Suppose $\alpha\in K$ is of the form $\alpha=\dfrac{\beta}{\sigma\beta}$ for some nonzero $\beta\in K$. Prove that $\mathrm{N}_{K/F}(\alpha)=1$.

(b) Suppose $\alpha\in K$ is of the form $\alpha=\beta-\sigma\beta$ for some $\beta\in K$. Prove that $\mathrm{Tr}_{K/F}(\alpha)=0$.

The next exercise and Exercise 26 following establish the multiplicative and additive forms of Hilbert's Theorem 90. These are instances of the vanishing of a first cohomology group, as will be discussed in Section 17.3.

23. (*Hilbert's Theorem 90*) Let K be a Galois extension of F with cyclic Galois group of order n generated by σ. Suppose $\alpha\in K$ has $\mathrm{N}_{K/F}(\alpha)=1$. Prove that α is of the form $\alpha=\dfrac{\beta}{\sigma\beta}$ for some nonzero $\beta\in K$. [By the linear independence of characters show there exists some $\theta\in K$ such that

$$\beta=\theta+\alpha\sigma(\theta)+(\alpha\sigma\alpha)\sigma^2(\theta)+\cdots+(\alpha\sigma\alpha\ldots\sigma^{n-2}\alpha)\sigma^{n-1}(\theta)$$

is nonzero. Compute $\frac{\beta}{\sigma\beta}$ using the fact that α has norm 1 to F.]

24. Prove that the rational solutions $a, b \in \mathbb{Q}$ of Pythagoras' equation $a^2 + b^2 = 1$ are of the form $a = \frac{s^2 - t^2}{s^2 + t^2}$ and $b = \frac{2st}{s^2 + t^2}$ for some $s, t \in \mathbb{Q}$ and hence show that any right triangle with integer sides has sides of lengths $(m^2 - n^2, 2mn, m^2 + n^2)$ for some integers m, n. [Note that $a^2 + b^2 = 1$ is equivalent to $N_{\mathbb{Q}(i)/\mathbb{Q}}(a + ib) = 1$, then use Hilbert's Theorem 90 above with $\beta = s + it$.]

25. Generalize the previous problem to determine all the rational solutions of the equation $a^2 + Db^2 = 1$ for $D \in \mathbb{Z}$, $D > 0$, D not a perfect square in $\mathbb{Z}$.

26. (*Additive Hilbert's Theorem 90*) Let K be a Galois extension of F with cyclic Galois group of order n generated by σ. Suppose $\alpha \in K$ has $\mathrm{Tr}_{K/F}(\alpha) = 0$. Prove that α is of the form $\alpha = \beta - \sigma\beta$ for some $\beta \in K$. [Let $\theta \in K$ be an element with $\mathrm{Tr}_{K/F}(\theta) \neq 0$ by a previous exercise, let

$$\beta = \frac{1}{\mathrm{Tr}_{K/F}(\theta)}[\alpha\sigma(\theta) + (\alpha + \sigma\alpha)\sigma^2(\theta) + \cdots + (\alpha + \sigma\alpha + \cdots + \sigma^{n-2}\alpha)\sigma^{n-1}(\theta)]$$

and compute $\beta - \sigma\beta$.]

27. Let $\alpha = \sqrt{(2 + \sqrt{2})(3 + \sqrt{3})}$ (positive real square roots for concreteness) and consider the extension $E = \mathbb{Q}(\alpha)$.

(a) Show that $a = (2 + \sqrt{2})(3 + \sqrt{3})$ is not a square in $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. [If $a = c^2$, $c \in F$, then $a\varphi(a) = (2 + \sqrt{2})^2(6) = (c\varphi c)^2$ for the automorphism $\varphi \in \mathrm{Gal}(F/\mathbb{Q})$ fixing $\mathbb{Q}(\sqrt{2})$. Since $c\varphi c = N_{F/\mathbb{Q}(\sqrt{2})}(c) \in \mathbb{Q}(\sqrt{2})$ conclude that this implies $\sqrt{6} \in \mathbb{Q}(\sqrt{2})$, a contradiction.]

(b) Conclude from (a) that $[E : \mathbb{Q}] = 8$. Prove that the roots of the minimal polynomial over $\mathbb{Q}$ for α are the 8 elements $\pm\sqrt{(2 \pm \sqrt{2})(3 \pm \sqrt{3})}$.

(c) Let $\beta = \sqrt{(2 - \sqrt{2})(3 + \sqrt{3})}$. Show that $\alpha\beta = \sqrt{2}(3 + \sqrt{3}) \in F$ so that $\beta \in E$. Show similarly that the other roots are also elements of E so that E is a Galois extension of $\mathbb{Q}$. Show that the elements of the Galois group are precisely the maps determined by mapping α to one of the eight elements in (b).

