SOLUTIONS TO WORKSHEET #6

Problem 1. — *Prove that* $\mathrm{Aut}_{\mathbf{F}_q}(\bar{\mathbf{F}}_q)$ *is an abelian group and that every element has infinite order.*

Solution. What is the algebraic closure of a field F? By definition, it is a field extension of F over which every polynomial with coefficients in F splits, and that this extension should be minimal for this property, meaning that there is no proper subfield which also splits all polynomials of F. Somewhat remarkably, algebraic closures exist in general, the rough idea of the construction being that you simply adjoin all roots of all polynomials over F. One way to make this precise is to choose a way to write the polynomial ring over F

$$F[x] = \bigcup_{\Lambda \subset F[x] \text{ finite}} \Lambda$$

as an increasing union of finite subsets $\Lambda \subset F[x]$; for instance, for a finite field $\mathbf{F}_q$, we could write

$$\mathbf{F}_q[x] = \bigcup_{d \geq 1} \mathbf{F}_q[x]_{\leq d}$$

as the increasing union of all polynomials of degrees at most d. With such a choice, an algebraic closure may be taken as the increasing union

$$\bar{F} = \bigcup_{\Lambda \subset F[x] \text{ finite}} \mathrm{SF}_F(\Lambda)$$

of the splitting fields of Λ. Since the sets Λ are nested, there are containment relations amongst the splitting fields, and so the union makes sense. Zorn's lemma then provides an upper bound, and this is $\bar{F}$. Notice that there are many choices involved in this construction, and so algebraic closures are not unique. But one may show that any two algebraic closures are isomorphic, and for this reasons we usually refer to any choice of an algebraic closure as *the* algebraic closure.

Typically, the extension $F \subset \bar{F}$ is very large, and tools for analyzing finite extensions may not directly apply. However, each $\alpha \in \bar{F}$ is defined over a finite extension of F in the sense that there is an intermediate field extension $F \subset L \subset \bar{F}$ such that $\alpha \in L$: Indeed, in the construction above, α is a root of a polynomial in one of the finite sets $\Lambda \subset F[x]$, so take $L := \mathrm{SF}_F(\Lambda)$. In this way, questions about $\bar{F}$ may be reduced, at least element-wise, to finite extensions of F.

On with the problem: We would like to show that the group $\mathrm{Aut}_{\mathbf{F}_q}(\bar{\mathbf{F}}_q)$ of $\mathbf{F}_q$-automorphisms of its algebraic closure is an abelian group. So given any pair $\mathbf{F}_q$-automorphisms $\sigma, \tau : \bar{\mathbf{F}}_q \to \bar{\mathbf{F}}_q$, we would like to show that the two composites

$$\sigma \circ \tau : \bar{\mathbf{F}}_q \to \bar{\mathbf{F}}_q \text{ and } \tau \circ \sigma : \bar{\mathbf{F}}_q \to \bar{\mathbf{F}}_q$$

are the same $\mathbf{F}_q$-automorphisms. What does this mean? Well, these are two functions on the set $\bar{\mathbf{F}}_q$, and two functions are the same if and only if their values on every element of $\bar{\mathbf{F}}_q$ coincide. In other words, we would like to show that

$$\sigma \circ \tau(\alpha) = \tau \circ \sigma(\alpha) \text{ for all } \alpha \in \bar{\mathbf{F}}_q.$$

As explained above, there is a intermediate field extension $\mathbf{F}_q \subseteq \mathbf{F}_{q^n} \subset \bar{\mathbf{F}}_q$ which is finite over the base such that $\alpha \in \mathbf{F}_{q^n}$. Now observe that any $\varphi \in \mathrm{Aut}_{\mathbf{F}_q}(\bar{\mathbf{F}}_q)$ preserves the subfield $\mathbf{F}_{q^n} \subset \bar{\mathbf{F}}_q$. Indeed, write $\mathbf{F}_{q^n}$ as the splitting field of some finite set $\Lambda \subset \mathbf{F}_q[x]$ of polynomials with coefficients in $\mathbf{F}_q$. Since φ fixes $\mathbf{F}_q$, it also fixes the set Λ in that

$$\Lambda^\varphi := \{\varphi^{-1}(a_0) + \varphi^{-1}(a_1)x + \cdots + \varphi^{-1}(a_n)x^n : a_0 + a_1 x + \cdots + a_n x^n \in \Lambda\} = \Lambda,$$

