Modified Problem Set 9 – Due Thursday, March 30

Please turn in at least one of problems 1-3 and at least two of 4-7.

1. Let K be the field $\mathbb{Q}(\omega)$, where ω is a primitive 3rd root of unity. Write $\alpha \mapsto \bar{\alpha}$ for the nontrivial automorphism of K. Let $L = K(\sqrt[3]{\alpha}, \sqrt[3]{\bar{\alpha}})$ for some $\alpha \in K$.
   (a) Show that $L/\mathbb{Q}$ is Galois. Show that $\#\mathrm{Gal}(L/\mathbb{Q})$ divides 18 and that $\#\mathrm{Gal}(L/\mathbb{Q})$ is even.
   (b) Show that $\mathrm{Gal}(L/\mathbb{Q})$ is a subgroup of S_3 if and only if $\alpha/\bar{\alpha}$ is a cube in K.
   (c) Show that $\mathrm{Gal}(L/\mathbb{Q})$ is a subgroup of $\mathbb{Z}/6$ if and only if $\alpha\bar{\alpha}$ is a cube in K.
   (d) Let $\alpha = 7(2-\omega)$. Note that $\alpha\bar{\alpha} = 7^3$. Explicitly write out how an order two element of $\mathrm{Gal}(L/\mathbb{Q})$ permutes the cube roots of α and $\bar{\alpha}$.

2. Let L/K be a finite extension of fields. For $\theta \in L$, define $\mathrm{Tr}(\theta)$ to be the trace of the map $x \mapsto \theta x$, where we are thinking of this map as $[L:K] \times [L:K]$ matrix with entries in K.
   (a) Show that $\mathrm{Tr}(\theta_1 + \theta_2) = \mathrm{Tr}(\theta_1) + \mathrm{Tr}(\theta_2)$. Show that, for $a \in K$, we have $\mathrm{Tr}(a\theta) = a\mathrm{Tr}(\theta)$.
   (b) Suppose that $L = K(\theta)$, and $f(x) = x^n + f_{n-1}x^{n-1} + \cdots + f_1 x + f_0$ is the minimal polynomial of θ. Show that $\mathrm{Tr}(\theta) = -f_{n-1}$.
   (c) Let $f(x)$ be the minimal polynomial of θ and let $[L : K(\theta)] = m$. Show $\mathrm{Tr}(\theta) = -mf_{n-1}$.
   (d) Let L/K be Galois with Galois group G. Show that $\mathrm{Tr}(\theta) = \sum_{g \in G} g\theta$.
   (e) (**Harder**) Suppose that $L = K(\theta)$ and $x^n + f_{n-1}x^{n-1} + \cdots + f_1 x + f_0$ is the minimal polynomial of θ. Define the polynomial $g(x) = 1 + f_{n-1}x + \cdots + f_0 x^n = x^n f(1/x)$. Show:

   $$\sum_{j=1}^{\infty} \mathrm{Tr}(\theta^j) x^j = -x\frac{g'(x)}{g(x)}.$$

   Show that, if f' is not the zero polynomial, then $\mathrm{Tr}(\theta^j) \neq 0$ for some j.

3. The aim of this problem is to work out the classification of finite fields. Let K be a finite field of order q and let p be its characteristic.
   (a) Show that $|K| = p^n$ for some n.
   (b) Show that every $\theta \in F$ obeys $\theta^q = \theta$.
   (c) Show that the polynomial $x^q - x$ has distinct roots in any field of characteristic p.
   (d) Show that K is the splitting field of $x^q - x$.
   (e) Define $\phi : K \to K$ by $\phi(\theta) = \theta^p$. Show that ϕ is an automorphism of K, and that $\mathrm{Gal}(K/\mathbb{F}_p)$ is the cyclic group generated by ϕ.
   (f) Show that any two fields of order q are isomorphic.
   (g) Show that, for any prime power q, there is a field of order q. (Hint: Define L to be the splitting field of $x^q - x$. Show that every element of L is a root of $x^q - x$.)

4. In this problem, we will present a Galois theoretic proof that $\mathbb{C}$ is algebraically closed. Let $f \in \mathbb{C}[x]$ and let L be the splitting field of $f(x)\overline{f}(x)$, where $\overline{f}$ is the result of applying complex conjugation to the coefficients of f.
   (a) Show that L is Galois over $\mathbb{R}$.
   Let $G = \mathrm{Gal}(L/\mathbb{R})$. Let $|G| = 2^r s$ with s odd.
   (b) Show that there is an irreducible polynomial in $\mathbb{R}[x]$ of degree s. Using the intermediate value theorem, show that $s = 1$.
   (c) Show that, if $r \geq 2$, there is an irreducible quadratic polynomial in $\mathbb{C}[x]$. Obtain a contradiction to the fact that every complex number has a square root.[1]
   So $G = C_2$ and $L = \mathbb{C}$, as desired.

5. Let L/K be a Galois extension with Galois group G. Let F be a field with $K \subset F \subset L$ and let H be the subgroup of G fixing F. Let $X \subset G$ be the set of $g \in G$ with $gF = F$.
   (a) Describe X in terms of purely group theoretic operations involving G and H.
   (b) Let $A = \mathrm{Aut}(F/K)$. Describe a map $X \to A$ and show that it is a surjection.
   (c) Describe A in terms of purely group theoretic operations involving G and H.

6. Let $f(x)$ be an irreducible polynomial of degree 4 with rational coefficients and roots α_1, α_2, α_3 and α_4. Suppose that α_1 and α_2 are real and α_3 and α_4 are not real.
   (a) Let
   $$\beta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3)(\alpha_2 - \alpha_4)(\alpha_3 - \alpha_4).$$
   Show that β^2 is a negative rational number.
   (b) Show that the Galois group of the splitting field of f over $\mathbb{Q}$ is either S_4 or the dihedral group of order 8. (Hint – think about complex conjugation to rule out some cases.)

7. Let L/K be Galois with $\mathrm{Gal}(L/K) \cong C_n$. Let $\theta_1 \to \theta_2 \to \cdots \to \theta_n \to \theta_1$ be an n-element orbit.
   (a) Show that $L = K(\theta_1)$.
   (b) Show that there is a polynomial $f \in K[x]$ such that $f(\theta_i) = \theta_{i+1}$ for all i.

[1] Proof: $\left(\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}} + \sqrt{\frac{\sqrt{a^2+b^2}-a}{2}}\, i \right)^2 = a + bi.$