Proposition. *1. Let K/F be Galois [possibly infinite], E be an intermediate extension, $G \stackrel{\text{def}}{=} \mathrm{Gal}(K/F)$, $H \stackrel{\text{def}}{=} \mathrm{Gal}(K/E)$ [and so $H \leq G$], $\mathrm{Emb}_{E/F} = \{\sigma_i \ : \ i \in I\}$ [for some set of indices I], and $\tilde{\sigma}_i$ an extension of σ_i to K [and so $\tilde{\sigma}_i \in G$, since K/F is normal]. Then, $\{\tilde{\sigma}_i \ : \ i \in I\}$ is a complete set of distinct representatives of left cosets of H in G.*

2. Let α be algebraic over F, $d \stackrel{\text{def}}{=} [F[\alpha] : F]_{\text{ins}}$, and $\mathrm{Emb}_{F[a]/F} = \{\alpha_1, \dots, \sigma_n\}$ [and so $n = [F[\alpha] : F]_{\text{sep}}$]. Then, $m_{\alpha,F} = \left[\prod_{i=1}^n (x - \sigma_i(\alpha))\right]^d$.

Proof. Part 1 was done in class.

First suppose that α is *separable* over F, i.e., $d = 1$. Let K/F be the Galois closure (i.e., normal closure) of $F[\alpha]/F$, $G \stackrel{\text{def}}{=} \mathrm{Gal}(K/F)$, $H \stackrel{\text{def}}{=} \mathrm{Gal}(K/F[\alpha])$, and $f \stackrel{\text{def}}{=} \prod_{i=1}^n (x - \sigma_i(\alpha))$. [We need to show $f = m_{\alpha,F}$.]

If $\tilde{\sigma}_i$ is an extension of σ_i to K [and so $\tilde{\sigma}_i \in G$], then $f = \prod_{i=1}^n (x - \tilde{\sigma}_i(\alpha))$. [Note that $f \in K[x]$.]

From part 1, we know that $\mathcal{S} \stackrel{\text{def}}{=} \{\tilde{\sigma}_i H \ : \ i = 1, \dots, n\}$ is a complete set of representatives of left cosets of H in G, and so [as we've seen in group theory], for all $\sigma \in G$, we have that $\sigma\mathcal{S} = \{\sigma\tilde{\sigma}_i H \ : \ i = 1, \dots, n\}$ is simply a permutation of $\mathcal{S}$. This implies there is some permutation $\phi \in S_n$ such that for any i we have that $\sigma\tilde{\sigma}_i = \tilde{\sigma}_{\phi(i)}\tau_i$, for some $\tau_i \in H$. Then,

$$f^\sigma = \prod_{i=1}^n (x - \sigma(\tilde{\sigma}_i(\alpha))) = \prod_{i=1}^n (x - \tilde{\sigma}_{\phi(i)}(\tau_i(\alpha))) = \prod_{i=1}^n (x - \tilde{\sigma}_{\phi(i)}(\alpha)) = \prod_{i=1}^n (x - \tilde{\sigma}_i(\alpha)) = f.$$

Since $\sigma \in G$ was arbitrary [and the fixed field of G is F], we have that $f \in F[x]$.

Also, since the identity map is in $\mathrm{Emb}_{F[\alpha]/F}$, we have that $f(\alpha) = 0$.

Thus, since f is monic, $f(\alpha) = 0$, $\deg(f) = n = [F[\alpha] : F] = \deg(m_{\alpha,F})$ [since we are assuming α is separable over F], we must have $f = m_{\alpha,F}$.

Now suppose that α is *inseparable* with $\mathrm{char}(F) = p > 0$ and $d = p^k$, for some $k \geq 1$. Then $\beta \stackrel{\text{def}}{=} \alpha^{p^k}$ is separable over F. Let $E \stackrel{\text{def}}{=} F[\beta]$. Then, E/F is separable [and $F[\alpha]/E$ is purely inseparable]. Moreover, we have that $\mathrm{Emb}_{E/F} = \{\sigma_i|_E \ : \ i = 1, \dots, n\}$ [as $\mathrm{Emb}_{K/F}$

and $\mathrm{Emb}_{E/F}$ have the same number of elements and every embedding of E/F has a *unique* extension to $F[\alpha]$, as $F[\alpha]/E$ has separable degree 1].

Then, by the separable case done above, we have that

$$m_{\beta,F} = \prod_{i=1}^{n} (x - \sigma_i|_E(\beta)) = \prod_{i=1}^{n} (x - \sigma_i(\beta)) = \prod (x - \sigma_i(\alpha)^{p^k}).$$

Now, let $f \stackrel{\text{def}}{=} m_{\beta,F}(x^{p^k}) = [\prod_{i=1}^{n}(x - \sigma_i(\alpha))]^{p^k}$. Then, $f \in F[x]$ [as $m_{\beta,F} \in F[x]$], is monic, and $f(\alpha) = m_{\beta,F}(\alpha^{p^k}) = m_{\beta,F}(\beta) = 0$. Also, $\deg(f) = p^k \cdot n = [F[\alpha] : F] = m_{\alpha,F}$. Hence $f = m_{\alpha,F}$.

$\square$