Date: October 30, 2025.

and so

$$\varphi(\mathbf{F}_{q^n}) = \varphi(\mathrm{SF}_{\mathbf{F}_q}(\Lambda)) = \mathrm{SF}_{\mathbf{F}_q}(\Lambda^\varphi) = \mathrm{SF}_{\mathbf{F}_q}(\Lambda) = \mathbf{F}_{q^n}.$$

Note that this does not mean that φ fixes $\mathbf{F}_{q^n}$ element-wise, just that any element of $\mathbf{F}_{q^n}$ gets sent back to an element of $\mathbf{F}_{q^n}$!

The property $\sigma(\mathbf{F}_{q^n}) = \mathbf{F}_{q^n}$ means that there is a well-defined restriction homomorphism

$$\mathrm{Aut}_{\mathbf{F}_q}(\bar{\mathbf{F}}_q) \to \mathrm{Gal}(\mathbf{F}_{q^n}/\mathbf{F}_q) \colon \varphi \mapsto \varphi|_{\mathbf{F}_{q^n}}.$$

In a previous problem set, we have seen that $\mathrm{Gal}(\mathbf{F}_{q^n}/\mathbf{F}_q) \cong C_{n-1}$ is a cyclic group, whence abelian. So, returning to the automorphisms σ and τ, and the element $\alpha \in \mathbf{F}_{q^n} \subset \bar{\mathbf{F}}_q$, we have

$$\sigma \circ \tau(\alpha) = \sigma|_{\mathbf{F}_{q^n}} \circ \tau|_{\mathbf{F}_{q^n}}(\alpha) = \tau|_{\mathbf{F}_{q^n}} \circ \sigma|_{\mathbf{F}_{q^n}}(\alpha) = \tau \circ \sigma(\alpha).$$

Since we can do this for any $\alpha \in \bar{\mathbf{F}}_q$, $\sigma \circ \tau = \tau \circ \sigma$, and so $\mathrm{Aut}_{\mathbf{F}_q}(\bar{\mathbf{F}}_q)$ is abelian.

The existence of the restriction maps $\mathrm{Aut}_{\mathbf{F}_q}(\bar{\mathbf{F}}_q) \to \mathrm{Gal}(\mathbf{F}_{q^n}/\mathbf{F}_q) \cong C_{n-1}$ for all $n \geq 1$ implies much more: for instance, it implies that any nontrivial element of $\mathrm{Aut}_{\mathbf{F}_q}(\bar{\mathbf{F}}_q)$ must have infinite order. Indeed, given a nontrivial $\mathbf{F}_q$-automorphism $\sigma \colon \bar{\mathbf{F}}_q \to \bar{\mathbf{F}}_q$, let $\mathbf{F}_{q^n}$ be any finite subextension on which the restriction

$$\sigma|_{\mathbf{F}_{q^n}} \in \mathrm{Gal}(\mathbf{F}_{q^n}/\mathbf{F}_q) \cong C_{n-1}$$

is nontrivial. On a previous set, we showed that the cyclic group C_{n-1} is generated by the q-power Frobenius automorphism $\mathrm{Fr} \colon \mathbf{F}_{q^n} \to \mathbf{F}_{q^n}$. Thus $\sigma|_{\mathbf{F}_{q^n}} = \mathrm{Fr}^e$ is the q^e-power Frobenius for some integer $0 < e < n-1$. Since restriction preserves the Frobenius map, this means that for any intermediate finite field $\mathbf{F}_{q^n} \subset \mathbf{F}_{q^m} \subset \bar{\mathbf{F}}_q$, the restriction of σ to $\mathbf{F}_{q^m}$ also acts as the q^e-power Frobenius. But the order of $\sigma|_{\mathbf{F}_{q^m}} = \mathrm{Fr}^e$ in $\mathrm{Gal}(\mathbf{F}_{q^m}/\mathbf{F}_q) \cong C_{m-1}$ is $(m-1)/\gcd(e, m-1)$ and this grows arbitrarily large as m grows. This is only possible if σ itself is of infinite order in $\mathrm{Gal}(\bar{\mathbf{F}}_q/\mathbf{F}_q)$. ■

