3. Доведіть, що для $x \in \mathbb{F}_{p^s}$ виконується $\mathrm{Tr}(x) = 0 \Leftrightarrow x = y - y^p$ для деякого $y \in \mathbb{F}_{p^s}$

Розглянемо лінійне над $\mathbb{F}_p$ відображення $T: \mathbb{F}_{p^s} \to \mathbb{F}_{p^s}$, $y \mapsto y - y^p$

Воно лінійне адже

$T(y_1+y_2) = (y_1 + y_2) - (y_1+y_2)^p = y_1 + y_2 - y_1^p - y_2^p =$
$= y_1 - y_1^p + y_2 - y_2^p = T(y_1) + T(y_2)$ $\forall y_1, y_2 \in \mathbb{F}_{p^s}$

$T(\lambda y) = \lambda y - (\lambda y)^p = \lambda y - \lambda^p y^p =$
$= \lambda y - \lambda y^p = \lambda(y - y^p) = \lambda T(y)$
$\forall \lambda \in \mathbb{F}_p$ $\forall y \in \mathbb{F}_{p^s}$

При цьому

$\mathrm{Ker}\, T = \{y \in \mathbb{F}_{p^s} : y - y^p = 0\} =$
$= \{y \in \mathbb{F}_{p^s} : y = y^p\} = \mathbb{F}_p$

Тоді $\dim_{\mathbb{F}_p} \mathrm{Ker}\, T = 1$

Тоді $\dim_{\mathbb{F}_p} \operatorname{Im} T = s - \dim_{\mathbb{F}_p} \operatorname{Ker} T =$
$= s - 1$

Твердження вправи еквівалентне тому, що $\operatorname{Ker} Tr = \operatorname{Im} T$

Покажемо, що $\operatorname{Im} T \subset \operatorname{Ker} Tr$

$x \in \operatorname{Im} T \iff \exists y \in \mathbb{F}_{p^s} : x = y - y^p$

$\Rightarrow Tr(x) = Tr(y - y^p) =$
$= y - y^p + (y - y^p)^p + \ldots + (y - y^p)^{p^{s-1}} =$
$= y - \cancel{y^p} + \cancel{y^p} - y^{p^2} + \ldots + \cancel{y^{p^{s-1}}} - y^{p^s} =$
$= y - y^{p^s} = 0 \Rightarrow x \in \operatorname{Ker} Tr.$

виконується для всіх елементів $\mathbb{F}_{p^s}$

Тепер помітимо, що
$\dim_{\mathbb{F}_p} \operatorname{Ker} Tr = s - \dim_{\mathbb{F}_p} \operatorname{Im} Tr =$
$= s - 1 = \dim_{\mathbb{F}_p} \operatorname{Im} T$

Маємо:

$$\left.\begin{array}{l} \operatorname{Im} T \subset \operatorname{Ker} Tr \\ \dim_{\mathbb{F}_p} \operatorname{Im} T = \dim_{\mathbb{F}_p} \operatorname{Ker} Tr \end{array}\right\} \Rightarrow$$

$\Rightarrow \operatorname{Im} T = \operatorname{Ker} Tr$

$\boxed{\checkmark}$

---

Примітка: При доведенні була використана властивість
$(a-b)^{p^d} = a^{p^d} - b^{p^d} \quad \forall a, b \in \mathbb{F}_{p^s}$
яка не доводилась на лекції
Але для непарних $p$
$(a-b)^{p^d} = (a+(-b))^{p^d} =$
$= a^{p^d} + (-1)^{p^d} b^{p^d} = a^{p^d} - b^{p^d}$
А при $p=2$ $\forall x \in \mathbb{F}_{p^s}: x = -x$
тому
$(a-b)^{p^d} = (a+b)^{p^d} = a^{p^d} + b^{p^d} =$
$= a^{p^d} - b^{p^d}$