Exercice 1 (*Extrait du sujet 2007*)

Soit $\mathbb{F}_{16}$ le corps fini à 16 éléments.

1. (a) Comment peut-on construire $\mathbb{F}_{16}$?
   (b) Démontrer que le groupe multiplicatif $\mathbb{F}_{16}^*$ est formé des puissances successives d'un élément ω vérifiant l'égalité $\omega^4+\omega^3+1=0$.
   (c) Démontrer que ω, ω^2, ω^4 et ω^8 sont les racines du polynôme X^4+X^3+1 dans $\mathbb{F}_{16}$.
   (d) Démontrer que la famille $(\omega,\omega^2,\omega^4,\omega^8)$ est une base de $\mathbb{F}_{16}$ sur $\mathbb{F}_2$.
2. (a) Soit $a\in\mathbb{F}_{16}$. Résoudre dans $\mathbb{F}_{16}$ l'équation $x^5=a$, en discutant éventuellement selon la valeur de a.
   (b) Démontrer qu'il existe quatre éléments $\gamma\in\mathbb{F}_{16}$ tels que, pour chacun d'eux, la famille $(\gamma,\gamma^2,\gamma^4,\gamma^8)$ est une base de $\mathbb{F}_{16}$ sur $\mathbb{F}_2$ telle que le produit de deux de ses éléments appartient à la base ou est égal à 1.

Exercice 2 (*Extrait du sujet 2011*)

Soit p un nombre premier. Soit $\mathbb{F}_p$ le corps fini $\mathbb{Z}/p\mathbb{Z}$. Soit $\overline{\mathbb{F}_p}$ une clôture algébrique du corps $\mathbb{F}_p$. Pour $P\in\mathbb{Z}[X]$, on note $\overline{P}$ l'élément de $\mathbb{F}_p[X]$ obtenu en réduisant P modulo p. Si $M\in\mathcal{M}_l(\mathbb{Z})$, on note $\overline{M}$ la matrice de $\mathcal{M}_l(\mathbb{F}_p)$ obtenue en réduisant M modulo p.

1. Montrer que si M,N sont deux matrices de $\mathcal{M}_l(\mathbb{Z})$ semblables sur $\mathbb{Z}$, alors $\overline{M}$ et $\overline{N}$ sont semblables sur $\mathbb{F}_p$.
2. Soit $P\in\mathbb{Z}[X]$ non constant dont les racines dans $\mathbb{C}$ sont simples.
   (a) Montrer qu'il existe $d\in\mathbb{N}^*$ et $S,T\in\mathbb{Z}[X]$ tels que : $SP+TP'=d$.
   (b) Si p ne divise pas d, montrer que les racines de $\overline{P}$ dans $\overline{\mathbb{F}_p}$ sont simples.
3. Soit $M\in\mathcal{M}_l(\mathbb{Z})$ diagonalisable sur $\mathbb{C}$.
   (a) Montrer qu'il existe un élément $P\in\mathbb{Z}[X]$ unitaire dont les racines complexes sont toutes simples et tel que $P(M)=0$.
   (b) Montrer qu'il existe un entier d_M tel que si p ne divise pas d_M alors $\overline{M}$ est diagonalisable sur $\overline{\mathbb{F}_p}$.

Exercice 3 (*Extrait du sujet 2002*)

Soit p un nombre premier impair. On appelle espace semi-quadratique un triplet (E,b,f) où E est un espace vectoriel de dimension finie sur $\mathbb{F}_p$, b une forme bilinéaire sur E non dégénérée et f une forme linéaire sur E telle que :

$$\forall x\in E,\forall y\in E,\quad b(x,y)+b(y,x)=2f(x)f(y). \tag{1}$$

Un espace semi-quadratique (E,b,f) possède un vecteur centre e et un poids λ définis par :

$$\forall x\in E,\quad b(x,e)=f(x)\quad\text{et}\quad f(e)=\frac{1-\lambda}{2}.$$

Soient $\mathcal{E}=(E,b,f)$ et $\mathcal{E}'=(E',b',f')$ deux espaces semi-quadratiques. On appelle isomorphisme de $\mathcal{E}$ sur $\mathcal{E}'$ une application linéaire bijective $\phi:E\longrightarrow E'$ telle que :

$$\forall x\in E,\quad f'(\phi(x))=f(x),$$
$$\forall x\in E,\forall y\in E,\quad b'(\phi(x),\phi(y))=b(x,y).$$

1. Soit $\mathcal{E}=(E,b,f)$ un espace semi-quadratique de dimension 1 et de poids -1. Soit e le vecteur centre de $\mathcal{E}$. Montrer que : $f(e)=b(e,e)=1$.
   En déduire qu'il existe un espace semi-quadratique de dimension 1 et de poids -1. Puis montrer que deux tels espaces sont isomorphes.
2. Soit E_n l'espace vectoriel $\mathbb{F}_p^n$ de dimension n, on note $\{e_1,\dots,e_n\}$ sa base canonique. La forme linéaire sur E_n qui envoie chaque e_i en 1 sera notée f.
   Montrer qu'il existe une unique forme bilinéaire b sur E_n telle que :
   – $\forall i\le n$, $b(e_i,e_i)=1$;
   – $\forall i<j\le n$, $b(e_i,e_j)=0$;
   – $\mathcal{E}_n=(E_n,b,f)$ est un espace semi-quadratique.
   Calculer $b(e_i,e_j)$ pour $i>j$.
3. Soient $m,n\in\mathbb{N}^*$. Montrer que $\mathcal{E}_{n+m}$ est isomorphe au produit orthogonal de $\mathcal{E}_n$ et de $\mathcal{E}_m$.