Problem 2. — *Let $G \neq \{1\}$ be a finite abelian group.*

(i) *Prove that there exists a Galois extension $L/\mathbf{Q}$ such that $\mathrm{Gal}(L/\mathbf{Q}) \simeq G$.*

(ii) *Let $K/\mathbf{Q}$ be a finite extension. Prove that there exist infinitely many Galois extensions L/K such that $\mathrm{Gal}(L/K) \simeq G$.*

Solution. Write $G \cong C_{q_1} \times \cdots \times C_{q_s}$ as a product of prime power cyclic groups. Applying Dirichlet's theorem on the infinitude of primes in arithmetic progression to the sequences $(aq_i + 1)_{a \geq 1}$ shows that there exists primes p_i such that $q_i \mid p_i - 1$. Consider now the cyclotomic extension $\mathbf{Q} \subset \mathbf{Q}(\omega)$ where ω is a primitive n-th root of unity

$$n := p_1 \cdots p_s \text{ so that } \mathrm{Gal}(\mathbf{Q}(\omega)/\mathbf{Q}) \cong (\mathbf{Z}/n\mathbf{Z})^\times \cong C_{p_1-1} \times \cdots \times C_{p_s-1},$$

the latter isomorphism due to the Chinese remainder theorem. The divisibility relation ensures that C_{q_i} is a quotient of C_{p_i-1} for each $1 \leq i \leq s$, meaning that G is a quotient of $\mathrm{Gal}(\mathbf{Q}(\omega)/\mathbf{Q})$. The fundamental theorem of Galois theory thus provides an intermediate extension $\mathbf{Q} \subset L \subset \mathbf{Q}(\omega)$ satisfying $\mathrm{Gal}(L/\mathbf{Q}) \cong G$.

Suppose now that we are given a finite extension $\mathbf{Q} \subset K$. Then K contains only finitely many roots of unity; in particular, there exists an integer $N \geq 1$ such that K does not contain any primitive n-th root of unity for $n \geq N$. Thus is ω is a primitive n-th root of unity for $n = p_1 \cdots p_s$ as above, this time with the extra stipulation that $p_i \geq N$ for each $1 \leq i \leq s$, then the extension $K(\omega)$ satisfies

$$\mathrm{Gal}(K(\omega)/K) \cong \mathrm{Gal}(\mathbf{Q}(\omega)/\mathbf{Q}) \cong C_{p_1-1} \times \cdots \times C_{p_s-1}$$

at which point an intermediate field extension $K \subset L \subset K(\omega)$ with Galois group G can be found as above. Since there are infinitely many different choices of the p_i by Dirichlet's theorem, and each

extension L is generated by different roots of unity for distinct prime products, this gives infinitely many distinct Galois extensions with the same Galois group G. ■

Problem 3. — *Let K be a field such that every finite extension L/K is cyclic. Show that there exists $\sigma \in \mathrm{Aut}_K(\bar{K})$ such that $K = \bar{K}^\sigma = \{x \in \bar{K} : \sigma(x) = x\}$.*

Solution. How to describe the group $\mathrm{Aut}_K(\bar{K})$? In Problem 1, properties of elements $\sigma : \bar{K} \to \bar{K}$ were understood by restricting it to various finite subextensions $K \subset L \subset \bar{K}$. Since every element of $\bar{K}$ is contained in some finite subextension, this suggests that σ is also determined by knowing how it restricts to each such L! How to make sense of this?

To a first approximation, it appears that to specify an element $\sigma \in \mathrm{Aut}_K(\bar{K})$, it ought to be enough to specify its restriction $\sigma_L \in \mathrm{Gal}(L/K)$ for every finite subextension $K \subset L \subset \bar{K}$. In other words, the data of σ should be the same as the data of the tuple

$$(\sigma_L)_L \in \prod\nolimits_{K \subset L \text{ finite}} \mathrm{Gal}(L/K)$$

consisting of its purported restrictions to each finite extension $K \subset L$. This, however, neglects a basic compatibility: if there were a tower of finite field extensions $K \subset F \subset L$, then the restriction of σ first to L and then to F should be the same as the restriction of σ directly to F! In symbols, writing

$$\rho_L : \mathrm{Aut}_K(\bar{K}) \to \mathrm{Gal}(L/K), \;\; \rho_F : \mathrm{Aut}_K(\bar{K}) \to \mathrm{Gal}(F/K), \;\; \rho_{L,F} : \mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K)$$

for the restriction maps, we ought to have $\rho_{L,F}(\rho_L(\sigma)) = \rho_F(\sigma)$. Thus the tuple $(\sigma_L)_L$ cannot be an arbitrary tuple of elements in the product, but one that satisfies the additional compatibility condition

$$\rho_{L,F}(\sigma_L) = \sigma_F \;\text{ for every tower } K \subset F \subset L \text{ of finite extensions.}$$

