3.3 Tutorial 1 NNEW MAST30005 Semester 1, 2024: Last week's theorems

Last week we covered the following theorems. Write careful proofs of each.

Proposition 3.1. *Let $\mathbb{K}$ be a field and let H be a subgroup of $\mathrm{Aut}(\mathbb{K})$. Then $\mathbb{K}^H$ is a subfield of $\mathbb{K}$.*

Theorem 3.2. *Let $\varphi\colon A \to R$ be a ring homomorphism. Let $K = \ker(\varphi)$. Then the function*

$$\begin{array}{ccc} \dfrac{A}{\ker(\varphi)} & \to & \mathrm{im}(\varphi) \\ a+K & \mapsto & \varphi(a) \end{array} \qquad \textit{is a ring isomorphism.}$$

Proposition 3.3. *Let $\mathbb{F}$ be a subfield of a field $\mathbb{K}$ and let $\alpha \in \mathbb{K}$. Let $\mathbb{F}[x] \xrightarrow{\mathrm{ev}_{\alpha,\mathbb{F}}} \mathbb{K}$ be the evaluation homomorphism. Let $\mathbb{F}(\alpha)$ be the smallest subfield of $\mathbb{K}$ containing $\mathbb{F}$ and α. Let*

$$\mathbb{F}[\alpha] = \mathrm{im}(\mathrm{ev}_{\alpha,\mathbb{F}}) \qquad \textit{and let} \quad m_{\alpha,\mathbb{F}}(x) = c_0 + c_1 x + \cdots c_{\ell-1}x^{\ell-1} + x^\ell \quad \in \mathbb{F}[x]$$

be such that

$$\ker(\mathrm{ev}_{\alpha,\mathbb{F}}) = (m_{\alpha,\mathbb{F}}(x)), \qquad \textit{where} \quad (m_{\alpha,\mathbb{F}}(x)) = m_{\alpha,\mathbb{F}}(x)\mathbb{F}[x] = \{m_{\alpha,\mathbb{F}}(x)g \mid g \in \mathbb{F}[x]\}.$$

Then

$$\mathbb{F}(\alpha) = \mathbb{F}[\alpha] \cong \frac{\mathbb{F}[x]}{(m_{\alpha,\mathbb{F}}(x))},$$

and, as a vector space over $\mathbb{F}$,

$$\mathbb{F}(\alpha) \qquad \textit{has } \mathbb{F}\textit{-basis} \quad \{1, \alpha, \alpha^2, \ldots, \alpha^{\ell-1}\}.$$

Theorem 3.4. *Let $\mathbb{E}$ be a subfield of $\mathbb{K}$ and assume that there exists $f \in \mathbb{E}[x]$ such that $\mathbb{K}$ is the splitting field of f over $\mathbb{E}$. Then the map*

$$\begin{array}{ccc} \{\textit{field inclusions } \mathbb{F} \subseteq \mathbb{E} \subseteq \mathbb{K}\} & \longleftrightarrow & \{\textit{group inclusions } \mathrm{Aut}_{\mathbb{E}}(\mathbb{K}) \supseteq H \supseteq \{1\}\} \\ \mathbb{F} & \longmapsto & \mathrm{Aut}_{\mathbb{F}}(\mathbb{K}) \\ \mathbb{K}^H & \longleftarrow\!\shortmid & H \end{array}$$

is an isomorphism of posets.

Some worked steps for the proof of Theorem 3.3:

HW 1: Show that $\mathrm{im}(\mathrm{ev}_{\alpha,\mathbb{F}}) = \mathbb{F}[\alpha]$.

Proof. This is clearly true.
This proof, as it is, should get 0 marks (or maybe negative marks). It is offensive to the reader that is trying hard and earnestly to learn this stuff and that reader does not deserve insults. □

HW 2: Show that $\mathbb{F}\text{-span}\{1, \alpha, \alpha^2, \ldots, \alpha^{\ell-1}\} = \mathbb{F}[\alpha]$.

