T. 4.3

a) $\boxed{\text{Th: } f(x) = x^2 - x - 1 \in \mathbb{F}_3[x] \text{ is IRREDUCIBLE}}$

FACT: $f(x)$ of degree 2 is irreducible $\Leftrightarrow$ it has no roots in $\mathbb{F}_3$

proof $\Rightarrow$) To prove "$A \Rightarrow B$", we show that "NOT $A \Leftarrow$ NOT B"

Therefore, the proof of this fact revolves around the fact that if $f(x)$ had at least one root, it would be possible to express it as

$$f(x) = (x-a)(x-b)$$

making $f(x)$ reducible.

$\Leftarrow$) Once again, to prove "$A \Leftarrow B$" we show that "NOT $A \Rightarrow$ NOT B"

If $f(x)$ is reducible $\Rightarrow f(x) = (x-a)(x-b)$

Therefore it is indeed reducible.

So, let us see that $f(x) \in \mathbb{F}_3[x]$ has no roots:

- $f(0) = -1 \neq 0$
- $f(1) = -1 \neq 0$
- $f(2) = 1 \neq 0$

Since $0, 1, 2$ are all the possible values that x can assume, $f(x)$ indeed has no roots in $\mathbb{F}_3(x)$ and therefore is irreducible. ✓

Let $\alpha \in \mathbb{F}_3$ s.t. $f(\alpha) = 0$, i.e. $\alpha^2 - \alpha - 1 = 0$

So we know that α satisfies the property that

$$\alpha^2 - \alpha - 1 = 0 \Leftrightarrow \alpha^2 = \alpha + 1 \Leftrightarrow \alpha = \alpha^2 - 1$$

$\boxed{\text{Th: } \alpha \text{ is a generator of the multiplicative group } \mathbb{F}_9^\times}$

As seen in class, we have the following:

<u>Proposition:</u> If F is a finite field

$$\Rightarrow F^\times \text{ (the multiplic. group) is cyclic of order } p^n - 1.$$

Therefore, we already know that $\mathbb{F}_9^\times$ will have 8 elements.

To see if α is a generator of $\mathbb{F}_9^\times$, I compute it's powers α^i for $i=0,\dots,8$ (expecting $\alpha^8 = \alpha^0 = 1$).

Indeed $\mathbb{F}_9^\times$ is a group w.r.t. the multiplication and

$$\text{if } \{\alpha^i : i=0,\dots,7\} = \mathbb{F}_9^\times = \mathbb{F}_9 \setminus \{0\} \Rightarrow \langle \alpha \rangle = \mathbb{F}_9^\times \Rightarrow \alpha \text{ is a generator.}$$

Computations:

$$\begin{aligned}
\alpha^0 &= 1 = 1 + 0\cdot\alpha \\
\alpha^1 &= \alpha = 0 + 1\cdot\alpha \\
\alpha^2 &= \alpha + 1 = 1 + 1\cdot\alpha \\
\alpha^3 &= \alpha\cdot\alpha^2 = \alpha(\alpha+1) = \alpha^2 + \alpha = 1 + \alpha + \alpha = 1 + 2\cdot\alpha \\
\alpha^4 &= \alpha\cdot\alpha^3 = \alpha(1+2\alpha) = \alpha + 2\alpha^2 = \alpha + 2(1+\alpha) = 2 + 3\alpha \equiv 2 + 0\cdot\alpha \\
\alpha^5 &= \alpha\cdot\alpha^4 = 2\alpha = 0 + 2\cdot\alpha \\
\alpha^6 &= \alpha\cdot\alpha^5 = 2\alpha^2 = 2(1+\alpha) = 2 + 2\cdot\alpha \\
\alpha^7 &= \alpha\cdot\alpha^6 = \alpha(2+2\alpha) = 2\alpha + 2\alpha^2 = 2\alpha + 2(1+\alpha) = 2\alpha + 2 + 2\alpha = 2 + 1\cdot\alpha \\
\alpha^8 &= \alpha\cdot\alpha^7 = \alpha(2+\alpha) \equiv 2\alpha + \alpha^2 = 2\alpha + (1+\alpha) = 1 + 3\alpha \equiv 1 = \alpha^0
\end{aligned}$$

So we obtained all the possible combinations for $a + b\alpha$ for $a, b \in \mathbb{F}_3$, except $a + b\alpha = 0 + 0\cdot\alpha = 0$ as expected.

Therefore we use the fact that all the elements of $\mathbb{F}_9$ can be written as $a + b\alpha$ for some $a, b \in \mathbb{F}_3$, as mentioned in the exercise.

$$\langle \alpha \rangle = \mathbb{F}_9 \setminus \{0\} = \mathbb{F}_9^\times$$

because we cannot obtain $a + b\alpha = 0 + 0\cdot\alpha = 0$

So α is a generator of $\mathbb{F}_9^\times$ $\square$

b) $\boxed{\begin{array}{l}\text{Find the DL of } \alpha - 2 \text{ to the base } \alpha - 1, \text{ if it exists.} \\ \text{I.e. find } n \in \mathbb{Z} \text{ s.t. } (\alpha-1)^n = \alpha - 2 \in \mathbb{F}_9\end{array}}$

We first recall again that all the elements of $\mathbb{F}_9$ can be written as $a+b\alpha$ for some $a, b \in \mathbb{F}_3$, as mentioned in the exercise.

Therefore, from part a) we have that

$$\alpha^7 = \alpha + 2 \overset{b=2\in\mathbb{F}_3}{\equiv_3} \alpha - 1 \quad , \quad \alpha^2 = \alpha + 1 \overset{b=1\in\mathbb{F}_3}{\equiv_3} \alpha - 2$$

Therefore we should find $n \in \mathbb{Z}$ s.t.

$$\alpha^{7n} = \alpha^2 \pmod 9$$

Equivalently, working on the exponents:

$$7n \equiv 2 \pmod 8$$

Since $7^{-1} \bmod 8 = 7$, we have

$$n \equiv 14 \pmod 8 \implies n \equiv 6 \pmod 8$$

Therefore, $n=6$ is the DL of $\alpha - 2$ in the base $\alpha - 1$.