Since the restriction maps are group homomorphisms, the set

$$G := \left\{(\sigma_L)_L \in \prod\nolimits_{K \subset L} \mathrm{Gal}(L/K) : \rho_{L,F}(\sigma_L) = \sigma_F \;\text{ for every } K \subset F \subset L\right\}$$

is a subgroup of the big product. Moreover, the comments above imply that the product of restriction maps $\mathrm{Aut}_K(\bar{K}) \to \prod_{L \subset K} \mathrm{Gal}(L/K)$ factors through this subgroup G. In other words, the product of the restriction maps provides a group homomorphism

$$\rho : \mathrm{Aut}_K(\bar{K}) \to G.$$

This map is an isomorphism: Injectivity follows from the fact that an element of $\mathrm{Aut}_K(\bar{K})$ is the identity if and only if its restriction to every finite subextension $K \subset L$ is the identity. As for surjectivity, well, think about what it means to specify an element of $\mathrm{Aut}_K(\bar{K})$: Given the tuple $(\sigma_L)_L$, define a K-automorphism $\sigma : \bar{K} \to \bar{K}$ by setting

$$\sigma(x) = \sigma_L(x) \;\text{ for every } x \in L \subset \bar{K}.$$

That is, given an element $x \in \bar{K}$, choose a finite extension $K \subset L$ in which it lies, and take $\sigma(x)$ just to be $\sigma_L(x)$. We must show that this is well-defined in that the choice of finite extension L containing x is immaterial. So let $K \subset L'$ be another one containing x. Then x actually lies in a common subextension $F := L \cap L'$. Compatibility of the tuple $(\sigma_L)_L$ with restrictions means that, in more familiar and suggestive notation, $\sigma_L|_F = \sigma_F = \sigma_{L'}|_F$, and so

$$\sigma_L(x) = \sigma_F(x) = \sigma_{L'}(x).$$

Therefore $\sigma(x)$ above is well-defined, establishing surjectivity of ρ.

Finally, to address the Problem: If each finite extension $K \subset L$ were cyclic, then I claim there is an element $(\sigma_L)_L \in G$ in the group constructed above where $\sigma_L \in \mathrm{Gal}(L/K)$ is a cyclic generator. Since $L^{\sigma_L} = K$, if such an element were to exist, then the corresponding element $\sigma \in \mathrm{Aut}_K(\bar{K})$ would also satisfy $\bar{K}^\sigma = K$, as required. That the compatible sequence of generators exists in G can be deduced

from the following fact about cyclic groups: If $\phi : C_n \to C_m$ is a surjective homomorphism of cyclic groups, then a generator of C_n maps to a generator of C_m; conversely, every generator of C_m is the image of a generator of C_n. ■

Problem 4. — *Let L/K be a Galois extension with Galois group G. Define the trace map*

$$\mathrm{Tr}_{L/K} : L \to L \qquad \ell \mapsto \sum_{g \in G} g(\ell)$$

(i) *Prove that* $\mathrm{im}(\mathrm{Tr}_{L/K}) \subset K$ *and* $\mathrm{Tr}_{L/K}$ *is K-linear.*

(ii) *Assume that* $[L : K] = |G| = n$ *and* $G = \langle \sigma \rangle$ *is cyclic and prove that* $\ker(\mathrm{Tr}_{L/K}) = \mathrm{im}(\sigma - \mathrm{id}_L)$.

Solution. For (i), note that for any $h \in G$ and $\ell \in L$,

$$h(\mathrm{Tr}_{L/K}(\ell)) = \sum_{g \in G} h(g(\ell)) = \sum_{g \in h \cdot G} g'(\ell) = \sum_{g \in G} g(\ell) = \mathrm{Tr}_{L/K}(\ell)$$

since multiplication by h provides a bijection of G onto itself. Since $\mathrm{Tr}_{L/K}(\ell)$ is fixed by the action of all elements of G, it lies in K. Since $\ell \in L$ was arbitrary, this means that $\mathrm{im}(\mathrm{Tr}_{L/K}) \subseteq K$. To see that $\mathrm{Tr}_{L/K}$ is K-linear, simply observe that each $g \in G$ is a K-linear map of L and that a sum of K-linear maps is still K-linear.