Proof. To show: $\mathbb{F}\text{-span}\{1, \alpha, \ldots, \alpha^{\ell-1}\} = \mathbb{F}[\alpha]$.
Since $\mathbb{F}[\alpha] = \mathrm{im}(\mathrm{ev}_{\alpha,\mathbb{F}})$ and $\mathbb{F}[x]$ is spanned by $\{1, x, x^2, \ldots\}$ then $\mathbb{F}[\alpha]$ is spanned by $\{1, \alpha, \alpha^2, \ldots\}$.
If $k \in \mathbb{Z}_{\geq 0}$ then $\alpha^{\ell+k} = \alpha^k(-c_0 - \cdots - c_{\ell-1}\alpha^{\ell-1}) \in \mathbb{F}\text{-span}\{1, \alpha, \ldots, \alpha^{\ell+k-1}\}$
So $\mathbb{F}[\alpha]$ is spanned by $\{1, \alpha, \ldots, \alpha^{\ell-1}\}$.
This proof, as it is, shold not get full marks. It has too many skipped steps and the writing is rather incomprehensible. □

HW 3: Show that $\{1, \alpha, \alpha^2, \ldots, \alpha^{\ell-1}\}$ is $\mathbb{F}$-linearly independent in $\mathbb{F}[\alpha]$.

Proof. (c) To show: $\{1, \alpha, \ldots, \alpha^{\ell-1}\}$ is linearly independent.
Assume that $a_0 + a_1\alpha + \cdots a_{\ell-1}\alpha^{\ell-1} = 0$.
Then $a_0 + a_1x + \cdots + a_{\ell-1}x^{\ell-1} \in \ker(\mathrm{ev}_\alpha)$.
So there exists $f \in \mathbb{F}[x]$ such that $a_0 + a_1x + \cdots + a_{\ell-1}x^{\ell-1} = f \cdot m_{\alpha,\mathbb{F}}(x)$.
Since $\deg(m_{\alpha,\mathbb{F}}(x)) = \ell$ and $\deg(a_0 + a_1x + \cdots + a_{\ell-1}x^{\ell-1}) \leq \ell - 1$

$$\text{then} \qquad f = 0 \text{ and } a_0 = a_1 = \cdots = a_{\ell-1} = 0.$$

So $\{1, \alpha, \ldots, \alpha^{\ell-1}\}$ is linearly independent. □

HW 4: Show that $m_{\alpha,\mathbb{F}}(x)$ exists.

Proof. To show: $m_{\alpha,\mathbb{F}}(x)$ exists (i.e. that $\ker(\mathrm{ev}_\alpha)$ is generated by a single element).
Let $m(x) = c_0 + c_1x + \cdots + c_\ell x^\ell \in \mathbb{F}[x]$ be a minimal degree element of $\ker(\mathrm{ev}_\alpha)$ with $c_\ell \neq 0$.
Let

$$m_{\alpha,\mathbb{F}}(x) = c_\ell^{-1}m(x) = a_0 + a_1x + \cdots + a_{\ell-1}x^{\ell-1} + x^\ell.$$

To show: If $p(x) \in \ker(\mathrm{ev}_\alpha$ then there exists $g(x) \in \mathbb{F}[x]$ such that $p(x) = m_{\alpha,\mathbb{F}}](x)g(x)$.
Assume $p(x) \in \ker(\mathrm{ev}_\alpha)$.
Write $p(x) = m_{\alpha,\mathbb{F}}(x)g(x) + r(x)$, with $\deg(r(x)) < \ell$.
To show: $r(x) = 0$.
Since $p(x) \in \ker(\mathrm{ev}_\alpha)$ and $m_{\alpha,\mathbb{F}}(x)g(x) \in \ker(\mathrm{ev}_\alpha)$ then $r(x) = p(x) - m_{\alpha,\mathbb{F}}(x)g(x) \in \ker(\mathrm{ev}_\alpha)$.
Since $m_{\alpha,\mathbb{F}}(x)$ is minimal degree of elements of $\ker(\mathrm{ev}_\alpha)$ then $r(x) = 0$.
So there exists $g(x) \in \mathbb{F}[x]$ such that $p(x) = m_{\alpha,\mathbb{F}}(x)g(x)$.
So $p(x) \in (m_{\alpha,\mathbb{F}}(x))$. □

HW 5: Show that $\mathbb{F}(\alpha) = \mathbb{F}[\alpha]$.