(d) Let $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$ be the automorphism which maps α to β. Show that since $\sigma(\alpha^2) = \beta^2$ that $\sigma(\sqrt{2}) = -\sqrt{2}$ and $\sigma(\sqrt{3}) = \sqrt{3}$. From $\alpha\beta = \sqrt{2}(3 + \sqrt{3})$ conclude that $\sigma(\alpha\beta) = -\alpha\beta$ and hence $\sigma(\beta) = -\alpha$. Show that σ is an element of order 4 in $\mathrm{Gal}(E/\mathbb{Q})$.

(e) Show similarly that the map τ defined by $\tau(\alpha) = \sqrt{(2 + \sqrt{2})(3 - \sqrt{3})}$ is an element of order 4 in $\mathrm{Gal}(E/\mathbb{Q})$. Prove that σ and τ generate the Galois group, $\sigma^4 = \tau^4 = 1$, $\sigma^2 = \tau^2$ and that $\sigma\tau = \tau\sigma^3$.

(f) Conclude that $\mathrm{Gal}(E/\mathbb{Q}) \cong Q_8$, the quaternion group of order 8.

28. Let $f(x) \in F[x]$ be an irreducible polynomial of degree n over the field F, let L be the splitting field of $f(x)$ over F and let α be a root of $f(x)$ in L. If K is any Galois extension of F contained in L, show that the polynomial $f(x)$ splits into a product of m irreducible polynomials each of degree d over K, where $m = [F(\alpha) \cap K : F]$ and $d = [K(\alpha) : K]$ (cf. also the generalization in Exercise 4 of Section 4). [If H is the subgroup of the Galois group of L over F corresponding to K then the factors of $f(x)$ over K correspond to the orbits of H on the roots of $f(x)$. Then use Exercise 9 of Section 4.1.]

29. Let k be a field and let $k(t)$ be the field of rational functions in the variable t. Define the maps σ and τ of $k(t)$ to itself by $\sigma f(t) = f(\frac{1}{1-t})$ and $\tau f(t) = f(\frac{1}{t})$ for $f(t) \in k(t)$.

(a) Prove that σ and τ are automorphisms of $k(t)$ (cf. Exercise 8 of Section 1) and that the group $G = \langle \sigma, \tau \rangle$ they generate is isomorphic to S_3.

(b) Prove that the element $t = \dfrac{(t^2 - t + 1)^3}{t^2(t-1)^2}$ is fixed by all the elements of G.

(c) Prove that $k(t)$ is precisely the fixed field of G in $k(t)$ [compute the degree of the extension].

30. Prove that the fixed field of the subgroup of automorphisms generated by τ in the previous problem is $k(t + \frac{1}{t})$. Prove that the fixed field of the subgroup generated by the automorphism $\tau\sigma^2$ (which maps t to $1-t$) is $k(t(1-t))$. Determine the fixed field of the subgroup generated by $\tau\sigma$ and the fixed field of the subgroup generated by σ.

31. Let K be a finite extension of F of degree n. Let α be an element of K.

(a) Prove that α acting by left multiplication on K is an F-linear transformation T_α of K.

(b) Prove that the minimal polynomial for α over F is the same as the minimal polynomial for the linear transformation T_α.

(c) Prove that the trace $\mathrm{Tr}_{K/F}(\alpha)$ is the trace of the $n \times n$ matrix defined by T_α (which justifies these two uses of the same word "trace"). Prove that the norm $\mathrm{N}_{K/F}(\alpha)$ is the determinant of T_α.

14.3 FINITE FIELDS

A finite field $\mathbb{F}$ has characteristic p for some prime p so is a finite dimensional vector space over $\mathbb{F}_p$. If the dimension is n, i.e., $[\mathbb{F} : \mathbb{F}_p] = n$, then $\mathbb{F}$ has precisely p^n elements. We have already seen (following Proposition 13.37) that $\mathbb{F}$ is then isomorphic to the splitting field of the polynomial $x^{p^n} - x$, hence is unique up to isomorphism. We denote the finite field of order p^n by $\mathbb{F}_{p^n}$.

The field $\mathbb{F}_{p^n}$ is Galois over $\mathbb{F}_p$, with cyclic Galois group of order n generated by the Frobenius automorphism

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \sigma_p \rangle \cong \mathbb{Z}/n\mathbb{Z}$$

where

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

(Example 7 following Corollary 6). By the Fundamental Theorem, every subfield of $\mathbb{F}_{p^n}$ corresponds to a subgroup of $\mathbb{Z}/n\mathbb{Z}$. Hence for every divisor d of n there is precisely one subfield of $\mathbb{F}_{p^n}$ of degree d over $\mathbb{F}_p$, namely the fixed field of the subgroup generated by σ_p^d of order n/d, and there are no other subfields. This field is isomorphic to $\mathbb{F}_{p^d}$, the unique finite field of order p^d.

Since the Galois group is abelian, every subgroup is normal, so each of the subfields $\mathbb{F}_{p^d}$ (d a divisor of n) is Galois over $\mathbb{F}_p$ (which is also clear from the fact that these are themselves splitting fields). Further, the Galois group $\mathrm{Gal}(\mathbb{F}_{p^d}/\mathbb{F}_p)$ is generated by the image of σ_p in the quotient group $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)/\langle \sigma_p^d \rangle$. If we denote this element