For (ii), in the case G is cyclic of order n, choose a generator σ and write $G = \langle \sigma \rangle = \{\mathrm{id}_L, \sigma, \ldots, \sigma^{n-1}\}$. Then the trace of $\ell \in L$ may be expressed as

$$\mathrm{Tr}_{L/K}(\ell) = \sum_{i=0}^{n-1} \sigma^i(\ell)$$

With this, it is straightforward to see that $\mathrm{im}(\sigma - \mathrm{id}_L) \subseteq \ker(\mathrm{Tr}_{L/K})$:

$$\mathrm{Tr}_{L/K} \circ (\sigma - \mathrm{id}_L)(\ell) = \sum_{i=0}^{n-1} \sigma^{i+1}(\ell) - \sum_{i=0}^{n-1} \sigma(\ell) = \sigma^n(\ell) - \ell = 0.$$

In fact, $\mathrm{im}(\sigma - \mathrm{id}_L) = \ker(\mathrm{Tr}_{L/K})$: Both functions are K-linear operators on L, and so the spaces in question are K-vector spaces. Therefore, with the containment relation, it suffices to see that the two spaces have the same dimension over K. For the image:

$$\dim_K \mathrm{im}(\sigma - \mathrm{id}_L) = \dim_K L - \dim_K \ker(\sigma - \mathrm{id}_L) = n - 1$$

since $\ker(\sigma - \mathrm{id}_L) = \{\ell \in L : \sigma(\ell) = \ell\} = L^\sigma = K$. For the trace, use (i) and view it as a K-linear functional $\mathrm{Tr}_{L/K} : L \to K$. It now suffices to show that $\mathrm{Tr}_{L/K}$ is a nonzero map, upon which we see that the trace is in fact surjective and its kernel must have dimension $n-1$, matching that of the image of $\sigma - \mathrm{id}_L$. When $n = \#G$ is not divisible by the characteristic $p := \mathrm{char}\, K$, this is quite easy since, for any $x \in K^\times$,

$$\mathrm{Tr}_{L/K}(x) = \sum_{i=0}^{n-1} \sigma^i(x) = \sum_{i=0}^{n-1} x = nx \neq 0.$$

When $p \mid n$, we have to work a bit harder to find an element not in the kernel of the trace.

Consider first the case where $n = p$. Artin–Schreier theory shows that the extension $K \subset L$ is of the form $L = K(\alpha)$ where α is a root of an irreducible polynomial of the form $f(x) = x^p - x - c \in K[x]$. Furthermore, the Galois group $G = \langle \sigma \rangle \cong \mathbf{F}_p$ acts by translation on α in the sense that $\sigma^i(\alpha) = \alpha + i$, where $0 \leq i \leq p-1$ is viewed as an element of $\mathbf{F}_p \subset K$. To look for a candidate element with nonzero trace, since $\mathrm{Tr}_{L/K}$ is additive and every element of L is a polynomial of degree $\leq p-1$ in α, we might wish to consider first the traces of powers of α: for each $0 \leq k \leq p-1$,

$$\mathrm{Tr}_{L/K}(\alpha^k) = \sum_{i=0}^{p-1} \sigma^i(\alpha^k) = \sum_{i=0}^{p-1} \sigma^i(\alpha)^k = \sum_{i=0}^{p-1} (\alpha + i)^k$$

and this may be expanded further using the binomial formula. As a first pass, consider the two extreme coefficients of this expression: On the one hand, the highest degree of α is α^j, but this comes

repeated with a coefficient of $p = 0$! On the other hand, the lowest degree in α comes from the sum of powers of the constants $i \in \mathbf{F}_q$, yielding

$$\sum_{i=0}^{p-1} i^k = 0^k + \sum_{i=1}^{p-1} i^k = \sum_{i \in \mathbf{F}_p^\times} i^k.$$