Proof. To show: $\mathbb{F}[\alpha]$ is a field.
To show: If $\beta \in \mathbb{F}[\alpha]$ and $\beta \neq 0$ then $\beta^{-1} \in \mathbb{F}[\alpha]$.
Assume $\beta \in \mathbb{F}[\alpha]$ and $\beta \neq 0$.
The $\mathbb{F}$-linear transformation of $\mathbb{F}[\alpha]$ given by multiplication by β is

$$\begin{array}{ccc} \mathbb{F}[\alpha] & \xrightarrow{\cdot\beta} & \mathbb{F}[\alpha] \\ \gamma & \mapsto & \gamma\beta \end{array}$$

If $\gamma \in \mathbb{F}[\alpha]$ and $\gamma\beta = 0$ then $\gamma = -0$.
So $\ker(\cdot\beta) = 0$.
Since $\mathbb{F}[\alpha]$ is a finite dimensional vector space over $\mathbb{F}$ then $\mathrm{im}(\cdot\beta) = \mathbb{F}[\alpha]$.
So the linear transformation $\cdot\beta$ is surjective.
So $1 \in \mathrm{im}(\cdot\beta)$.
So there exists $\gamma \in \mathbb{F}[\alpha]$ such that $\gamma\beta = 1$.
Let $\beta^{-1} = \gamma$. $\square$

Some worked steps for the proof of Theorem 3.4:
Let $\mathbb{K}$ be a field.

- Let $\mathbb{F}$ be a subfield of $\mathbb{K}$. The **Galois group of** $\mathbb{K}$ **over** $\mathbb{F}$ is

$$\mathrm{Gal}(\mathbb{F}) = \mathrm{Aut}_{\mathbb{F}}(\mathbb{K}) = \{\sigma \in \mathrm{Aut}(\mathbb{K}) \mid \text{if } e \in \mathbb{F} \text{ then } \sigma(e) = e\}.$$

- Let H be a subgroup of $\mathrm{Aut}(\mathbb{K})$. The **fixed field of** H is

$$\mathrm{Fix}(H) = \mathbb{K}^H = \{e \in \mathbb{K} \mid \text{if } \sigma \in H \text{ then } \sigma(e) = e\}.$$

HW 1: Show that $\mathrm{Aut}_{\mathbb{E}}(\mathbb{K})$ is a subgroup of $\mathrm{Aut}(\mathbb{K})$.

HW 2: Show that $\mathbb{K}^H$ is a subfield of $\mathbb{K}$.

HW 3: Let $\mathbb{F} \subseteq \mathbb{K}$ be a subfield of $\mathbb{K}$. Show that $\mathrm{Fix}(\mathrm{Gal}(\mathbb{F}) \supseteq \mathbb{F}$.

Proof. To show: If $y \in \mathbb{F}$ then $y \in \mathrm{Fix}(\mathrm{Gal}(\mathbb{F}))$.
Assume $y \in \mathbb{F}$,
To show: $y \in \mathrm{Fix}(\mathrm{Gal}(\mathbb{F}))$.
To show: If $\sigma \in \mathrm{Gal}(\mathbb{F})$ then $\sigma(y) = y$.
Assume $\sigma \in \mathrm{Gal}(\mathbb{F})$.
To show: $\sigma(y) = y$.
Since $y \in F$ and $\sigma \in Aut_{\mathbb{F}}(\mathbb{K})$ then $\sigma(y) = y$.
So $y \in \mathrm{Fix}(\mathrm{Gal}(\mathbb{F}))$.
So $\mathrm{Fix}(\mathrm{Gal}(\mathbb{F})) \supseteq \mathbb{F}$. $\square$

HW 4: Let H be a subgroup of $\mathrm{Aut}(\mathbb{K})$. Show that $\mathrm{Gal}(\mathrm{Fix}(H)) \supseteq H$.

