Corrigé

A.I

1) Si $s = -\alpha^2$ avec $\alpha \in (\mathbb{Z}/p\mathbb{Z})^\times$, on a $x^2 + sy^2 = (x - \alpha y)(x + \alpha y)$. Comme p est impair, la matrice $\begin{pmatrix} 1 & -\alpha \\ 1 & \alpha \end{pmatrix}$ est inversible. Donc pour tout $t \in (\mathbb{Z}/p\mathbb{Z})^\times$, l'ensemble $\mathcal{A}_p(S,t)$ est en bijection avec $\{(u,v) \in (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/p\mathbb{Z})^\times ; uv = t\}$ par $(x,y) \mapsto (x - \alpha y, x + \alpha y)$. Ce dernier ensemble est de cardinal $p-1$; on a donc $A_p(S,t) = p - 1$.

2.a. Un polynôme de degré deux à coefficients dans un corps commutatif est irréductible si et seulement si il n'a pas de racine dans ce corps. Ici, $X^2 + s$ est irréductible sur $\mathbb{Z}/p\mathbb{Z}$. Le choix d'une racine de $X^2 + s$ dans K fournit un homomorphisme surjectif et injectif d'anneaux $\mathbb{Z}/p\mathbb{Z}[X]/(X^2 + s) \to K$. Le terme de gauche est un espace vectoriel de dimension 2 sur $\mathbb{Z}/p\mathbb{Z}$ (de base $\{1, \overline{X}\}$ où $\overline{X}$ désigne la classe de X modulo $(X^2 + s)$). Le corps K est donc d'ordre p^2.

2.b. On a $F(0) = 0$, $F(1) = 1$ et $F : K^\times \to K^\times$ est un homomorphisme de groupes multiplicatifs. Pour voir que F est additif, il suffit de noter par la formule du binôme de Newton que les coefficients binomiaux $\begin{pmatrix} p \\ i \end{pmatrix}$ $(i = 1, \ldots, p-1)$ sont divisibles par p. C'est clair car $i! \cdot (p-i)! \begin{pmatrix} p \\ i \end{pmatrix} = p!$ est divisible par p. Comme les deux premiers facteurs sont premiers à p, c'est que p divise le troisième. Ainsi F est un homomorphisme de corps. Tout homomorphisme de corps est injectif. Comme K est fini, F est donc bijectif. On a $F \circ F(z) = z^{p^2}$. Comme $K^\times$ est un groupe d'ordre $p^2 - 1$, on a pour tout $z \in K^\times$, $z^{p^2-1} = 1$, donc $z^{p^2} = z$. Cette relation est aussi satisfaite par 0, donc on a $F \circ F = Id_K$.

Si $z^p = z$, z est racine du polynôme $X^p - X$ de degré p. Par le petit théorème de Fermat, ce polynôme a exactement p racines. Le noyau de $F - Id_K$ est donc $\mathbb{Z}/p\mathbb{Z}$.

2.c. Soit $\alpha \in K$ une racine de $X^2 + s$. $F(\alpha)$ est encore racine de $X^2 + s$ car $s \in \mathbb{Z}/p\mathbb{Z}$ est fixé par F. Comme $\alpha \notin \mathbb{Z}/p\mathbb{Z}$, on a $F(\alpha) \neq \alpha$. Comme l'autre racine est $-\alpha$, on a $F(\alpha) = -\alpha$.

3.a. On a $N(z) = zF(z)$. C'est donc un homomorphisme multiplicatif de $K^\times$ dans lui-même. De plus $(N(z))^p = z^{p^2+p} = z^{1+p} = N(z)$ car $F \circ F = Id_K$. Ainsi, $N(z) \in (Z/p\mathbb{Z})^\times$.

3.b. Si $N(z) = 1$, z est racine de $X^{p+1} - 1$; ainsi l'ordre de $\operatorname{Ker} N$ est au plus $p + 1$ et celui de $\operatorname{Im} N$ au plus $p - 1$. Comme celui de $K^\times$ est $(p-1)(p+1)$, on tire de l'isomorphisme $K^\times / \operatorname{Ker} N \cong \operatorname{Im} N$ que $\operatorname{Card} \operatorname{Ker} N = p + 1$ et $\operatorname{Card} \operatorname{Im} N = p - 1$.

3.c. On a $N(x + y\alpha) = (x + y\alpha)F(x + y\alpha) = (x + y\alpha)(x - y\alpha) = x^2 - y^2\alpha^2 = x^2 + sy^2$.