The third expression shows that this sum might be understood as a *character sum* for the finite cyclic group $\mathbf{F}_p^\times \cong C_{p-1}$. General considerations from the representation theory of finite groups then shows that we can arrange for this quantity to be nonzero by choosing a trivial character; in other words, we would like to choose the exponent $0 \leq k \leq p-1$ such that $i^k = 1$ for every $i \in \mathbf{F}_p^\times$. Since $\mathbf{F}_p^\times$ is a finite group of order $p-1$, this can be achieved by taking $k = p-1$. Thus we are led to compute

$$\mathrm{Tr}_{L/K}(\alpha^{p-1}) = \sum_{i=0}^{p-1} (\alpha + i)^{p-1} = \sum_{i=0}^{p-1} (\alpha^{p-1} - i\alpha^{p-2} + \cdots + i^{p-1}) = \sum_{i=1}^{p-1} 1 = p-1,$$

where all the intermediate coefficients sum up to zero because they will be character sums corresponding to nontrivial characters of $\mathbf{F}_p^\times$. In any case, even without knowing exactly what the intermediate coefficients are, it is easy to see that the constant coefficient of $\mathrm{Tr}_{L/K}(\alpha^{p-1})$ is $p-1 \neq 0$, which is enough for our purposes.

In the general case that $p \mid n$, write $n = mp^e$ where $p \nmid m$, and use the fundamental theorem of finitely generated abelian groups to write $G \cong G_1 \times G_2$ where $\#G_1 = m$ and $\#G_2 = p^e$. Repeatedly applying Cauchy's theorem in group theory to G_2 and its quotients provides a sequence of subgroups

$$G =: H_e \supseteq H_{e-1} \supseteq \cdots \supseteq H_1 \supseteq H_0 := \{1\}$$

such that $H_i / H_{i-1} \cong C_p$ for each $1 \leq i \leq e$. Since any subgroup of an abelian group is normal, the fundamental theorem of Galois theory translates all this to a sequence of Galois field extensions

$$F \subset E_e \subset E_{e-1} \subset \cdots \subset E_1 \subset E_0 := L$$

where $\mathrm{Gal}(E_e/F) \cong G_1$ and $\mathrm{Gal}(E_{i-1}/E_i) \cong H_i/H_{i-1} \cong C_p$ for each $1 \leq i \leq p$. We now use the fact that the trace maps $\mathrm{Tr}_{E_e/F}$ and $\mathrm{Tr}_{E_{i-1}/E_i}$ are all surjective in order to construct a sequence of elements $x_i \in E_i$ as follows: Choose an element $x_e \in E_e$ such that $\mathrm{Tr}_{E_e/F}(x_e) = 1$. Now let $0 \leq j \leq e-1$ and inductively suppose that $x_{e-j} \in E_{e-j}$ has been constructed. Take $x_{e-j-1} \in E_{e-j-1}$ to be any element such that

$$\mathrm{Tr}_{E_{e-j-1}/E_{e-j}}(x_{e-j-1}) = x_{e-j}.$$

In this way, we obtain an element $x := x_0 \in E_0 = L$ with the property that

$$\mathrm{Tr}_{E_e/F} \circ \mathrm{Tr}_{E_{e-1}/E_e} \circ \cdots \circ \mathrm{Tr}_{E_1/E_2} \circ \mathrm{Tr}_{L/E_1}(x) = 1.$$

To finally conclude, it remains to show that traces are compatible towers of field extensions, so that we may identify the composition of traces as $\mathrm{Tr}_{L/F}$. More generally, let's show that if $F \subset E \subset L$ is a tower of Galois field extensions, then

$$\mathrm{Tr}_{L/F} = \mathrm{Tr}_{E/F} \circ \mathrm{Tr}_{L/E}.$$

Set $G := \mathrm{Gal}(L/F)$ and $H := \mathrm{Gal}(L/E)$, so that $\mathrm{Gal}(E/F) \cong G/H$. For each $\bar{g} \in G/H$, choose a lift $g \in G$ along the quotient map $G \to G/H$, so that $gH \subseteq H$ is the coset corresponding to $\bar{g}$. Then

$$\mathrm{Tr}_{E/F} \circ \mathrm{Tr}_{L/E}(\ell) = \sum_{\bar{g} \in G/H} \sum_{h \in H} g(h(\ell)) = \sum_{\bar{g} \in G/H} \sum_{h' \in gH} h'(\ell) = \sum_{g' \in G} g'(\ell) = \mathrm{Tr}_{L/F}(\ell)$$

for any $\ell \in L$. Thus $\mathrm{Tr}_{L/F} = \mathrm{Tr}_{E/F} \circ \mathrm{Tr}_{L/E}$, as claimed. ∎

Problem 5. — *Prove that* $\mathbf{Q}(\sqrt[3]{2})$ *is not a subfield of any cyclotomic extension of* $\mathbf{Q}$.