Proof. To show: If $\sigma \in H$ then $\sigma \in \mathrm{Gal}(\mathrm{Fix}(H))$.
Assume $\sigma \in H$.
To show: $\sigma \in \mathrm{Gal}(\mathrm{Fix}(H))$.
To show: If $y \in \mathrm{Fix}(H)$ then $\sigma(y) = y$.
Assume $y \in \mathrm{Fix}(H)$.
To show: $\sigma(y) = y$.
Since $y \in \mathrm{Fix}(H)$ then y satisfies: If $\sigma \in H$ then $\sigma(y) = y$.
So $\sigma(y) = y$.
So, If $\sigma \in H$ then $\sigma \in \mathrm{Gal}(\mathrm{Fix}(H))$.
So $\mathrm{Gal}(\mathrm{Fix}(H)) \supseteq H$. □

HW 5: Let $\mathbb{F}$ and $\mathbb{G}$ be subfields of $\mathbb{K}$ and assume that $\mathbb{F} \subseteq \mathbb{G}$. Show that $\mathrm{Gal}(\mathbb{G}) \subseteq \mathrm{Gal}(\mathbb{F})$.

Proof. Assume that $\mathbb{F} \subseteq \mathbb{G}$.
To show: $\mathrm{Gal}(\mathbb{G}) \subseteq \mathrm{Gal}(\mathbb{F})$.
To show: If $\sigma \in \mathrm{Gal}(\mathbb{G})$ then $\sigma \in \mathrm{Gal}(\mathbb{F})$.
Assume $\sigma \in \mathrm{Gal}(\mathbb{G})$.
To show: $\sigma \in \mathrm{Gal}(\mathbb{F})$.
To show: If $y \in \mathbb{F}$ then $\sigma(y) = y$.
Assume$y \in \mathbb{F}$.
To show: $\sigma(y) = y$.
Since $\sigma \in \mathrm{Aut}_{\mathbb{G}}(\mathbb{K})$ and $y \in \mathbb{F}$ and $\mathbb{F} \subseteq \mathbb{G}$ then $\sigma(y) = y$.
So $\sigma \in \mathrm{Gal}(\mathbb{F})$.
So $\mathrm{Gal}(\mathbb{G}) \subseteq \mathrm{Gal}(\mathbb{F})$. □

HW 6:. Let G and H be subgroups of $\mathrm{Aut}(\mathbb{K}))$ and assume that $G \subseteq H$. Show that $\mathrm{Fix}(G) \supseteq \mathrm{Fix}(H)$.

Proof. Assume $G \subseteq H$.
To show: $\mathrm{Fix}(G) \supseteq \mathrm{Fix}(H)$.
To show: If $y \in \mathrm{Fix}(G)$ then $y \in \mathrm{Fix}(H)$.
Assume $y \in \mathrm{Fix}(G)$.
To show: $y \in \mathrm{Fix}(H)$.
To show: if $\sigma \in H$ then $\sigma(y) = y$.
Assume $\sigma \in H$.
To show: $\sigma(y) = y$.
Since $y \in \mathrm{Fix}(G)$ and $\sigma \in H$ and $H \subseteq G$ then $\sigma(y) = y$.
So $y \in \mathrm{Fix}(H)$.
So $\mathrm{Fix}(G) \supseteq \mathrm{Fix}(H)$. □

HW 7:. Let H be a subgroup of $\mathrm{Aut}(\mathbb{K}))$. Show that $\mathrm{Fix}(\mathrm{Gal}(\mathrm{Fix}(H))) = \mathrm{Fix}(H)$.

Proof.
To show: (a) $\mathrm{Fix}(\mathrm{Gal}(\mathrm{Fix}(H))) \subseteq \mathrm{Fix}(H)$.
(b) $\mathrm{Fix}(\mathrm{Gal}(\mathrm{Fix}(H))) \supseteq \mathrm{Fix}(H)$.

(b) By HW 4, $\mathrm{Gal}(\mathrm{Fix}(H)) \supseteq H$.
Thus, by HW 6, then $\mathrm{Fix}(\mathrm{Gal}(\mathrm{Fix}(H))) \subseteq \mathrm{Fix}(H)$.

(a) Let $\mathbb{F} = \mathrm{Fix}(H)$.
By HW 3, $\mathbb{F} \subseteq \mathrm{Fix}(\mathrm{Gal}(\mathbb{F})$.

So $\mathrm{Fix}(H) \subseteq \mathrm{Fix}(\mathrm{Gal}(\mathrm{Fix}(H)))$.

□

HW 8:. Let $\mathbb{F}$ be a subfield of $\mathbb{K}$. Show that $\mathrm{Gal}(\mathrm{Fix}(\mathrm{Gal}(\mathbb{F}))) = \mathrm{Gal}(\mathbb{F})$.

