QUIZ 3, MATH100C, SPRING 2021

1. (5 points) Suppose F is a field, $\overline{F}$ is an algebraic closure of F, and $\alpha \in \overline{F}$. Suppose $F[\alpha]/F$ is a Galois extension and $[F[\alpha] : F] = p$ where p is a prime. Prove that $L[\alpha]/L$ is Galois and $[L[\alpha] : L]$ is either 1 or p, for every $L \in \operatorname{Int}(\overline{F}/F)$.

   Outline of solution. One can directly verify that if $F[\alpha]$ is a splitting field of $f \in F[x] \setminus F$ over F then $L[\alpha]$ is a splitting field of f over L (in fact one can take $f = m_{\alpha,F}$). Because f being separable in $F[x]$ implies being separable in $L[x]$, we see $L[\alpha]/L$ is Galois. For the second statement, notice one has a restriction homomorphism $\operatorname{Aut}_L(L[\alpha]) \to \operatorname{Aut}_F(F[\alpha])$, which is easily verified to be injective. From this one finds by Lagrange's theorem that $[L[\alpha] : L]$ divides $[F[\alpha] : F] = p$, which gives the result.

2. Let $\overline{\mathbb{Q}} := \{\alpha \in \mathbb{C} \mid \alpha \text{ is algebraic over } \mathbb{Q}\}$.
   (a) (3 points) Prove that $\overline{\mathbb{Q}}$ is algebraically closed.

   Solution. Suppose $f(x) \in \overline{\mathbb{Q}}[x] \setminus \mathbb{Q}$. Then $f(x) \in \mathbb{C}[x] \setminus \mathbb{C}$ so because $\mathbb{C}$ is algebraically closed there exists some $\alpha \in \mathbb{C}$ which is a zero of f. We claim $\alpha \in \overline{\mathbb{Q}}$: one needs to see that α is algebraic over $\mathbb{Q}$. By construction α is algebraic over $\overline{\mathbb{Q}}$, so $\overline{\mathbb{Q}}[\alpha]/\overline{\mathbb{Q}}$ is algebraic, and $\overline{\mathbb{Q}}/\mathbb{Q}$ is algerbaic by construction, so $\overline{\mathbb{Q}}[\alpha]/\mathbb{Q}$ is an algerbaic extension, and thus α is algebraic over $\mathbb{Q}$ as desired.

   (b) (5 points) Suppose $\alpha_0 \in \overline{\mathbb{Q}} \setminus \mathbb{Q}$ and let $\Sigma_{\alpha_0} = \{E \in \operatorname{Int}(\overline{\mathbb{Q}}/\mathbb{Q}) \mid \alpha_0 \notin E\}$. Prove that Σ_{α_0} has a maximal element F with respect to inclusion.

   Outline of solution. One should invoke Zorn's lemma: Σ_{α_0} is a poset with respect to inclusion (important subtle detail: Σ_{α_0} is nonempty because $\alpha_0 \notin \mathbb{Q}$), and if $\mathscr{C}$ is a chain in Σ_{α_0} then it is straightforward to verify that $L := \bigcup_{E\in\mathscr{C}} E$ is inside Σ_{α_0} and is an upper bound for $\mathscr{C}$. Thus the conditions of Zorn's lemma are satisfied and the conclusion follows.

   (c) (5 points) Suppose $F \in \Sigma_{\alpha_0}$ is a maximal element, and $E \in \operatorname{Int}(\overline{\mathbb{Q}}/F)$ and E/F is a finite Galois extension. Prove that $\operatorname{Aut}_F(E)$ is cyclic.

   Solution. By the maximality of F, if $K \in \operatorname{Int}(E/F)$ is not equal to F, then $K \notin \Sigma_{\alpha_0}$ which means $\alpha_0 \in K$. Suppose that $\operatorname{Aut}_F(E)$ is not cyclic; then for every $\sigma \in \operatorname{Aut}_F(E)$ one has $\langle\sigma\rangle \neq \operatorname{Aut}_F(E)$, which implies by the fundamental theorem of Galois theory that $\operatorname{Fix}(\sigma) \neq F$, which by our remarks above implies $\alpha_0 \in \operatorname{Fix}(\sigma)$. But then $\sigma(\alpha_0) = \alpha_0$, and because $\sigma \in \operatorname{Aut}_F(E)$ was arbitrary and E/F is Galois we conclude $\alpha_0 \in F$, which is a contradiction.

