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 $\{1, 2, \ldots, n\}$ 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 $\{1, 2, \ldots, p\}$ 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 $\{\theta_1, \theta_2, \ldots, \theta_N\}$ be a subset of $L$ which is mapped to itself by $\text{Gal}(L/K)$. Show that $K(\sqrt[3]{\theta_1}, \ldots, \sqrt[3]{\theta_N})$ 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 $\text{Gal}(L/K)$ as a subgroup of $S_n$ by its action on $\{\theta_1, \ldots, \theta_n\}$. 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 $\text{Gal}(L/K)$ on $\{\theta_1, \ldots, \theta_n\}$.

2. To check that you understand what you have done, suppose let $n = 8$, let $\text{Gal}(L/K) \cong \text{GL}_2(\mathbb{F}_3)$ and suppose $\text{Gal}(L/K)$ acts on the $\theta_j$ in the way that $\text{GL}_2(\mathbb{F}_3)$ 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 separable, $\Phi \neq 0$.

1. Show that $\Phi \in K$.

2. Show that, if $\Phi$ is a square in $K$, then $\text{Aut}(L/K) \subseteq A_n$.

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

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 $\text{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ 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 $m_\theta$ in rational canonical form.

Problem 9.7. We return to the discussion of constructible numbers from worksheet 18. Let $\theta_1, \theta_2, \theta_3, \ldots, \theta_N$ be a sequence of complex numbers where each $\theta_k$ is either

- a rational number,
- of one of the forms $\theta_i + \theta_j, \theta_i - \theta_j, \theta_i \theta_j$ or $\theta_i/\theta_j$ for some $i, j < k$ or
- of the form $\sqrt[3]{\theta_j}$ for some $j < k$.

Show that there is a Galois extension $L/\mathbb{Q}$ such that all the $\theta_j$ 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 $\omega$ 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 $\alpha$ of $K$, let $L = K(\sqrt[3]{\alpha}, \sqrt[3]{\overline{\alpha}})$.

1. Show that $L/\mathbb{Q}$ is a Galois extension.

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

3. If $\alpha \overline{\alpha}$ is a cube in $K$, show that $\text{Gal}(L/\mathbb{Q})$ is abelian.