GALOIS THEORY: SOLUTIONS TO HOMEWORK 13

1. Let f denote the polynomial $t^3 - 7$.
   (a) Write down a splitting field extension for f over $\mathbb{Q}$.
   Solution: Let $\zeta = e^{2\pi i/3} = \frac{1}{2}(-1 + \sqrt{-3}) \in \mathbb{Q}$ be a primitive cube root of unity, and put $\alpha = \sqrt[3]{7} \in \mathbb{Q}$. Then f splits as $(t-\alpha)(t-\zeta\alpha)(t-\zeta^2\alpha)$ over $\mathbb{Q}$, and a splitting field for f is $L = \mathbb{Q}(\alpha, \zeta) = \mathbb{Q}(\sqrt[3]{7}, \sqrt{-3})$.
   (b) Show that $\mathrm{Gal}_{\mathbb{Q}}(f) \cong S_3$.
   Solution: Note that f is irreducible by Eisenstein's criterion using the prime 7 and Gauss' lemma. The Galois group is thus isomorphic to a transitive subgroup of S_3, and hence either S_3 or A_3. Since $\sqrt{-3} \notin \mathbb{Q}(\alpha) \subset \mathbb{R}$, the Tower Law yields

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot 3 = 6.$$

   Therefore, the Galois group of f has order 6, and hence is isomorphic to S_3.
2. Use the Galois correspondence to determine all subfields of the splitting field that you wrote down in part (a) of question 1. Draw the lattice of subfields and corresponding lattice of subgroups of S_3.
   Solution: Write $\beta_1 = \alpha$, $\beta_2 = \zeta\alpha$, $\beta_3 = \zeta^2\alpha$, and consider the Galois group G of $t^3 - 7$, namely $\mathrm{Gal}(L : \mathbb{Q}) \cong S_3$. Since all possible permutations of roots must occur as automorphisms in G, we have in particular the automorphism σ that cyclically permutes the β_i, so that

$$\alpha \mapsto \zeta\alpha \quad \text{and} \quad \zeta \mapsto \zeta,$$

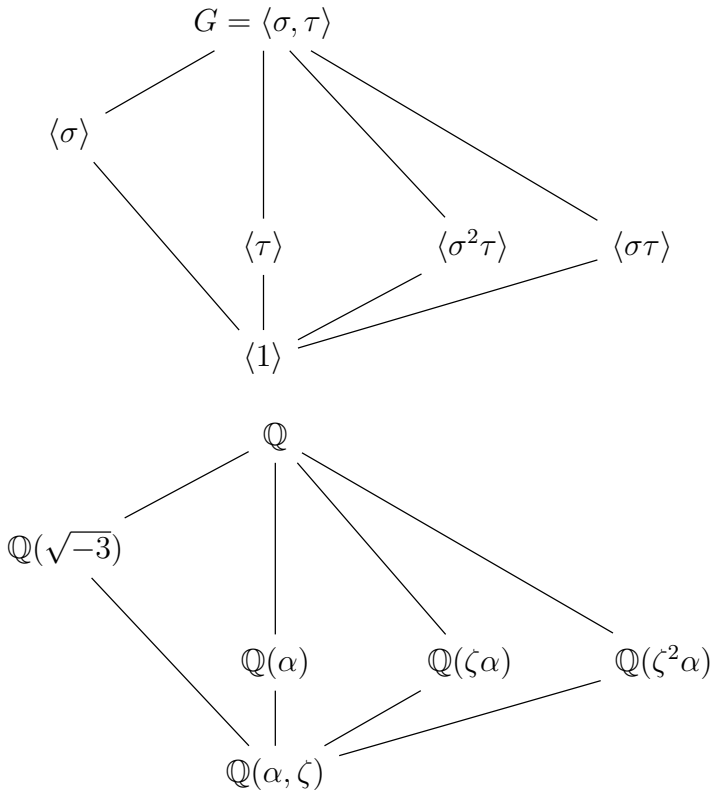
   and also the permutation τ that interchanges two of the roots, leaving the third fixed, so that

$$\alpha \mapsto \alpha \quad \text{and} \quad \zeta \mapsto \zeta^2.$$

   Notice that one has

$$G \cong \langle \sigma, \tau | \sigma^3 = \tau^2 = 1, \tau\sigma = \sigma^2\tau \rangle.$$

   The fields L, and $\mathbb{Q}$, are the fixed fields of $\{\mathrm{id}\}$, and G, respectively. As for the intermediate fields, we have the three cubic extensions $\mathbb{Q}(\alpha)$, $\mathbb{Q}(\zeta\alpha)$ and $\mathbb{Q}(\zeta^2\alpha)$, corresponding to the subgroups $\langle\tau\rangle$, $\langle\sigma^2\tau\rangle$ and $\langle\sigma\tau\rangle$, respectively, of index 3 in G. Finally, the subgroup $\langle\sigma\rangle$ of index 2 in G fixes the quadratic extension $\mathbb{Q}(\zeta) = \mathbb{Q}(\sqrt{-3})$.



