Galois theory, Problems 5

To be handed in 6th December 2017 **SOLUTIONS**

1. Suppose that $L : M : K$ is an algebraic tower of fields. Prove that $L : K$ is separable if and only if $L : M$ and $M : K$ are both separable.
   Solution: We showed in Proposition 7.1 that when $L : K$ is separable, then so too is $L : M$. Meanwhile, the separability, in such circumstances, of $M : K$ is inherited from that of $L : K$. Conversely, suppose that $L : M$ and $M : K$ are both separable, and suppose that $\alpha \in L$. Then since $L : M$ is separable, one finds that α is separable over M. The polynomial $m_\alpha(M)$ has its coefficients defined in a subfield M' of M with $M' : K$ a finite separable extension. Since $m_\alpha(M') = m_\alpha(M)$ is separable, we deduce that α is separable over M'. Thus, since $M' : K$ is finite and separable, it follows from the primitive element theorem that there exists $\beta \in M'$ such that $M' = K(\beta)$, whence Theorem 7.4 implies that $M'(\alpha) : K$, or equivalently $K(\alpha, \beta) : K$, is separable. Consequently, we deduce that $\alpha \in K(\alpha, \beta)$ is separable over K. Since this conclusion holds for all $\alpha \in L$, we conclude that $L : K$ is separable.

2. Suppose that $E : K$ and $F : K$ are finite extensions with $E \subseteq L$ and $F \subseteq L$, with L a field.

   (a) Show that when $E : K$ is separable, then so too is $EF : F$.
   Solution: By the primitive element theorem, we may suppose that $E = K(\alpha)$ for some $\alpha \in E$ separable over K. Thus $EF = F(\alpha)$. Since α is separable over K, it is also separable over F, and hence it follows from Theorem 7.4 that $F(\alpha) : F$, or equivalently $EF : F$, is separable.

   (b) Show that when $E : K$ and $F : K$ are both separable, then so too are $EF : K$ and $E \cap F : K$.
   Solution: When $E : K$ and $F : K$ are both separable, then $EF : F$ is separable, and hence $EF : F : K$ is a tower of extensions with $EF : F$ and $F : K$ both separable. Then it follows from problem 1 that $EF : K$ is separable. Likewise, one has the tower $E : E \cap F : K$ of extensions with $E : K$ separable. Then it follows from problem 1 that $E \cap F : K$ is separable.

3. Let f denote the polynomial $t^3 - 7$.

   (i) 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 $L = \mathbb{Q}(\alpha, \zeta) = \mathbb{Q}(\sqrt[3]{5}, \sqrt{-3})$.

   (ii) 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 $\sqrt{-3} \notin \mathbb{Q}(\alpha) \subset \mathbb{R}$, it follows from the Tower Law that
   $$[L : \mathbb{Q}] = [L : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot 3 = 6.$$
   Therefore, the Galois group of f has order 6, and hence is isomorphic to S_3.

   (iii) Use the Galois correspondence to determine all subfields of the splitting field that you wrote down in part (i). 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

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

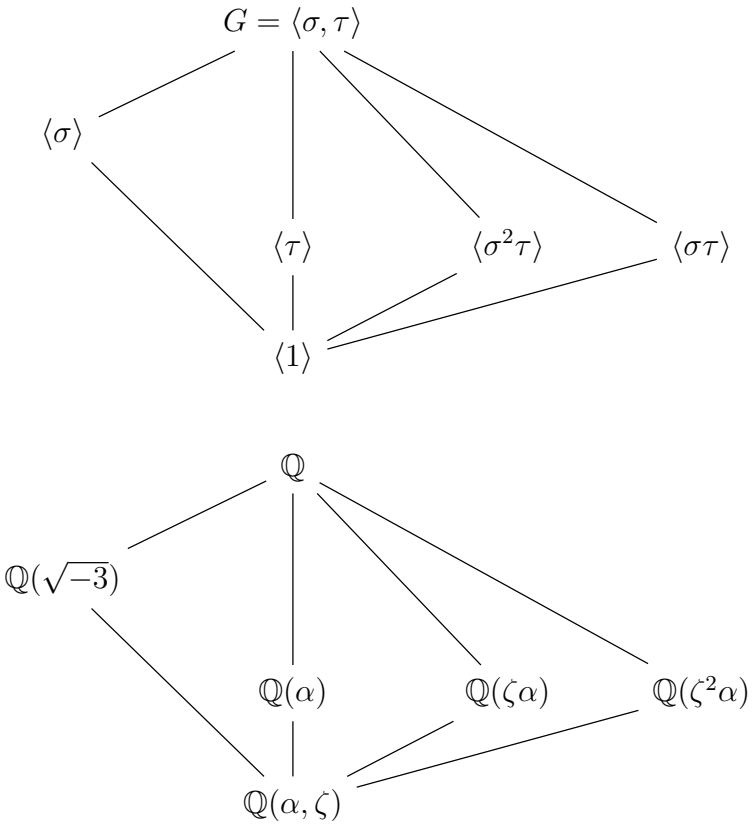
and also the permutation τ that interchanges two of the roots, leaving the third fixed, so that

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

Notice that

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

The fields L, and $\mathbb{Q}$, are the fixed fields of $\{id\}$, 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 $\mathbb{Q}(\zeta) = \mathbb{Q}(\sqrt{-3})$.