Proof.
To show: (a) $\mathrm{Gal}(\mathrm{Fix}(\mathrm{Gal}(\mathbb{F}))) \subseteq \mathrm{Gal}(\mathbb{F})$.
(b) $\mathrm{Gal}(\mathrm{Fix}(\mathrm{Gal}(\mathbb{F}))) \supseteq \mathrm{Gal}(\mathbb{F})$.

(b) By HW 3, $\mathrm{Fix}(\mathrm{Gal}(\mathbb{F})) \supseteq \mathbb{F}$.
Thus, by HW 5, then $\mathrm{Gal}(\mathrm{Fix}(\mathrm{Gal}(\mathbb{F}))) \subseteq \mathrm{Gal}(\mathbb{F})$.

(a) Let $H = \mathrm{Gal}(\mathbb{F})$.
By HW 4, $H \subseteq \mathrm{Gal}(\mathrm{Fix}(H)$.
So $\mathrm{Gal}(\mathbb{F}) \subseteq \mathrm{Gal}(\mathrm{Fix}(\mathrm{Gal}(H))$.

□

HW 9:. Let $\mathbb{F}$ be a subfield of $\mathbb{K}$ and let $\sigma \in \mathrm{Aut}(\mathbb{K})$. Show that $\mathrm{Gal}(\sigma(\mathbb{F})) = \sigma\mathrm{Gal}(\mathbb{F})\sigma^{-1}$ (subgroups of $\mathrm{Aut}(\mathbb{K})$).

Proof. Assume $\sigma \in \mathrm{Aut}(\mathbb{K})$.
To show: $\mathrm{Gal}(\sigma(\mathbb{F})) = \sigma\mathrm{Gal}(\mathbb{F})\sigma^{-1}$.
To show: (a) $\mathrm{Gal}(\sigma(\mathbb{F})) \subseteq \sigma\mathrm{Gal}(\mathbb{F})\sigma^{-1}$.
(b) $\mathrm{Gal}(\sigma(\mathbb{F})) \supseteq \sigma\mathrm{Gal}(\mathbb{F})\sigma^{-1}$

(a) To show: $\mathrm{Gal}(\sigma(\mathbb{F})) \subseteq \sigma\mathrm{Gal}(\mathbb{F})\sigma^{-1}$.
To show: If $\tau \in \mathrm{Gal}(\sigma(\mathbb{F}))$ then $\tau \in \sigma\mathrm{Gal}(\mathbb{F})\sigma^{-1}$.
Assume $\tau \in \mathrm{Gal}(\sigma(\mathbb{F}))$
To show: $\tau \in \sigma\mathrm{Gal}(\mathbb{F})\sigma^{-1}$.
To show: $\sigma^{-1}\tau\sigma \in \mathrm{Gal}(\mathbb{F})$.
To show: If $y \in \mathbb{F}$ then $\sigma^{-1}\tau\sigma(y) = y$.
Assume $y \in \mathbb{F}$.
To show: $\sigma^{-1}\tau\sigma(y) = y$.
Since $\sigma(y) \in \sigma(\mathbb{F})$ and $\tau \in \mathrm{Gal}(\sigma\mathbb{F})$ then $\tau(\sigma(y)) = \sigma(y)$ and

$$\sigma^{-1}\tau\sigma(y) = \sigma^{-1}\sigma(y) = y.$$

So $\sigma^{-1}\tau\sigma \in \mathrm{Gal}(\mathbb{F})$.
So $\tau \in \sigma\mathrm{Gal}(\mathbb{F})\sigma^{-1}$.
So $\mathrm{Gal}(\sigma(\mathbb{F})) \subseteq \sigma\mathrm{Gal}(\mathbb{F})\sigma^{-1}$.