4) Notons qu'étant donnés deux éléments x, y de $\mathbb{Z}/p\mathbb{Z}$, on a $x + y\alpha \in K^\times$ si et seulement si x et y sont non-nuls. On peut donc écrire $\mathcal{A}_p(S,t) = \{z \in K^\times ; N(z) = t\}$. Choisissons $z_0 \in K^\times$ tel que $N(z_0) = t$. On a alors $N(z) = t$ si et seulement si $N(zz_0^{-1}) = 1$, c'est-à-dire $zz_0^{-1} \in \operatorname{Ker} N$. Ainsi $z \mapsto zz_0^{-1}$ est une bijection de $\mathcal{A}_p(S,t)$ vers $\operatorname{Ker} N$. L'ordre de $\mathcal{A}_p(S,t)$ est donc $p+1$ par 3.b.

A.II

1.a. On a $b(x,y) = \frac{1}{2}[b(x+y,x+y) - b(x,x) - b(y,y)]$. Si donc $b(t,t) = 0$ pour tout vecteur t, on a $b = 0$.

1.b. On raisonne par récurrence sur la dimension de V. Si $b = 0$ il n'y a rien à démontrer. Sinon, on prend $e_1 \in V$ tel que $b(e_1, e_1) \neq 0$. La relation $x = x - \frac{b(e_1,x)}{b(e_1,e_1)} \cdot e_1 + \frac{b(e_1,x)}{b(e_1,e_1)} \cdot e_1$ montre que V est somme directe de la droite engendrée par e_1 et de son orthogonal V_1. On applique alors l'hypothèse de récurrence à V_1 pour conclure.

1.c. On prend $V = M_{m,1}(\mathbb{Z}/p\mathbb{Z})$ et $b(X,Y) = {}^tXSY$. Soit P l'inverse de la matrice d'une base orthogonale de b. On a $S = {}^tPDP$ où D est diagonale.

2) La relation ${}^tXSX = T$ signifie pour tout i, j $b(v_i, v_j) = t_{i,j}$.

3) L'application

$$\mathcal{A}_p(S,T) \to \mathcal{A}_p({}^tPSP, {}^tQTQ), \quad X \mapsto P^{-1}XQ$$

est bijective.

4.a. On partitionne l'intervalle $[1,r]$ de $\mathbb{Z}$ en les sous-ensembles $\Phi(d)$ constitués des entiers dont le plus grand commun diviseur avec r est r/d, d parcourant l'ensemble des diviseurs positifs de d. La multiplication par r/d établit une bijection de $\Phi(d)$ avec l'ensemble des entiers premiers à d dans $[1,d]$. Son ordre est $\phi(d)$. On a donc $r = \sum_{d|r} \phi(d)$.

4.b. Un élément $x \in K^\times$ est d'ordre divisant d si et seulement si il est racine du polynôme de degré d $X^d - 1$. Il y a donc au plus d tels éléments dans $K^\times$.

4.c. Si $K^\times$ possède un élément x d'ordre d (diviseur $q-1$), il possède au moins d éléments d'ordre divisant d. Il en possède au plus d par la question précédente, donc exactement d, qui forment un groupe cyclique engendré par x. L'ensemble $(K^\times)_d$ des éléments d'ordre exactement d est donc d'ordre $\phi(d)$.

4.d. Si pour un diviseur d de $q-1$ il n'y a pas d'élément d'ordre d(*i.e.* $(K^\times)_d = \emptyset$), on a $q - 1 = \operatorname{Card} K^\times = \sum_{\delta|q-1} \operatorname{Card}(K^\times)_\delta < \sum_{\delta|q-1} \phi(\delta) = q-1$, ce qui est une contradiction.

A.III

1.a. L'homomorphisme $(\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times, x \mapsto x^2$ a pour noyau $\{\pm 1\}$. Son image est donc d'indice 2 dans $(\mathbb{Z}/p\mathbb{Z})^\times$. C'est dire qu'il y a autant de carrés que de non carrés dans $(\mathbb{Z}/p\mathbb{Z})^\times$.Soit a un non carré, tout non carré peut sécrire ax^2. Ainsi le produit de deux non carrés est un carré (et le produit d'un carré par un non carré est un non-carré, et le produit de deux carrés est un carré). Ceci montre que $x \mapsto (\frac{a}{p})$ est un homomorphisme.