Solution. Suppose that $\mathbf{Q}(\sqrt[3]{2})$ is an intermediate extension of some cyclotomic extension $\mathbf{Q} \subset \mathbf{Q}(\sqrt[3]{2}) \subset \mathbf{Q}(\omega_n)$. The cyclotomic extension itself $\mathbf{Q} \subset \mathbf{Q}(\omega_n)$ is Galois and its Galois group G is abelian. By the Galois correspondence, the subextension $\mathbf{Q}(\sqrt[3]{2})$ corresponds to a subgroup $H \subseteq G$. Since G is abelian, the subgroup H is also normal in G. But the main theorem of Galois theory then implies that the extension $\mathbf{Q} \subset \mathbf{Q}(\sqrt[3]{2})$ is Galois with group G/H—this contradicts the fact that $\mathbf{Q}(\sqrt[3]{2})$ is not normal over $\mathbf{Q}$, as was seen on a previous problem set. ■

Problem 6. — *Let $f \in \mathbf{Q}[x]$ be a cubic polynomial such that $\mathrm{Gal}(\mathrm{SF}_{\mathbf{Q}}(f)/\mathbf{Q}) = C_3$. Prove that all the roots of f are real.*

Solution. A cubic polynomial with real coefficients always has at least one real root. Suppose that at least one α of the remaining two roots of f were non-real. Then since f has real coefficients, this implies that the remaining root must be the complex conjugate $\bar{\alpha}$, whence non-real. But this implies that $\mathrm{Gal}(\mathrm{SF}_{\mathbf{Q}}(f)/\mathbf{Q})$ contains complex conjugation, whence an element of order 2. This is, of course, not possible if the group is isomorphic to the cyclic group C_3. ■

Problem 7. — *Let L/K be a cyclic extension of degree three of fields of characteristic not equal to two. Write $G = \mathrm{Gal}(L/K) = \{1, \sigma, \sigma^2\}$ and for $\beta \in L$ define the norm map*

$$\mathrm{Nm}_{L/K}(\beta) := \prod\nolimits_{g \in G} g(\beta) = \beta \cdot \sigma(\beta) \cdot \sigma^2(\beta).$$

Fix $\beta \in L^\times \setminus K^\times$ not a square with $\mathrm{Nm}_{L/K}(\beta) = 1$ and let α be a root of $x^2 - \beta$.

(i) *Prove that the normal closure of $L(\alpha)$ over K is a Galois extension of K with Galois group A_4.*

(ii) *Let now $L = \mathbf{Q}(\zeta_7 + \zeta_7^{-1})$ and $K = \mathbf{Q}$, where ζ_7 is a primitive 7-th root of unity. Then, L/K is a cubic cyclic extension. Check that $\beta = \zeta_7 + \zeta_7^{-1}$ has the properties outlined above.*

Solution. How might $L(\alpha)$ not be normal over K? Well, let's try to find a polynomial over K which is satisfied by α, and let's try to see whether there are some further roots we need to add. Since $\beta = \alpha^2$, the thing we ought to look at is the minimal polynomial of β over K:

$$f(x) = (x - \beta)(x - \sigma(\beta))(x - \sigma^2(\beta)) = x^3 + ax^2 + bx + 1$$

for some $a, b \in K$. Substituting x^2 for the variable, we have a polynomial

$$g(x) := f(x^2) = x^6 + ax^4 + bx^2 + 1 = (x^2 - \beta)(x^2 - \sigma(\beta))(x^2 - \sigma^2(\beta)).$$

And so we see that we need to add square roots of $\sigma(\beta)$ and $\sigma^2(\beta)$ in order to get the normal closure K' of $L(\alpha)$ over K! Since $\beta \cdot \sigma(\beta) \cdot \sigma^2(\beta) = 1$ is a square, we see that as soon as any two out of three elements on the left has a square root, then so will the third. Thus

$$K' = L(\alpha, \alpha') \text{ where } \alpha' \text{ is a root of } x^2 - \sigma(\beta).$$

