QUIZ 2 SOLUTIONS, MATH100C, SPRING 2021

For questions 3 and 4 you can use the following theorem from group theory:

Suppose p is a prime and G is a subgroup of S_p which acts transitively on $\{1, \ldots, p\}$. Then G is solvable if and only if every non-trivial element of G fixes at most one point; that means if $\sigma \in G$, $\sigma(i) = i$, and $\sigma(j) = j$ for distinct values i and j, then $\sigma = \mathrm{id}$.

1. Suppose F is a field of characteristic $p > 0$. Suppose E/F is a purely in separable extension and L/E is an algebraic extension. Suppose $\alpha \in L$.
   (a) (1 points) Prove that $m_{\alpha,E}$ divides $m_{\alpha,F}$ in $E[x]$.

   Solution. Because $F \subseteq E$ we have $m_{\alpha,F} \in E[x]$, and because $m_{\alpha,F}(\alpha) = 0$, we deduce from the defining property of the minimal polynomial that $m_{\alpha,E} | m_{\alpha,F}$ in $E[x]$.

   (b) (2 points) Prove that for some integer power q of p, we have $m^q_{\alpha,E} \in F[x]$.

   Solution. Write $m_{\alpha,E}(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n$ for $a_i \in E$. Because E/F is purely inseparable, for each i we can find some $m_i \geq 0$ such that $a_i^{p^{m_i}} \in F$. Letting $m = \mathrm{lcm}(m_i)$ and letting $q = p^m$ we have $a_i^q \in F$ for each i. But then

   $$m^q_{\alpha,E}(x) = (a_0 + \cdots + a_{n-1}x^{n-1} + x^n)^q = a_0^q + \cdots + a_{n-1}^q x^{(n-1)q} + x^{nq} \in F[x].$$

   (c) (1 points) Prove that for some integer power q of p, $m_{\alpha,F}$ divides $m^q_{\alpha,E}$ in $E[x]$.

   Solution. Take q as in part (b). Then $m^q_{\alpha,E} \in F[x]$ and $m^q_{\alpha,E}(\alpha) = 0$, so by the defining property of the minimal polynomial we obtain $m_{\alpha,F} | m^q_{\alpha,E}$ in $E[x]$.

   (d) (4 points) Prove that if $m_{\alpha,F}$ is separable in $F[x]$, then $[F[\alpha] : F] = [E[\alpha] : E]$.

   Solution. Part (a) tells us that that $m_{\alpha,E}$ is separable in $E[x]$ and that every root of $m_{\alpha,E}$ (taken in some splitting field over L) is also a root of $m_{\alpha,F}$. But part (c) tells us that every root of $m_{\alpha,F}$ is also a root of $m^q_{\alpha,E}$, and hence is also a root of $m_{\alpha,E}$. Thus we see that $m_{\alpha,F}$ and $m_{\alpha,E}$ have precisely the same roots in some splitting field, so because they are both separable polynomials in $E[x]$ we find that $m_{\alpha,F} = m_{\alpha,E}$.

2. Suppose F is a field of characteristic zero and $f \in F[x]$ is a monic irreducible polynomial. Let E be a splitting field of f over F. Suppose $f(x) = \prod_{i=1}^n (x - \alpha_i)$ in $E[x]$. Let $G := \mathrm{Aut}_F(E)$ and $G_i := \mathrm{Aut}_{F[\alpha_i]}(E)$.
   (a) (3 points) Prove that there is $\sigma_i \in G$ such that $\sigma_i(\alpha_1) = \alpha_i$ for every i.

   Outline of solution. This follows from the fact that f is irreducible: one can find an F-isomorphism $\theta_i : F[\alpha_1] \to F[\alpha_i]$ for any i, and then this can be extended to the splitting field E to get the desired σ_i.

   (b) (3 points) Prove that $G_i = \sigma_i G_1 \sigma_i^{-1}$ for every i.

   Solution. Notice $\sigma \in G_i$ if and only if $\sigma(\alpha_i) = \alpha_i$.

   On one hand if $\theta \in G_1$ then one has $(\sigma_i \theta \sigma_i^{-1})(\alpha_i) = \sigma_i(\theta(\alpha_1)) = \sigma_i(\alpha_1) = \alpha_i$, so $\sigma_i \theta \sigma_i^{-1} \in G_i$.

   Conversely if $\theta \in G_i$ then one has $(\sigma_i^{-1}\theta\sigma_i)(\alpha_1) = \sigma_i^{-1}(\theta(\alpha_i)) = \sigma_i^{-1}(\alpha_i) = \alpha_1$, and thus $\theta = \sigma_i(\sigma_i^{-1}\theta\sigma_i)\sigma_i^{-1} \in \sigma_i G_1 \sigma_i^{-1}$.