4. Let f denote the polynomial $t^3 + t + 1$.

   (i) Write down a splitting field extension for f over $\mathbb{F}_2$.
   Solution: If α is a root of $t^3 + t + 1$ lying in a splitting field extension L for this polynomial over $\mathbb{F}_2$, then

$$f(t) = t^3 + t + 1 = (t + \alpha)(t^2 + \alpha t + \alpha^2 + 1) = (t + \alpha)(t + \alpha^2)(t + \alpha^2 + \alpha).$$

   Then $\mathbb{F}_2(\alpha) : \mathbb{F}_2$ is a splitting field extension for $t^3 + t + 1$ over $\mathbb{F}_2$.

(ii) What is $\mathrm{Gal}_{\mathbb{F}_2}(f)$? Justify your answer, and determine all subfields of the splitting field that you wrote down in part (i).
Solution: Since f is a separable polynomial, we find that $\mathbb{F}_2(\alpha) : \mathbb{F}_2$ is a Galois extension, with Galois group of order $[\mathbb{F}_2(\alpha) : \mathbb{F}_2] = 3$. Hence, the group must be cyclic.

In this case it's not too difficult to write down the automorphisms. If $\sigma(x) = x^2$ then we have $\sigma(xy) = \sigma(x)\sigma(y)$ and $\sigma(x+y) = x^2 + 2xy + y^2 = x^2 + y^2 = \sigma(x) + \sigma(y)$, so σ is an automorphism, with $\sigma(\alpha) = \alpha^2$. We get another automorphism by squaring σ, so that $\sigma^2(x) = \sigma(\sigma(x)) = \sigma(x^2) = x^4$, and in particular $\sigma^2(\alpha) = \alpha^4 = \alpha^2 + \alpha$. Thus, the identity, σ and σ^2 are the three automorphisms. One can also check directly that σ has order 3, thus $\sigma^3(\alpha) = \alpha^8 = \alpha$.

Since the cyclic group $\langle\sigma\rangle$ of order 3 has no proper subgroups, it follows from the Fundamental Theorem of Galois Theory that $\mathbb{F}_2(\alpha)$ has no proper subfields, and hence the only subfields are the trivial ones $\mathbb{F}_2$ and $\mathbb{F}_2(\alpha)$.

5. Let $L : K$ be a finite Galois extension with Galois group G. For any $\alpha \in L$, define the polynomial $f_\alpha(t) = \prod_{\sigma\in G}(t - \sigma(\alpha))$.

(i) Show that $f_\alpha \in K[t]$.
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 $\tau \in G$. Thus, whenever $\tau \in G$, one has

$$\tau(f_\alpha(t)) = \prod_{\sigma\in G}(t - \tau(\sigma(\alpha))) = \prod_{\rho\in G}(t - \rho(\alpha)) = f_\alpha(t).$$

Then $f_\alpha(t)$ has each of its coefficients in the fixed field of G, so $f_\alpha \in K[t]$.

(ii) Prove that if $\sigma(\alpha) \neq \tau(\alpha)$ whenever $\sigma, \tau \in G$ satisfy $\sigma \neq \tau$, then $f_\alpha = m_\alpha(K)$.
Solution: Since the identity element belongs to G, one has $f_\alpha(\alpha) = 0$, whence the minimal polynomial $m_\alpha(K)$ of α over K must divide f_α. But over $L[t]$ one has that $t - \alpha$ divides $m_\alpha(K)$. Then since $m_\alpha(K)$ is fixed by the action of G (its coefficients lie in K), we find that $t - \sigma(\alpha)$ divides $\sigma(m_\alpha(K)) = m_\alpha(K)$ for each $\sigma \in G$. By hypothesis, moreover, the elements $\sigma(\alpha)$ are distinct for $\sigma \in G$, and thus $\prod_{\sigma\in G}(t - \sigma(\alpha)) = f_\alpha(t)$ divides $m_\alpha(K)$. Thus we find that $m_\alpha(K)$ and f_α divide each other, and this implies that f_α is the minimal polynomial of α.

(iii) Use part (ii) to calculate the minimal polynomial of $2\sqrt{-3} - \sqrt{2}$ over $\mathbb{Q}$.
Solution: The field extension $\mathbb{Q}(\sqrt{2}, \sqrt{-3}) : \mathbb{Q}$ is a splitting field extension for the polynomial $(t^2 - 2)(t^2 + 3)$, and hence is finite and Galois. One checks easily (via the Tower Law) that $[\mathbb{Q}(\sqrt{2}, \sqrt{-3}) : \mathbb{Q}] = 4$, and thus the conjugates of $2\sqrt{-3} - \sqrt{2}$ under the action of $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{-3}) : \mathbb{Q})$ are $\pm(2\sqrt{-3} - \sqrt{2})$ and $\pm(2\sqrt{-3} + \sqrt{2})$. Then applying the conclusion of part (ii), we find that the minimal polynomial of $2\sqrt{-3} - \sqrt{2}$ is

$$(t^2 - (2\sqrt{-3} - \sqrt{2})^2)(t^2 - (2\sqrt{-3} + \sqrt{2})^2) = t^4 + 20t^2 + 196.$$

6. 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. Show that whenever K is a subfield of L, then $|K| = p^d$ for some divisor d of n. Show further that for each divisor d of n, there is a unique subfield K of L.
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 $|K| = p^d$.

Suppose next 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.