3. (4 points) Suppose $\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$. Suppose $\sigma \in \operatorname{Aut}_{\mathbb{Q}}(\overline{\mathbb{Q}})$ and let $F := \operatorname{Fix}(\langle\sigma\rangle)$. Suppose $E \in \operatorname{Int}(\overline{\mathbb{Q}}/F)$ and E/F is a finite Galois extension. Prove that $\operatorname{Aut}_F(E) = \langle\sigma|_E\rangle$.

   Notice $\langle\sigma|_E\rangle \subseteq \operatorname{Aut}_F(E)$. To show equality notice that
   $$F \subseteq \operatorname{Fix}(\langle\sigma|_E\rangle) \subseteq \operatorname{Fix}(\langle\sigma\rangle) = F,$$
   thus $F = \operatorname{Fix}(\langle\sigma|_E\rangle)$. As a result one has $\operatorname{Aut}_F(E) = \operatorname{Aut}_{\operatorname{Fix}(\langle\sigma|_E\rangle)}(E) = \langle\sigma|_E\rangle$.

4. Suppose $\zeta_n := e^{\frac{2\pi i}{n}} \in \mathbb{C}$ and $K_n := \mathbb{Q}[\zeta_n] \cap \mathbb{R}$.
   (a) (4 points) Prove that $K_n/\mathbb{Q}$ is a Galois extension and $[K_n : \mathbb{Q}] = \frac{\phi(n)}{2}$ where $\phi(n)$ is the Euler ϕ-function.

Solution. Recall $\mathbb{Q}[\zeta_n]/\mathbb{Q}$ is Galois with $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\zeta_n])$ cyclic. Thus $\mathrm{Aut}_{K_n}(\mathbb{Q}[\zeta_n])$ is automatically normal in $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\zeta_n])$ and we deduce from the fundamental theorem of Galois theory that $K_n/\mathbb{Q}$ is Galois. Also notice that $\zeta_n + \zeta_n^{-1} \in K_n$ (for instance it is fixed by complex conjugation), and ζ_n satisfies the polynomial $x^2 + (\zeta_n - \zeta_n^{-1})x + 1 \in K_n[x]$, so from this one deduces $[\mathbb{Q}[\zeta_n] : K_n] = \deg(m_{\zeta_n, K_n}) \leq 2$. On the other hand $\zeta_n \notin K_n$ (because $\zeta_n \notin \mathbb{R}$) so one deduces equality $[\mathbb{Q}[\zeta_n] : K_n] = 2$. From tower law one gets the desired equality $[K_n : \mathbb{Q}] = \frac{[\mathbb{Q}[\zeta_n]:\mathbb{Q}]}{2} = \frac{\phi(n)}{2}$.

(b) (2 points) Prove that for every $\alpha \in K_n$ all the complex zeros of $m_{\alpha,\mathbb{Q}}$ are in $\mathbb{R}$.

Solution. Because $K_n/\mathbb{Q}$ is Galois (in particular normal) one sees that $m_{\alpha,\mathbb{Q}}$ splits into linear factors in K_n, hence all complex zeros of $m_{\alpha,\mathbb{Q}}$ are in K_n, hence in $\mathbb{R}$.

(c) (2 points) Suppose $\alpha \in K_n^\times$ and $\alpha^m \in \mathbb{Q}$ for some positive integer m. Prove that $\alpha^2 \in \mathbb{Q}$.

Solution. If $\alpha^m \in \mathbb{Q}$ then one has $m_{\alpha,\mathbb{Q}}(x) | x^m - \alpha^m$ in $\mathbb{Q}[x]$. By part (b) $m_{\alpha,\mathbb{Q}}$ has all complex zeros in $\mathbb{R}$, but the complex zeros of $x^m - \alpha^m$ are exactly $\alpha, \zeta_m\alpha, \zeta_m^2\alpha, \ldots, \zeta_m^{m-1}\alpha$. Thus the set of roots of $m_{\alpha,\mathbb{Q}}$ in $\mathbb{C}$ is either $\{\alpha\}$ or $\{\alpha, \zeta_m^{m/2}\alpha\}$ (the latter only being a possibility when m is even), i.e. either $m_{\alpha,\mathbb{Q}}(x) = x - \alpha$ or $m_{\alpha,\mathbb{Q}}(x) = (x-\alpha)(x+\alpha)$. In the former case one has $\alpha \in \mathbb{Q}$, and in the latter case one has $\alpha^2 \in \mathbb{Q}$.