(c) (3 points) Prove that if G is abelian, then $E = F[\alpha_1]$.

Solution. Notice E/F is Galois: normality is by design and separability is automatic as $\mathrm{char}(F) = 0$. Thus we can invoke the fundamental theorem of Galois theory, which tells us $E = F[\alpha_1]$ if and only if $\mathrm{Aut}_{F[\alpha_1]}(E) = \{\mathrm{id}\}$, i.e. if and only if $G_1 = \{\mathrm{id}\}$. To see this, suppose $\theta \in G_1$. Then by part (b) one has $\sigma_i \theta \sigma_i^{-1} \in G_i$ for each i, but because G is abelian this says that $\theta \in G_i$ for each i, meaning $\theta(\alpha_i) = \alpha_i$ for each i. Because $E = F[\alpha_1, \ldots, \alpha_n]$ we deduce $\theta = \mathrm{id}$, which shows the result.

3. (5 points) Let F be a characteristic zero field. Suppose p is a prime number, and f is a monic irreducible polynomial of degree p in $F[x]$. Let E be a splitting field of f over F. Suppose f is solvable by radicals over F. Prove that if α and α' are two distinct zeros of f, then $E = F[\alpha, \alpha']$.

Solution. The fact that f is solvable by radical over F implies that $\mathscr{G}_{f,F}$ is a solvable group. If we think of $\mathscr{G}_{f,F}$ as a subgroup of S_p, then the fact that f is irreducible implies that $\mathscr{G}_{f,F}$ acts transitively on $\{1, \ldots, p\}$ (this follows from Problem 2a, or one could repeat the argument here). Thus we can invoke the fact given above, and conclude that any non-trivial element of $\mathscr{G}_{f,F}$ fixes at most one point. It follows that if α, α' are distinct zeros of f, then the only element of $\mathscr{G}_{f,F}$ which fixes both α and α' is the identity. Thus $\mathrm{Aut}_{F[\alpha,\alpha']}(E) = \{\mathrm{id}\} = \mathrm{Aut}_E(E)$, and then it follows from the fundamental theorem of Galois theory that $E = F[\alpha, \alpha']$.

4. Suppose p is a prime number more than 4, and $f(x) = x^p - 4x + 2 \in \mathbb{Q}[x]$.

(a) (1 points) Prove that f' has exactly 2 real zeros in $\mathbb{C}$.

Solution. We calculate $f'(x) = px^{p-1} - 4$, and directly see the real zeros of f' are $\pm \sqrt[p-1]{4/p}$.

(b) (2 points) Prove that f has exactly 3 real zeros in $\mathbb{C}$.

Solution. If f has n real zeros, say $a_1 < a_2 < \cdots < a_n$, then using Rolle's theorem one finds for each $i \in [1, n-1]$ some $x_i \in (a_i, a_{i+1})$ with $f'(x_i) = 0$. This means f' has at least $n - 1$ real zeros, so combining with part (a) we see that f has at most 3 real zeros. On the other hand, we notice that $f(-2) < 0$, $f(0) > 0$, $f(1) < 0$ and $f(2) > 0$, so the intermediate value theorem tells us that f has zeros in the intervals $(-2, 0)$, $(0, 1)$ and $(1, 2)$, so f has at least 3 real zeros. Thus f has exactly 3 real zeros.

(c) (2 points) Prove that f is irreducible in $\mathbb{Q}[x]$.

Solution. Because f is primitive this is equivalent to being irreducible in $\mathbb{Z}[x]$, and this fact follows immediately from Eisenstein's criterion with $p = 2$.

(d) (3 points) Prove that f is not solvable by radicals over $\mathbb{Q}$.

Solution. As we have argued twice now, the fact that f is irreducible implies that $\mathscr{G}_{f,\mathbb{Q}}$ acts transitively on the roots of f. If we let $E \subseteq \mathbb{C}$ be a splitting field of f over $\mathbb{Q}$, so $\mathscr{G}_{f,\mathbb{Q}} = \mathrm{Aut}_{\mathbb{Q}}(E)$, and we let $\tau \in \mathscr{G}_{f,\mathbb{Q}}$ denote the restriction of complex conjugation to E (which makes sense because $E/\mathbb{Q}$ is normal), then notice that $\tau \neq \mathrm{id}$ because f has $p > 4$ zeros, of which only 3 are real. But τ fixes these three real roots, and then using the fact given at the top of the page one concludes that $\mathscr{G}_{f,\mathbb{Q}}$ cannot be solvable, so f is not solvable by radicals over $\mathbb{Q}$.