Since K' is the splitting field of two quadratic polynomials over L, $\mathrm{Gal}(K'/L) \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Since $\mathrm{Gal}(L/K) \cong \mathbf{Z}/3\mathbf{Z}$, we have a short exact sequence

$$0 \to \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \to \mathrm{Gal}(K'/K) \to \mathbf{Z}/3\mathbf{Z} \to 0.$$

Thus to conclude that $\mathrm{Gal}(K'/K) \cong A_4$, it suffices to show that this $\mathrm{Gal}(K'/K)$ is not the product of three cyclic groups; in particular, it suffices to show that the Galois group is not abelian. Let $\tau : K' \to K'$ be the automorphism determined by $\tau(\alpha) = -\alpha$, and let $\tilde{\sigma} : K' \to K'$ be the extension of the cyclic generator σ of $\mathrm{Gal}(L/K)$. Then

$$\tilde{\sigma}(\alpha)^2 = \tilde{\sigma}(\alpha^2) = \tilde{\sigma}(\beta) = \sigma(\beta),$$

and so $\tilde{\sigma}(\alpha) = \alpha'$. Thus

$$\tau(\tilde{(}\sigma)(\alpha)) = \tau(\alpha') = \alpha' \neq -\alpha' = \tilde{\sigma}(-\alpha') = \tilde{\sigma}(\tau(\alpha)).$$

We now verify that $L := \mathbf{Q}(\zeta_7 + \zeta_7^{-1})$ satisfies the conditions of (i): First, to see that it is a cubic extension over $\mathbf{Q}$, consider the tower of field extensions

$$\mathbf{Q} \subset \mathbf{Q}(\zeta_7 + \zeta_7^{-1}) \subset \mathbf{Q}(\zeta_7).$$

The cyclotomic extension $\mathbf{Q} \subset \mathbf{Q}(\zeta_7)$ is of degree 6 with Galois group $(\mathbf{Z}/7\mathbf{Z})^\times \cong C_6$, the generator the $\mathbf{Q}$-automorphism σ determined by $\sigma(\zeta_7) = \zeta_7^3$. To see that $\mathbf{Q}(\zeta_7 + \zeta_7^{-1}) \subset \mathbf{Q}(\zeta_7)$ is of degree 2, it now suffices to observe that the subgroup $C_2 \subset C_6$ is generated by the $\mathbf{Q}$-automorphism $\sigma^3(\zeta_7) = \zeta_7^6 = \zeta_7^{-1}$ so that

$$\sigma^3(\zeta_7 + \zeta_7^{-1}) = \zeta_7^{-1} + \zeta_7 \text{ whereas } \sigma(\zeta_7 + \zeta_7^{-1}) = \zeta_7^3 + \zeta_7^{-3}.$$

Multiplicativity of degrees now implies that $\mathbf{Q} \subset \mathbf{Q}(\zeta_7 + \zeta_7^{-1})$ is of degree 3. This also implies that $\mathrm{Gal}(\mathbf{Q}(\zeta_7 + \zeta_7^{-1})/\mathbf{Q}) \cong \{1, \sigma, \sigma^2\}$, so that

$$\begin{aligned}
\mathrm{Nm}_{\mathbf{Q}(\zeta_7+\zeta_7^{-1})/\mathbf{Q}}(\zeta_7 + \zeta_7^{-1}) &= (\zeta_7 + \zeta_7^{-1}) \cdot \sigma(\zeta_7 + \zeta_7^{-1}) \cdot \sigma^2(\zeta_7 + \zeta_7^{-1}) \\
&= (\zeta_7 + \zeta_7^{-1}) \cdot (\zeta_7^3 + \zeta_7^{-3}) \cdot (\zeta_7^2 + \zeta_7^{-2}) \\
&= \zeta_7^6 + \zeta_7^4 + \zeta_7^2 + 2 + \zeta_7^{-2} + \zeta_7^{-4} + \zeta_7^{-6} \\
&= \zeta_7^6 + \zeta_7^4 + \zeta_7^2 + 2 + \zeta_7^5 + \zeta_7^3 + \zeta_7 \\
&= 1
\end{aligned}$$

where the final line uses the fact that $1 + \zeta_7 + \cdots + \zeta_7^5 + \zeta_7^6 = 0$. ■