Corrigé du devoir maison 2

Exercice 1

1. Soit (e, f) une base quelconque de E. On a $\phi(e, e) = \phi(f, f) = 0$ et puisque ϕ est non dégénérée, $\phi(e, f) = \lambda \in k^\times$. Alors la base $(e, \lambda^{-1} f)$ convient.
2. Pour $n = 1$, le résultat est clair puisque $\phi(e, e) = 0$ pour tout vecteur e de E. Supposons le résultat vrai en dimension impaire $\leq n - 2$ et montrons-le en dimension impaire n. Par l'absurde, supposons ϕ non dégénérée. Soit $e \in E \backslash \{0\}$. Alors il existe $f \in E$ tel que $\phi(e, f) = 1$, et la famille (e, f) est libre. Soit $P = \mathrm{Vect}(e, f)$ et $F = P^\perp$. Montrons que $E = P \oplus F$. Comme ϕ est non dégénérée, on a $\dim F = n - 2$, et il suffit de montrer $P \cap F = \{0\}$. Soit $x = ae + bf \in P \cap P^\perp$. Alors $\phi(e, x) = b = 0$ et $\phi(f, x) = -a = 0$, d'où $x = 0$. Par hypothèse de récurrence, $\phi|_{F \times F}$ est dégénérée, i.e. il existe $x \in F \backslash \{0\}$ orthogonal à F. Alors x est orthogonal à F et P, donc à E, ce qui contredit l'hypothèse.
3. On montre le résultat par récurrence sur m. Le cas $m = 1$ a été traité à la question 1. Supposons le résultat vrai en dimension $2m - 2$, et montrons-le en dimension $2m$. Soit $e_1 \in E \backslash \{0\}$, et soit $f_1 \in E$ tel que $\phi(e_1, f_1) = 1$. Comme dans la question précédente, on montre que $P = \mathrm{Vect}(e_1, f_1)$ est un plan de E et que $E = P \oplus P^\perp$. Si B est une base quelconque de $P^\perp$, alors la matrice de ϕ dans la base (e_1, f_1, B) est de la forme
$$\begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & M \end{pmatrix}$$
C'est une matrice diagonale par blocs inversible, donc M est inversible, ce qui signifie que la restriction de ϕ à $P^\perp \times P^\perp$ est non dégénérée. Par hypothèse de récurrence, on trouve une base $(e_2, f_2, \ldots, e_m, f_m)$ de $P^\perp$ telle que $\phi(e_i, e_j) = \phi(f_i, f_j) = 0$ et $\phi(e_i, f_j) = \delta_{i,j}$ pour tout $2 \leq i, j \leq m$. Alors la base $(e_1, f_1, \ldots, e_m, f_m)$ de E a la propriété voulue.
Remarque. Une telle base $(e_1, f_1, \ldots, e_m, f_m)$ de E est appelée *base symplectique* de E pour ϕ.

Exercice 2

1. Supposons $\dim E = 1$. Si e est un vecteur non nul de E, alors une forme quadratique non dégénérée q sur E s'écrit $q(xe) = q(e)x^2$ avec $q(e) \in \mathbf{F}_p^\times$. Si $q(e)$ est un carré, disons $q(e) = t^2$, alors $q(t^{-1}e) = 1$ et la base $(t^{-1}e)$ convient. Sinon, on a $q(e) = \alpha t^2$, et la base $(t^{-1}e)$ convient.
2. Puisque $\mathrm{Card}\, \mathbf{F}_p^{\times 2} = (p-1)/2$, l'ensemble des carrés de $\mathbf{F}_p$ est de cardinal $(p+1)/2$. Considérons les ensembles
$$S = \{ax^2 : x \in \mathbf{F}_p\}$$
$$T = \{1 - by^2 : y \in \mathbf{F}_p\}$$
Chacun de ces ensembles est de cardinal $(p+1)/2$, et comme $(p+1)/2 + (p+1)/2 > p$, le principe des tiroirs nous assure que $S \cap T \neq \emptyset$, d'où l'existence de $(x, y) \in \mathbf{F}_p^2$ tel que $ax^2 + by^2 = 1$.

3. D'après le cours, il existe une base $B = (e_1, \dots, e_n)$ orthogonale pour q, avec $q(e_i) \in \mathbf{F}_p^\times$. En posant $v = xe_1 + ye_2$, on a $q(v) = q(e_1)x^2 + q(e_2)y^2$, et la question précédente nous assure qu'il existe $v \in \mathrm{Vect}(e_1, e_2)$ tel que $q(v) = 1$.
4. Soit $D = \mathrm{Vect}(v)$ et $F = D^\perp$. Puisque $q(v) = \phi(v, v) \neq 0$, on a $D \cap F = \{0\}$ et donc $E = D \oplus F$ (somme directe orthogonale). Par hypothèse de récurrence appliquée à $q|_F$, il existe une base $(v_1, \dots, v_{n-1})$ de F dans laquelle $q|_F$ est de la forme voulue. Alors la base $(v, v_1, \dots, v_{n-1})$ convient.
5. Si q_1 et q_2 sont isomorphes, alors les matrices M_1 et M_2 sont congruentes : il existe $P \in \mathrm{GL}_n(\mathbf{F}_p)$ telle que $M_2 =^t PM_1P$. En particulier $\det M_2 = \det M_1 \cdot (\det P)^2$ c'est-à-dire $\alpha = (\det P)^2$, ce qui est absurde.
6. Soit q une forme quadratique non dégénérée sur E. On calcule son discriminant $\delta = \mathrm{disc}_B(q) \in \mathbf{F}_p^\times$ dans une base quelconque B de E. Si δ est un carré de $\mathbf{F}_p^\times$, alors q est isomorphe à q_1 ; sinon q est isomorphe à q_2.