(b) To show: $\mathrm{Gal}(\sigma(\mathbb{F})) \supseteq \sigma\mathrm{Gal}(\mathbb{F})\sigma^{-1}$.
To show: If $\tau \in \sigma\mathrm{Gal}(\mathbb{F})\sigma^{-1}$ then $\tau \in \mathrm{Gal}(\sigma(\mathbb{F}))$.
Assume $\tau \in \sigma\mathrm{Gal}(\mathbb{F})\sigma^{-1}$.
To show: $\tau \in \mathrm{Gal}(\sigma\mathbb{F})$.
To show: If $y \in \sigma(\mathbb{F})$ then $\tau(y) = y$.
Assume $y \in \sigma(\mathbb{F})$.
To show: $\tau(y) = y$.
Let $\beta \in \mathbb{F}$ such that $y = \sigma(\beta)$ and let $\gamma \in \mathrm{Gal}(\mathbb{F})$ such that $\tau = \sigma\gamma\sigma^{-1}$.

Then

$$\tau(y) = \sigma\gamma\sigma^{-1}(y) = \sigma\gamma\sigma^{-1}(\sigma(\beta)) = \sigma\gamma(\beta) = \sigma(\beta) = y.$$

So $\tau \in \mathrm{Gal}(\sigma\mathbb{F})$.

So $\mathrm{Gal}(\sigma(\mathbb{F})) \supseteq \sigma\mathrm{Gal}(\mathbb{F})\sigma^{-1}$.

So $\mathrm{Gal}(\sigma(\mathbb{F})) = \sigma\mathrm{Gal}(\mathbb{F})\sigma^{-1}$. □

HW 10:. Let H be a subgroup of $\mathrm{Aut}(\mathbb{K})$ and let $\sigma \in \mathrm{Aut}(\mathbb{K})$. Show that $\mathrm{Fix}(\sigma H\sigma^{-1}) = \sigma(\mathrm{Fix}(H))$ (subfields of $\mathbb{K}$).

Proof. Assume $\sigma \in \mathrm{Aut}(\mathbb{K})$.
To show: $\mathrm{Fix}(\sigma H\sigma^{-1}) = \sigma(\mathrm{Fix}(H))$.
To show: (a) $\mathrm{Fix}(\sigma H\sigma^{-1}) \subseteq \sigma(\mathrm{Fix}(H))$.
(b) $\mathrm{Fix}(\sigma H\sigma^{-1}) =\supseteq \sigma(\mathrm{Fix}(H))$.

(a) To show: $\mathrm{Fix}(\sigma H\sigma^{-1}) \subseteq \sigma(\mathrm{Fix}(H))$.
To show: If $y \in \mathrm{Fix}(\sigma H\sigma^{-1})$ then $y \in \sigma(\mathrm{Fix}(H))$.
Assume $y \in \mathrm{Fix}(\sigma H\sigma^{-1})$.
To show: $y \in \sigma(\mathrm{Fix}(H))$.
To show: $\sigma^{-1}(y) \in \mathrm{Fix}(H)$.
To show: If $\tau \in H$ then $\tau(\sigma^{-1}(y)) = \sigma^{-1}(y)$.
Assume $\tau \in H$.
To show: $\tau(\sigma^{-1}(y)) = \sigma^{-1}(y)$.
Since $y \in \mathrm{Fix}(\sigma H\sigma^{-1})$ and $\tau \in H$ then $\sigma\tau\sigma^{-1}(y) = y$ and

$$\tau\sigma^{-1}(y) = \sigma^{-1}\sigma\tau\sigma^{-1}(y) = \sigma^{-1}(y).$$

So $\sigma^{-1}(y) \in \mathrm{Fix}(H)$.
So $\mathrm{Fix}(\sigma H\sigma^{-1}) \subseteq \sigma(\mathrm{Fix}(H))$.

(b) To show: $\mathrm{Fix}(\sigma H\sigma^{-1}) \supseteq \sigma(\mathrm{Fix}(H))$.
To show: If $y \in \sigma(\mathrm{Fix}(H))$ then $y \in \mathrm{Fix}(\sigma H\sigma^{-1})$.
Assume $y \in \sigma(\mathrm{Fix}(H))$.
To show: $y \in \mathrm{Fix}(\sigma H\sigma^{-1})$.
To show: If $\tau \in \sigma H\sigma^{-1}$ then $\tau(y) = y$.
To show: Assume $\tau \in \sigma H\sigma^{-1}$.
To show: $\tau(y) = y$.
Let $\gamma \in H$ such that $\tau = \sigma\gamma\sigma^{-1}$ and let $\beta \in \mathrm{Fix}(H)$ such that $y = \sigma\beta$.
Since $\gamma \in H$ and $\beta \in \mathrm{Fix}(H)$ then $\gamma(\beta) = \beta$ and

$$\tau(y) = \sigma\gamma\sigma^{-1}(y) = \sigma\gamma\sigma^{-1}\sigma(\beta) = \sigma\gamma(\beta) = \sigma(\beta) = y.$$

So $y \in \mathrm{Fix}(\sigma H\sigma^{-1})$.
So $\mathrm{Fix}(\sigma H\sigma^{-1}) \supseteq \sigma(\mathrm{Fix}(H))$.

