# QUIZ 5, VERSION B, MATH100B, WINTER 2021

Carefully state theorems that you are using.

1. (3 points) Suppose $F$ is a field extension of $\mathbb{Q}$ and $[F : \mathbb{Q}] = 8$. Prove that $x^3 - 3$ is irreducible in $F[x]$.

2. Suppose $p$ is a prime and $n$ is a positive integer. We know that
$$\sigma_{p,n} : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}, \quad \sigma_{p,n}(a) := a^p$$
is an element of $\mathrm{Aut}_{\mathbb{Z}_p}(\mathbb{F}_{p^n})$.
   (a) (2 points) Prove that the order of $\sigma_{p,n}$ is $n$.
   (b) (3 points) Prove that $\mathrm{Aut}_{\mathbb{Z}_p}(\mathbb{F}_{p^n})$ is a cyclic group generated by $\sigma_{p,n}$.

3. Suppose $f(x) \in \mathbb{Q}[x]$ is a monic irreducible polynomial and $\deg f = p$ is a prime number. Suppose $E \subseteq \mathbb{C}$ is a splitting field of $f$ over $\mathbb{Q}$, and $\alpha \in E$ is a zero of $f$.
   (a) (2 points) Prove that $[\mathbb{Q}[\alpha] : \mathbb{Q}] = p$.
   (b) (1 points) Prove that $p$ divides $[E : \mathbb{Q}]$.
   (c) (4 points) Prove that $\mathrm{Aut}_{\mathbb{Q}}(E)$ has an element of order $p$.

4. Suppose $F$ is a field and $n$ is a positive integer. Suppose that the characteristic of $F$ is either 0 or a prime which does not divide $n$. Let $\Phi_n(x)$ be the $n$-th cyclotomic polynomial and view it as an element of $F[x]$. Suppose $E$ is a splitting field of $\Phi_n$ over $F$.
   (a) (2 points) Prove that $x^n - 1$ does not have multiple zeros in $E$.
   (b) (2 points) Suppose $\zeta \in E$ is a zero of $x^d - 1$ where $d$ is a positive integer less than $n$. Prove that $\Phi_k(\zeta) = 0$ for some $k \neq n$.
   (c) (5 points) Prove that $\zeta \in E$ is a zero of $\Phi_n(x)$ if and only if the multiplicative order of $\zeta$ is $n$.
   (d) (2 points) Suppose $\zeta \in E$ is a zero of $\Phi_n(x)$. Prove that $E = F[\zeta]$.
   (e) (4 points) Prove that $\mathrm{Aut}_F(E)$ is isomorphic to a subgroup $\mathbb{Z}_n^\times$.
   (f) (2 bonus points) Prove that if in the above setting $F = \mathbb{Z}_p$, then $\mathrm{Aut}_{\mathbb{Z}_p}(E)$, as a subgroup of $\mathbb{Z}_n^\times$, is generated by $[p]_n$.