QUIZ 4, VERSION A, MATH100B, WINTER 2021

1. Let $\zeta_n := e^{2\pi i/n}$.

   (a) (2 points) Prove that $\mathbb{Q}[\zeta_n]/\mathbb{Q}$ is Galois.

   Outline of solution. One can show that $\mathbb{Q}[\zeta_n]$ is the splitting field of $x^n - 1$ over $\mathbb{Q}$. Separability is automatic as we are in characteristic 0, or alternatively one can directly see that $x^n - 1$ does not have multiple zeros.

   (b) (2 points) Prove that $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\zeta_n])$ is abelian.

   Outline of solution. One can prove that the map $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\zeta_n]) \to \mathbb{Z}_n^{\times}$, taking $\theta \mapsto [i]_n$ whenever $\theta(\zeta_n) = \zeta_n^i$, is an isomorphism. In particular, $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\zeta_n])$ is abelian.

   (c) (2 points) Prove that $F/\mathbb{Q}$ is Galois for every $F \in \mathrm{Int}(\mathbb{Q}[\zeta_n]/\mathbb{Q})$.

   Solution. By the fundamental theorem of Galois theory, an intermediate subfield F of $\mathbb{Q}[\zeta_n]/\mathbb{Q}$ is Galois over $\mathbb{Q}$ if and only if the corresponding subgroup of $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\zeta_n])$ is normal. By part (b) this is always the case.

   (d) (2 points) Prove that $\mathbb{Q}(\sqrt[3]{2})$ is not a subfield of $\mathbb{Q}[\zeta_n]$ for any positive integer n.

   Solution. If $\mathbb{Q}(\sqrt[3]{2})$ were a subfield of $\mathbb{Q}[\zeta_n]$ then it would be Galois over $\mathbb{Q}$ by part (c), but we have seen that $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal.

2. Suppose E/F is a field of characteristic $p > 0$ and E/F is a field extension. Suppose $\gcd([E : F], p) = 1$.

   (a) (4 points) Prove that $m_{\alpha,F}(x)$ is separable in $F[x]$ for every $\alpha \in E$.

   Solution. We have proven that one can write $m_{\alpha,F}(x) = h(x^{p^k})$ for some irreducible, separable polynomial $h \in F[x]$ and some $k \in \mathbb{Z}^{\geq 0}$. As a result one sees that

   $$[F[\alpha] : F] = \deg(m_{\alpha,F}) = p^k \cdot \deg(h).$$

   Thus p^k divides $[F[\alpha] : F]$ and then by tower law one also obtains $p^k | [E : F]$. This contradicts our original hypothesis unless $k = 0$, but then $m_{\alpha,F}(x) = h(x)$, which is separable.

   (b) (2 points) Prove that E/F is a separable extension.

   Solution. By definition E/F is separable if and only if $m_{\alpha,F}(x)$ is separable in $F[x]$ for every $\alpha \in E$, and this is exactly what we proved in (a).

3. Suppose $f(x) \in \mathbb{Q}[x]$ is irreducible and it has both a real and non-real complex zero. Suppose $E \subseteq \mathbb{C}$ is a splitting field of f over $\mathbb{Q}$.

   (a) (2 points) Let $F := E \cap \mathbb{R}$. Prove that $[E : F] = 2$.

   Solution. Consider complex conjugation $\tau : \mathbb{C} \to \mathbb{C}$, i.e. $\tau(z) = \bar{z}$. Because $E/\mathbb{Q}$ is separable, one has $\tau(E) = E$ and so $\tau|_E \in \mathrm{Aut}_{\mathbb{Q}}(E)$. Notice then F is exactly equal to $\mathrm{Fix}(\langle \tau|_E \rangle)$, and thus we have

   $$[E : F] = [E : \mathrm{Fix}(\langle \tau|_E \rangle)] = |\langle \tau|_E \rangle| = 2.$$

   (Notice the fact that $o(\tau|_E) = 2$ is dependent on the fact that f has a non-real complex solution.)

(b) (4 points) Prove that $F/\mathbb{Q}$ is not a normal extension.

Solution. By assumption f has a zero in F, but f does not split in F because f has a non-real complex zero by hypothesis. Because f is irreducible, this violates the condition (3) for an extension to be normal as given in Theorem 22.2.1 (notice that if $\alpha \in F$ is a real zero of f then $f(x) = m_{\alpha,\mathbb{Q}}(x)$.)

4. (10 points) Suppose $f(x) \in \mathbb{Q}[x]$ is monic, irreducible and $\deg(f) = p$ is prime. Suppose $E \subseteq \mathbb{C}$ is a splitting field of f over $\mathbb{Q}$ and $\alpha \in E$ is a zero of f. Prove there is a $\theta \in \operatorname{Aut}_{\mathbb{Q}}(E)$ such that

$$f(x) = \prod_{i=0}^{p-1}(x - \theta^i(\alpha)).$$

Outline of solution. If we let R denote the roots of f in E then $\theta \mapsto \theta|_R$ defines an injective homomorphism $\operatorname{Aut}_{\mathbb{Q}}(E) \to S_R \simeq S_p$, and in this way we identify $\operatorname{Aut}_{\mathbb{Q}}(E)$ with a subgroup of S_p. Because f is irreducible one has $[\mathbb{Q}[\alpha] : \mathbb{Q}] = \deg(f) = p$, and by the tower law one then sees that p divides $[E : \mathbb{Q}]$. One can see that $E/\mathbb{Q}$ is Galois (separability is automatic because we are in characteristic 0) so one has $[E : \mathbb{Q}] = |\operatorname{Aut}_{\mathbb{Q}}(E)|$, and thus p divides $|\operatorname{Aut}_{\mathbb{Q}}(E)|$. Thus by Cauchy's theorem $\operatorname{Aut}_{\mathbb{Q}}(E)$ has an element of order p. Under the identification of $\operatorname{Aut}_{\mathbb{Q}}(E)$ with S_p this says that $\operatorname{Aut}_{\mathbb{Q}}(E)$ contains a cycle of length p (these are the only elements of order p in S_p). If we call this element θ then this means that $\alpha, \theta(\alpha), \cdots, \theta^{p-1}(\alpha)$ are all distinct roots of f, and then one gets the equality above by generalized factor theorem.