1.b. Si $b \in (\mathbb{Z}/p\mathbb{Z})^\times$, $a \mapsto ab$ est bijective, donc $\sum_{a \in \mathbb{Z}/p\mathbb{Z}} \omega^{ab} = \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \omega^a = \frac{\omega^p - 1}{\omega - 1} = 0$. Si $b = 0$, on a $\sum_{a \in \mathbb{Z}/p\mathbb{Z}} \omega^{ab} = p$.

1.c. On a $G_c = 1 + 2 \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^{\times 2}} \omega^{ca}$. D'autre part, $H_c = \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^{\times 2}} \omega^{ca} - \sum_{a \notin (\mathbb{Z}/p\mathbb{Z})^{\times 2}} \omega^{ca}$. Comme $c \in (\mathbb{Z}/p\mathbb{Z})^{\times}$, on a $\sum_{a \in \mathbb{Z}/p\mathbb{Z}} \omega^{ac} = 0 = 1 + \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^{\times 2}} \omega^{ac} + \sum_{a \notin (\mathbb{Z}/p\mathbb{Z})^{\times 2}} \omega^{ac}$, donc $1 + \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^{\times 2}} \omega^{ac} = - \sum_{a \notin (\mathbb{Z}/p\mathbb{Z})^{\times 2}} \omega^{ac}$. Ainsi, $H_c = \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^{\times 2}} \omega^{ac} + 1 + \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^{\times 2}} \omega^{ac} = G_c$.

2.a. Par 1.b, la somme $\frac{1}{p}. \sum_{a \in (\mathbb{Z}/p\mathbb{Z})} \omega^{ab}$ vaut 1 ou 0 suivant que b est nul ou pas. Donc $pA_p(S,t) = \sum_{X \in M_{m,1}(\mathbb{Z}/p\mathbb{Z})} \frac{1}{p} \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \omega^{a({}^tXSX - t)}$. D'où la formule annoncée.

2.b. On a ${}^tXDX = \sum_{i=1}^{m} s_i x_i^2$ donc $\omega^{a({}^tXDX - t)} = \omega^{as_1 x_1^2} \dots \omega^{as_m x_m^2} \omega^{-at}$ et

$pA_p(S,t) = \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \omega^{-at} (\sum_{x_1 \in \mathbb{Z}/p\mathbb{Z}} \omega^{as_1 x_1^2}) \cdot \dots \cdot (\sum_{x_m \in \mathbb{Z}/p\mathbb{Z}} \omega^{as_m x_m^2})$

La contribution du terme $a = 0$ vaut p^m. De plus, on a pour chaque $i = 1, \dots, m$. $\sum_{x_i \in \mathbb{Z}/p\mathbb{Z}} \omega^{as_i x_i^2} = G_{as_i} = (\frac{as_i}{p})G$. Donc $pA_p(S,t) = p^m + \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^{\times}} \omega^{-at} (\frac{as_1}{p}) \dots (\frac{as_m}{p}) G)$ et comme $(\frac{s_1}{p}) \cdot \dots \cdot (\frac{s_m}{p}) = (\frac{D}{p})$, on a : $pA_p(S,t) = p^m + G^m (\frac{D}{p}) \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^{\times}} \omega^{-at} (\frac{a}{p})^m$.

2.c. Prenons $m = 1$, $s_1 = 1$ et $t = 1$. On a $A_p(S,1) = 2$ donc comme $G_{-1} = (\frac{-1}{p})G$, on a $2p = p + G(\frac{-1}{p})G$, soit $p = G^2(\frac{-1}{p})$, ou encore $G^2 = (\frac{-1}{p})p$.

3.a. Pour S symétrique non-dégénérée quelconque, ,on applique A.II 1.c et 3 pour se ramener à S diagonale, de déterminant $s_1 \dots s_m = s$. On obtient donc $pA(S,t) = p^m + (\frac{s}{p}) G^m \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^{\times}} \omega^{-at} (\frac{a}{p})^m$.

Si $m = 2r$, on a $G^m \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^{\times}} \omega^{-at} (\frac{a}{p})^m = -(\frac{-1}{p})^r p^r$, donc $pA(S,t) = p^m (1 - (\frac{(-1)^{m/2} s}{p}) p^{-m/2})$ d'où la formule annoncée.

Si $m = 2r + 1$, on a $G^m \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^{\times}} \omega^{-at} (\frac{a}{p})^m = (\frac{-t}{p}) G^{m+1} = (\frac{-t}{p})(\frac{-1}{p})^{r+1} p^{r+1}$ donc $pA(S,t) = p^m (1 + (\frac{(-1)^{(m-1)/2} st}{p}) p^{(1-m)/2})$. D'où la formule annoncée.

