MODERN ALGEBRA II SPRING 2019:
TWELFTH PROBLEM SET

1. Let $E = F(\alpha, \beta)$ be a finite extension of the field $F$, so that $\alpha$ and $\beta$ are algebraic over $F$. Let $f = \text{irr}(\alpha, F)$ and let $g = \text{irr}(\beta, F)$. Suppose that $g$ is irreducible in $F(\alpha)[x]$. Show that $f$ is irreducible in $F(\beta)[x]$.
(Hint: let $d = \deg f$ and let $e = \deg g$. What is $[F(\alpha, \beta) : F]$?)

2. Let $F$ be a field of characteristic zero, let $f \in F[x]$ be an irreducible polynomial of degree $n$, and let $E$ be the splitting field of $f$. We have seen that, if $G = \text{Gal}(E/F)$, then $n$ divides the order of $G$ and the order of $G$ divides $n!$. Does $G$ necessarily contain an element of order exactly $n$? (Consider the case $F = \mathbb{Q}$ and $f = x^4 - 10x^2 + 1$.)

3. (Cyclotomic extensions.) Let $F$ be a field of characteristic zero and let $n \in \mathbb{N}$.

(ii) Let $K$ be an extension field of $F$ such that $x^n - 1$ is a product of linear factors in $K$. Let $\zeta$ be a primitive $n$th root of unity, i.e. a generator for the cyclic group of all $n$th roots of unity in $K$, and set $E = F(\zeta)$. In case $F = \mathbb{Q}$ and $K = \mathbb{C}$, we set $\zeta_n = e^{2\pi i/n}$.
Show that $E$ contains all $n$ distinct roots of $x^n - 1$, and hence that $E$ is a splitting field for $x^n - 1$ over $F$.

(ii) Let $\sigma \in \text{Gal}(E/F)$. Show that $\sigma(\zeta) = \zeta^i$ for a unique $i \in (\mathbb{Z}/n\mathbb{Z})^*$. The main point here is to show that $i$ must be relatively prime to $n$, or equivalently that the order of $\sigma(\zeta)$ is $n$. Finally show that the function

$$\sigma \in \text{Gal}(E/F) \mapsto i \in (\mathbb{Z}/n\mathbb{Z})^*,$$

where $\sigma(\zeta) = \zeta^i$, defines an injective homomorphism from $\text{Gal}(E/F)$ to $(\mathbb{Z}/n\mathbb{Z})^*$. In particular, $\text{Gal}(E/F)$ is abelian.

(iii) We have seen that, for $F = \mathbb{Q}$ and $n = p$ a prime number, $\Phi_p(x) = (x^p - 1)/(x - 1) \in \mathbb{Q}[x]$ and $\Phi_p(x)$ is irreducible, by the Eisenstein criterion. Using this fact, show that $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^*$, which is cyclic of order $p - 1$. (Warning: you must use the irreducibility of $\Phi_p$ in some way.)

(Note: As we have already mentioned, one can show that the polynomial

$$\Phi_n(x) = \prod_{i \in (\mathbb{Z}/n\mathbb{Z})^*} (x - \zeta^i)$$

has coefficients in \( \mathbb{Q} \) and is always irreducible in \( \mathbb{Q}[x] \). It then follows that \([\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)\) and that \( \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \) is isomorphic to \((\mathbb{Z}/n\mathbb{Z})^*\).

4. \((n^{th} \text{ root extensions})\) Let \( F \) be a field of characteristic zero and suppose that \( F \) contains all of the \( n^{th} \) roots of unity, i.e. that \( \#(\mu_n(F)) = n \) (here \( \#(\mu_n(F)) \) is the number of \( n^{th} \) roots of unity in \( F \)). Let \( f = x^n - a \) for some \( a \in F, \ a \neq 0 \). Let \( E \) be an extension field of \( F \) and let \( \alpha \in E \) be such that \( \alpha^n = a \). Finally, assume that \( E = F(\alpha) \).

(i) Show that \( E \) is a splitting field for \( f \) over \( F \).

(ii) Let \( \sigma \in \text{Gal}(E/F) \). Show that \( \sigma(\alpha) = \zeta \cdot \alpha \) for a unique \( n^{th} \) root of unity \( \zeta \).

(iii) Define the function
\[
\sigma \in \text{Gal}(E/F) \mapsto \zeta,
\]
where \( \zeta \) is the unique \( n^{th} \) root of unity such that \( \sigma(\alpha) = \zeta \cdot \alpha \). In other words,
\[
\rho(\sigma) = \frac{\sigma(\alpha)}{\alpha}.
\]
Show that \( \rho \) does not depend on the choice of \( \alpha \) (i.e. the particular choice of a root of \( x^n - a \)) and that \( \rho \) is an injective homomorphism from \( \text{Gal}(E/F) \) to the multiplicative group of all \( n^{th} \) roots of unity in \( E \), which is cyclic of order \( n \). Hence \( \text{Gal}(E/F) \) is a cyclic group of order dividing \( n \).

(iv) Under the above assumptions, what is \( \text{Gal}(E/F) \) when \( F = \mathbb{Q}(i) \) and \( f = x^4 - 2 \) (hence \( E = \mathbb{Q}(i, \sqrt{2}) \))? What is \( \text{Gal}(E/F) \) when \( F = \mathbb{Q}(i, \sqrt{2}) \) and \( f = x^4 - 2 \) (hence \( E = \mathbb{Q}(i, \sqrt{2}) \))?