3. Suppose that L is a finite field having p^n elements, where p is a prime number. Recall that $\mathrm{Gal}(L : \mathbb{F}_p) = \langle \varphi \rangle$, where φ denotes the Frobenius mapping.
   (a) Show that whenever K is a subfield of L, then $|K| = p^d$ for some divisor d of n.
   Solution: Suppose that K is a subfield of L, and write $\mathbb{F}_p$ for the prime subfield of L. Then, by the Fundamental Theorem of Galois Theory, we see that $\mathrm{Gal}(K : \mathbb{F}_p)$ is a subgroup of $\mathrm{Gal}(L : \mathbb{F}_p)$. But the latter group is cyclic of order n, so that by Lagrange's theorem, any subgroup of $\mathrm{Gal}(L : \mathbb{F}_p)$ must have order dividing n. Thus we see that $\mathrm{Gal}(K : \mathbb{F}_p)$ has order d for some divisor d of n. Furthermore, we know that any subgroup of a cyclic group is normal. Thus, again by the Fundamental Theorem, we see that the field extension $K : \mathbb{F}_p$ is normal. But L is algebraic over its prime subfield, hence K is separable, and thus Galois. Then we deduce that $[K : \mathbb{F}_p] = |\mathrm{Gal}(K : \mathbb{F}_p)| = d$, whence $|K| = p^d$.
   (b) Show that for each divisor d of n, there is a unique subfield K of L with $|K| = p^d$.
   Solution: Suppose that $d|n$. Observe that $\mathrm{Gal}(L : \mathbb{F}_p)$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ and is generated by the Frobenius monomorphism ϕ. But there is precisely one subgroup of $\mathbb{Z}/n\mathbb{Z}$ of index d, and so $\mathrm{Gal}(L : \mathbb{F}_p)$ likewise has precisely one subgroup of index d, namely $\langle \phi^d \rangle$. Then it follows from the Fundamental Theorem of Galois Theory that there is precisely one subfield K of L with $[K : \mathbb{F}_p] = d$, or equivalently, having p^d elements.

4. Let $L : K$ be a finite Galois extension with Galois group G.
   (a) For any $\alpha \in L$, define the *norm* of α by $\mathrm{N}(\alpha) = \prod_{\sigma\in G} \sigma(\alpha)$. Show that $\mathrm{N}(\alpha) \in K$.
   Solution: Since $L : K$ is Galois, the fixed field of G is K. Then $\beta \in K$ if and only if $\tau(\beta) = \beta$ for every $\tau \in G$. But whenever $\tau \in G$, one has
   $$\tau(\mathrm{N}(\alpha)) = \prod_{\sigma\in G} \tau(\sigma(\alpha)) = \prod_{\rho\in G} \rho(\alpha),$$
   since the action of τ on G is simply to permute the elements of G. Thus we see that $\tau(\mathrm{N}(\alpha)) = \mathrm{N}(\alpha)$ for every $\tau \in G$, whence $\mathrm{N}(\alpha) \in K$.
   (b) For any $\alpha \in L$, define the *trace* of α by $\mathrm{Tr}(\alpha) = \sum_{\sigma\in G} \sigma(\alpha)$. Show that $\mathrm{Tr}(\alpha) \in K$.
   Solution: Whenever $\tau \in G$, one has
   $$\tau(\mathrm{Tr}(\alpha)) = \sum_{\sigma\in G} \tau(\sigma(\alpha)) = \sum_{\rho\in G} \rho(\alpha),$$
   since the action of τ on G is simply to permute the elements of G. Thus we see that $\tau(\mathrm{Tr}(\alpha)) = \mathrm{Tr}(\alpha)$ for every $\tau \in G$, whence $\mathrm{Tr}(\alpha) \in K$.

5. Let p be a prime number, and n a natural number, and denote by $\mathbb{F}_q$ the finite field of $q = p^n$ elements with prime field $\mathbb{F}_p$. Let ϕ denote the Frobenius monomorphism from $\mathbb{F}_q$ into $\mathbb{F}_q$. Recall that $\mathrm{Gal}(\mathbb{F}_q : \mathbb{F}_p) = \langle\phi\rangle$.
   (a) Defining the trace of $\alpha \in \mathbb{F}_q$ as in question 4(b) above, show that there exists an element $\alpha \in \mathbb{F}_q$ having non-zero trace.
   Solution: Since $\mathrm{Gal}(\mathbb{F}_q : \mathbb{F}_p) = \langle\phi\rangle$ and $\phi^j(\alpha) = \alpha^{p^j}$ for each $\alpha \in \mathbb{F}_q$, we have
   $$\mathrm{Tr}(\alpha) = \alpha + \alpha^p + \ldots + \alpha^{p^{n-1}} = f(\alpha),$$
   where $f(t) = t + t^p + \ldots + t^{p^{n-1}}$. The polynomial f has at most $\deg(f) = p^{n-1}$ roots over $\mathbb{F}_q$, yet $\mathbb{F}_q$ has p^n elements. Thus $\mathbb{F}_q$ has at least $p^n - p^{n-1}$ elements α with $\mathrm{Tr}(\alpha) = f(\alpha) \neq 0$. So there exists $\alpha \in \mathbb{F}_q$ having non-zero trace.
   (b) Defining the norm of $\alpha \in \mathbb{F}_q$ as in question 4(a) above, show that there exists a non-zero element $\alpha \in \mathbb{F}_q^\times$ having norm different from 1.
   Solution: For each $\alpha \in \mathbb{F}_q^\times$, one has $\mathrm{N}(\alpha) = \alpha \cdot \alpha^p \cdot \ldots \cdot \alpha^{p^{n-1}} = \alpha^{(p^n-1)/(p-1)}$. Recalling that $\mathbb{F}_q^\times = \langle g\rangle$ for a suitable primitive element $g \in \mathbb{F}_q^\times$, we see that g has order $p^n - 1$, and thus (when $p \neq 2$) one has $N(g) = g^{(p^n-1)/(p-1)} \neq 1$. So there exists $\alpha \in \mathbb{F}_q$ having norm different from 1, *unless* $p = 2$, in which case *every* non-zero element of $\mathbb{F}_q$ has norm equal to 1.