Answers to Assignment 1.

1. If $\{\alpha_1, \ldots, \alpha_q\} = \mathbb{F}_q$, then $\left(\prod_{i=1}^{q} (x - \alpha_i)\right) + 1$ is a degree q polynomial that has no root in $\mathbb{F}_q$.

2. $\dim W = t$. If $k > n-t$, then any k-dimensional subspace of $\mathbb{F}_q^n$ must have nontrivial intersection with W.
$\therefore \nexists$ any such space for $k < n-t$.
If $k = 1$, then $\dfrac{q^n - q^t}{q-1} = \dfrac{q^t(q^{n-t}-1)}{q-1}$ is the required number.
$= |\mathbb{F}_q^n - W / \mathbb{F}_q^*|$

In general if W_1 is a k-diml subspace with $W_1 \cap W = \{0\}$,

Choose a basis B_1 of W_1. Let $B_1 = (v_1, \dots, v_k)$.

Then v_1 can be chosen in $q^n - q^t$ ways.

v_2 can be chosen in $q^n - q^{t+1}$ ways.

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad \overset{\shortparallel}{|\langle W, v_1 \rangle|}$

$\vdots$

v_k ——— " ——— $q^n - q^{t+k-1}$ ways.

& there are $(q^k - 1)(q^k - q) \cdots (q^k - q^{k-1})$ different bases of W_1.

$\therefore$ no. is
$$\frac{(q^n - q^t) \cdots (q^n - q^{t+(k-1)})}{(q^k - 1) \cdots (q^k - q^{k-1})}.$$

3. (a) Since $GL_n(\mathbb{F}_p)$ acts transitively on all bases of $\mathbb{F}_p^n$, $|GL_n(\mathbb{F}_p)| = (\#\text{ bases}) \cdot (|\text{stab}/\text{base}|)$

$$= (p^n - 1) \cdot \dots \cdot (p^n - p^{n-1}) \cdot 1$$

$1 \to$ (any lin. transf. fixing a base is Id)

(b) $$(p^n-1)\cdots(p^n-p^{n-1}) = p \cdot p^2 \cdot p^3 \cdots p^{n-1} \underbrace{(p^n-1)(p^{n-1}-1)\cdots(p-1)}_{N}$$

$$= p^{\frac{n(n-1)}{2}} \cdot N$$

$\to$ but $(N, p) = 1$.

$\therefore$ # p-Sylow subgroup is $p^{\frac{n(n-1)}{2}}$.

(c) $$\begin{bmatrix} 1 & * & \times & \times \\ 0 & \ddots & \times & \times \\ & & \ddots & \\ & & & 1 \end{bmatrix}$$ = upper triangular matrices with 1 on the diagonal is a subgp. of $GL_n(\mathbb{F}_p)$ is an example.

④ This is the most interesting question!

Note that x^4+x+1 is irreducible over $\mathbb{F}_2$.

(because it has no root & $(x^2+x+1)^2 \neq x^4+x+1$)

↳ only irred. poly of deg 2 in $\mathbb{F}_2[x]$

Ily, x^6+x+1 is irreducible over $\mathbb{F}_2$.

1. It has no root (only have to check 0 & 1)
2. $(x^3+ax^2+bx+c)(x^3+dx^2+ex+f)=x^6+x+1 \Rightarrow$ $c=f=1$.

   $a+d=0 \Rightarrow a=d$ — coeff of x^5

   either $e=0$ or $b=0$ — coeff of x

   These are enough to give contradiction
3. $(x^4+ax^3+bx^2+cx+1)(x^2+x+1) \neq x^6+x+1$ for any $a,b,c \in \{0,1\}$

Hence if α is a root of x^6+x+1 then $\deg[\mathbb{F}_2(\alpha) : \mathbb{F}_2] = 6$.

$\therefore \ \mathbb{F}_2(\alpha) = \mathbb{F}_{64}$. If γ is a root of x^4+x+1, then

$\mathbb{F}_2(\gamma) = \mathbb{F}_{16}$. $\quad \mathbb{F}_{64} \cap \mathbb{F}_{16} = \mathbb{F}_4$.

$\therefore$

$$\begin{tikzcd}
& \mathbb{F}_{4096} = \mathbb{F}_{64} \arrow[dl, dash, "2"'] \arrow[dd, dash, "6"] \arrow[dr, dash] & \\
\mathbb{F}_2(\alpha) = \mathbb{F}_{64} \arrow[dr, dash, "3"'] & & \mathbb{F}_{16} = \mathbb{F}_2(\gamma) \arrow[dl, dash, "2"] \\
& \mathbb{F}_4 \arrow[d, dash, "2"] & \\
& \mathbb{F}_2 &
\end{tikzcd}$$

Hence degree of irreducible poly of β over $\mathbb{F}_{64}$ is two, and its coefficients are from $\mathbb{F}_4 = \{0, 1, \beta, \beta+1\}$ where β is root of x^2+x+1.

(a) let $\beta = \alpha^5 + \alpha^4 + \alpha^3 + \alpha$.

then, $\beta^2 = \alpha^{10} + \alpha^8 + \alpha^6 + \alpha^2$ (raising to power 2 is a field iso. as characteristic is 2)

since $\alpha^6 = \alpha + 1$,

$\alpha^{10} = \alpha^5 + \alpha^4$, $\alpha^8 = \alpha^3 + \alpha^2$

$$\therefore \beta^2 = \alpha^5 + \alpha^4 + \alpha^3 + \cancel{\alpha^2 + \alpha^2}^{\,0} + \alpha + 1$$

$$\beta = \alpha^5 + \alpha^4 + \alpha^3 + \alpha$$

$$\Rightarrow \beta^2 + \beta + 1 = 2(\alpha^5 + \alpha^4 + \alpha^3 + \alpha + 1) = 0.$$

$\therefore$ β is a root of $x^2 + x + 1$.

write $(x^4 + x + 1) = (x^2 + ax + b)(x^2 + cx + d)$ $\in \mathbb{F}_4[x]$.

to get $a = c$ (coeff of x^3 is 0)

$bd = 1$ (const. coeff is 1)

$ad + bc = 1$ - coeff of x is 1

$b + d + ac = 0$ - coeff of x^2 is 0.

solve this to get : $x^4 + x + 1 = (x^2 + x + \beta)(x^2 + x + (\beta + 1))$!!!