PROBLEM SET 9: DUE WEDNESDAY, APRIL 1

Problem 9.1. This is a lemma we'll want soon, though it doesn't mention Galois theory:

(1) Let G be a subgroup of S_n. Define a relation $\sim$ on $\{1, 2, \dots, n\}$ by saying that, for $1 \leq i \neq j \leq n$, we have $i \sim j$ if $(ij) \in G$ and defining $i \sim i$ for $1 \leq i \leq n$. Show that $\sim$ is an equivalence relation.
(2) Let p be prime, let G be a subgroup of S_p that acts transitively on $\{1, 2, \dots p\}$ and suppose that G contains a transposition. Show that $G = S_p$.

Problem 9.2. Let L/K be a Galois extension, not of characteristic 2. Let $\{\theta_1, \theta_2, \dots, \theta_N\}$ be a subset of L which is mapped to itself by $\mathrm{Gal}(L/K)$. Show that $K(\sqrt{\theta_1}, \dots, \sqrt{\theta_N})$ is Galois.

Problem 9.3. Let K be a field, $f(x)$ a separable polynomial with coefficients in K and L a splitting field of f, where $f(x) = \prod(x - \theta_j)$.We consider $\mathrm{Gal}(L/K)$ as a subgroup of S_n by its action on $\{\theta_1, \dots, \theta_n\}$. Let $f(x)$ factor in $K(\theta_1)$ as $\prod g_j(x)$.

(1) Describe how to compute the degrees of the irreducible factors $g_j(x)$ in terms of the action of $\mathrm{Gal}(L/K)$ on $\{\theta_1, \dots, \theta_n\}$.
(2) To check that you understand what you have done, suppose let $n = 8$, let $\mathrm{Gal}(L/K) \cong \mathrm{GL}_2(\mathbb{F}_3)$ and suppose $\mathrm{Gal}(L/K)$ acts on the θ_j in the way that $\mathrm{GL}_2(\mathbb{F}_3)$ acts on the eight elements of $\mathbb{F}_3^2 \setminus \{(0, 0)\}$. How does $f(x)$ factor over $K(\theta_1)$?

Problem 9.4. Let K be a field, $f(x)$ a separable polynomial with coefficients in K and L a splitting field of f, where $f(x) = \prod(x - \theta_j)$. Let K have characteristic not 2. Set $\Phi = \prod_{i<j}(\theta_i - \theta_j)^2$. Note that, since f is seperable, $\Phi \neq 0$.

(1) Show that $\Phi \in K$.
(2) Show that, if Φ is a square in K, then $\mathrm{Aut}(L/K) \subseteq A_n$.
(3) Show that, if Φ is not square in K, then $\mathrm{Aut}(L/K) \not\subseteq A_n$.

Problem 9.5. Let p be a prime and let $q = p^n$. In problem 8.4, you showed that the splitting field of $x^q - x$ over $\mathbb{F}_p$ was a field with q elements, which we called $\mathbb{F}_q$. You may use the results of that problem without proof.

(1) Show that the extension $\mathbb{F}_q/\mathbb{F}_p$ is Galois; you may use any of our equivalent definitions of a Galois extension.
(2) Show that the Galois group $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ is cyclic, with generator the Frobenius map $\theta \mapsto \theta^p$.

Problem 9.6. Let $K \subseteq L \subseteq M$ be a chain of fields, with $[M : K] < \infty$. Recall the definitions of Norm and Trace from Problem 8.3.

(1) For $\theta \in M$, show that $T_{L/K}(T_{M/L}(\theta)) = T_{M/K}(\theta)$.
(2) For $\theta \in M$, show that $N_{L/K}(N_{M/L}(\theta)) = N_{M/K}(\theta)$. Hint: I found this problem easiest when I wrote the L-linear map m_θ in rational canonical form.

Problem 9.7. We return to the discussion of constructible numbers from worksheet 18. Let θ_1, θ_2, θ_3, …, θ_N be a sequence of complex numbers where each θ_k is either

- a rational number,
- of one of the forms $\theta_i + \theta_j$, $\theta_i - \theta_j$, $\theta_i\theta_j$ or θ_i/θ_j for some i, $j < k$ or
- of the form $\sqrt{\theta_j}$ for some $j < k$.

Show that there is a **Galois extension** $L/\mathbb{Q}$ such that all the θ_j lie in L, and $[L : \mathbb{Q}]$ is a power of 2. (Hint: There is a useful problem earlier on this problem set.)

Problem 9.8. Let ω be a primitive cube root of unity in $\mathbb{C}$. Let $K = \mathbb{Q}(\omega)$ and write $\alpha \mapsto \overline{\alpha}$ for the automorphism $\omega \mapsto \omega^{-1}$ of K. For a nonzero element α of K, let $L = K(\sqrt[3]{\alpha},\ \sqrt[3]{\overline{\alpha}})$.

(1) Show that $L/\mathbb{Q}$ is a Galois extension.
(2) Let $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ show that either (1) there are integers b and c such that $\sigma(\omega^i \sqrt[3]{\alpha}) = \omega^{b+i} \sqrt[3]{\alpha}$ and $\sigma(\omega^j \sqrt[3]{\overline{\alpha}}) = \omega^{c+j} \sqrt[3]{\overline{\alpha}}$ or else (2) there are integers b and c such that $\sigma(\omega^i \sqrt[3]{\alpha}) = \omega^{b-i} \sqrt[3]{\overline{\alpha}}$ and $\sigma(\omega^j \sqrt[3]{\overline{\alpha}}) = \omega^{c-j} \sqrt[3]{\alpha}$ (for all integers i, j).
(3) If $\alpha\overline{\alpha}^2$ is a cube in K, show that $\mathrm{Gal}(L/\mathbb{Q})$ is abelian.