So $\mathrm{Fix}(\sigma H\sigma^{-1}) = \sigma(\mathrm{Fix}(H))$. □

Some steps for the proof of Theorem 3.3:

HW: Show that $\mathrm{im}(\mathrm{ev}_{\alpha,\mathbb{F}}) = \mathbb{F}[\alpha]$.

HW: Show that $\mathbb{F}\text{-span}\{1, \alpha, \alpha^2, \ldots, \alpha^{\ell-1}\} = \mathbb{F}[\alpha]$.

HW: Show that $\{1, \alpha, \alpha^2, \ldots, \alpha^{\ell-1}\}$ is linearly independent in $\mathbb{F}[\alpha]$.

HW: Show that $m_{\alpha,\mathbb{F}}(x)$ exists.

HW: Show that $\mathbb{F}(\alpha) = \mathbb{F}[\alpha]$.

Some steps for the proof of Theorem 3.4:
Let $\mathbb{K}$ be a field.

- Let $\mathbb{F}$ be a subfield of $\mathbb{K}$. The **Galois group of** $\mathbb{K}$ **over** $\mathbb{F}$ is

$$\mathrm{Gal}(\mathbb{F}) = \mathrm{Aut}_{\mathbb{F}}(\mathbb{K}) = \{\sigma \in \mathrm{Aut}(\mathbb{K}) \mid \text{if } e \in \mathbb{F} \text{ then } \sigma(e) = e\}.$$

- Let H be a subgroup of $\mathrm{Aut}(\mathbb{K})$. The **fixed field of** H is

$$\mathrm{Fix}(H) = \mathbb{K}^H = \{e \in \mathbb{K} \mid \text{if } \sigma \in H \text{ then } \sigma(e) = e\}.$$

HW: Show that $\mathrm{Aut}_{\mathbb{E}}(\mathbb{K})$ is a subgroup of $\mathrm{Aut}(\mathbb{K})$.

HW: Show that $\mathbb{K}^H$ is a subfield of $\mathbb{K}$.

HW: Let $\mathbb{F} \subseteq \mathbb{K}$ be a subfield of $\mathbb{K}$. Show that $\mathrm{Fix}(\mathrm{Gal}(\mathbb{F}) \supseteq \mathbb{F}$.

HW: Let H be a subgroup of $\mathrm{Aut}(\mathbb{K})$. Show that $\mathrm{Gal}(\mathrm{Fix}(H)) \subseteq H$.

HW: Let $\mathbb{F}$ and $\mathbb{G}$ be subfields of $\mathbb{K}$ and assume that $\mathbb{F} \subseteq \mathbb{G}$. Show that $\mathrm{Gal}(\mathbb{G}) \subseteq \mathrm{Gal}(\mathbb{F})$.

HW: Let G and H be subgroups of $\mathrm{Aut}(\mathbb{K}))$ and assume that $G \subseteq H$. Show that $\mathrm{Fix}(G) \supseteq \mathrm{Fix}(H)$.

HW: Let H be a subgroup of $\mathrm{Aut}(\mathbb{K}))$. Show that $\mathrm{Fix}(\mathrm{Gal}(\mathrm{Fix}(H))) = \mathrm{Fix}(H)$.

HW: Let $\mathbb{F}$ be a subfield of $\mathbb{K}$. Show that $\mathrm{Gal}(\mathrm{Fix}(\mathrm{Gal}(\mathbb{F}))) = \mathrm{Gal}(\mathbb{F})$.

HW: Let $\mathbb{F}$ be a subfield of $\mathbb{K}$ and let $\sigma \in \mathrm{Aut}(\mathbb{E})$. Show that $\mathrm{Gal}(\sigma(\mathbb{F})) = \sigma \mathrm{Gal}(\mathbb{F})\sigma^{-1}$ (subgroups of $\mathrm{Aut}(\mathbb{K})$).

HW: Let H be a subgroup of $\mathrm{Aut}(\mathbb{K})$ and let $\sigma \in \mathrm{Aut}(\mathbb{E})$. Show that $\mathrm{Fix}(\sigma H \sigma^{-1}) = \sigma(\mathrm{Fix}(H))$ (subfields of $\mathbb{K}$).

HW: Let $\mathbb{F}$ be a subfield of $\mathbb{K}$ and assume that $\mathbb{K} \supseteq \mathbb{F}$ is the splitting field of a polynomial $f(x) \in \mathbb{F}[x]$ over $\mathbb{F}$ and that $f(x)$ factors as

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_\ell), \qquad \text{with } \alpha_1, \ldots, \alpha_\ell \in \mathbb{K}.$$

Show that $\mathbb{K} = \mathbb{F}(\alpha_1, \ldots, \alpha_\ell)$.

HW: Let $\mathbb{F}$ be a subfield of $\mathbb{K}$ and assume that $\mathbb{K} = \mathbb{F}(\alpha_1, \ldots, \alpha_\ell)$. Show that there exists $\gamma \in \mathbb{K}$ such that $\mathbb{K} = \mathbb{F}(\gamma)$.

HW: Let $\mathbb{F}$ be a subfield of $\mathbb{K}$ and assume that $\mathbb{K} \supseteq \mathbb{F}$ is Galois. Show that there exists $\gamma \in \mathbb{K}$ such that $\mathbb{K} = \mathbb{F}(\gamma)$.

HW: Let $\mathbb{F}$ be a subfield of $\mathbb{K}$ and assume that $\mathbb{K} \supseteq \mathbb{F}$ is Galois. Let $\gamma \in \mathbb{K}$ such that $\gamma \in \mathbb{K}$ such that $\mathbb{K} = \mathbb{F}(\gamma)$. Let $G = \mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$. Show that

$$m_{\gamma,\mathbb{F}}(x) = \prod_{\beta \in G\gamma} (x - \beta).$$

HW: Let $\mathbb{F}$ be a subfield of $\mathbb{K}$ and assume that $\mathbb{K} \supseteq \mathbb{F}$ is Galois. Let $\gamma \in \mathbb{K}$ such that $\mathbb{K} = \mathbb{F}(\gamma)$. Let $G = \mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$. Show that

$$\deg(m_{\gamma,\mathbb{F}}(x)) = |G|.$$

HW: Let $\mathbb{F}$ be a subfield of $\mathbb{K}$ and assume that $\mathbb{K} \supseteq \mathbb{F}$ is Galois. Let $\gamma \in \mathbb{K}$ such that $\mathbb{K} = \mathbb{F}(\gamma)$. Let $G = \mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$. Show that

$$\dim_{\mathbb{F}}(\mathbb{K}) = |G|.$$

HW: Let $\mathbb{F}$ be a subfield of $\mathbb{K}$ and assume that $\mathbb{K} \supseteq \mathbb{F}$ is Galois. Let $\gamma \in \mathbb{K}$ such that $\mathbb{K} = \mathbb{F}(\gamma)$. Let $G = \mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$. Let $G\gamma = \{g\gamma \mid g \in G\}$. Show that

$$\begin{array}{ccc} G & \to & G\gamma \\ g & \mapsto & g\gamma \end{array}$$

HW:. Let $\mathbb{F}$ be a subfield of $\mathbb{K}$ and assume that $\mathbb{K} \supseteq \mathbb{F}$ is Galois. Let $\gamma \in \mathbb{K}$ such that $\mathbb{K} = \mathbb{F}(\gamma)$. Show that $\mathrm{Fix}(\mathrm{Gal}(\mathbb{F})) = \mathbb{F}$.

HW:. Let H be a finite subgroup of $\mathrm{Aut}(\mathbb{K})$. Show that $\mathbb{K} \supseteq \mathbb{K}^H$ is a Galois extension.

HW:. Let H be a finite subgroup of $\mathrm{Aut}(\mathbb{K})$. Show that $\mathrm{Gal}(\mathrm{Fix}(H)) = H$.