3.b. Le seul cas de nullité intervient lorsque $m = 1$ et lorsque st n'est pas un carré.

A.IV

1.a. On écrit $X = (C_1, X_1)$ où C_1 est un vecteur colonne et $X_1 \in M_{m,n-1}(\mathbb{Z}/p\mathbb{Z})$. Alors un calcul par blocs montre que ${}^tXSX = T$ équivaut à ${}^tC_1 S C_1 = \delta$, ${}^tX_1 S X_1 = T_1$ et ${}^tC_1 S X_1 = 0$. L'application $X \mapsto C_1$ induit donc en particulier une application $\gamma : \mathcal{A}(S,T) \to \mathcal{A}(S,\delta)$.

1.b. Soit W l'orthogonal de C_1 dans l'espace quadratique $V = M_{m,1}(\mathbb{Z}/p\mathbb{Z})$ muni de $b(v,w) = {}^tvSw$. Soit $(v_i)_{i=2,\dots,m}$ une base de W. Soit $S_1 = (b(v_i,v_j))_{2\leqslant i,j\leqslant m}$ la matrice de b dans cette base. Soit $T_1 = (t_{i,j})_{2\leqslant i,j\leqslant n}$. Par la question précédente, on peut réécrire l'ensemble $\gamma^{-1}(C_1)$ comme

$$\{(w_2,\dots,w_n) \in W^{n-1}; b(w_i,w_j) = t_{i,j} \quad \text{pour tout } i,j \in [2,m]\}$$

Soit $X_1' \in M_{m-1,n-1}(\mathbb{Z}/p\mathbb{Z})$ la matrice des coordonnées des vecteurs colonnes w_j dans la base des v_i. On peut réécrire l'ensemble $\gamma^{-1}(C_1)$ comme

$$\mathcal{A}(S_1,T_1) = \{X_1' \in M_{m-1,n-1}(\mathbb{Z}/p\mathbb{Z}); {}^tX_1'S_1X_1' = T_1\}$$

Soit P la matrice de la base $(v_1,\dots,v_m)$. On a

$$\begin{pmatrix} \delta & 0 \\ 0 & S_1 \end{pmatrix} = {}^tPSP$$

Donc si $s_1 = \det S_1$, on a $\delta s_1 = s(\det P)^2$ et $(\frac{\delta s_1}{p}) = (\frac{s}{p})$.

2.a. Pour $n = 1$, vue la convention sur les cas de nullité de $\varepsilon_k^{(p)}(a)$, les formules pour $A_p(S,t)$ distinguant m pair ou impair peuvent être synthétisées en la seule formule $A_p(S,t) = p^{m-1}\psi_{p,m,1}(s,t)$. Si le résultat est vrai pour $n-1$, soit $T \in S_n(\mathbb{Z}/p\mathbb{Z})$; quitte à remplacer T par ${}^tQTQ$), ce qui ne change pas $A_p(S,T)$ par A.II.3, on peut supposer T diagonale (et en particulier de la forme de la question 1.2 ci-dessus. Avec les notations de la question 1.b, on a $A_p(S,T) = A_p(S,\delta)A_p(S_1,T_1)$. Par hypothèse de récurrence, $A_p(S_1,T_1) = p^{(m-1)(n-1)-(n-1)n/2}\psi_{p,m-1,n-1}(s_1,t_1)\prod_{m-n+1<2k<m}(1-\frac{1}{p^{2k}})$. et $A_p(S,\delta) = p^{m-1}\psi_{p,m,1}(s,\delta)$. Traitons par exemple le cas où m et n sont pairs. On observe que

- $(m-1)(n-1) - n(n-1)/2 + (m-1) = mn - n(n+1)/2$
- $\psi_{p,m,1}(s,\delta) = 1 - (\frac{(-1)^{m/2}s}{p})p^{-m/2}$ et
- $\psi_{p,m-1,n-1}(s_1,t_1) = 1 + (\frac{(-1)^{(m-n)/2}s_1t_1}{p})p^{(n-m)/2}$, et comme par la question 1.2 on a $s_1t_1\delta^2 = stu^2$, on trouve $\psi_{p,m,1}(s,\delta)\psi_{p,m-1,n-1}(s_1,t_1) = \psi_{p,m,n}(s,t)$. Comme on a aussi
- $\prod_{m-n<2k<m}(1-\frac{1}{p^{2k}}) = \prod_{m-n+1<2k<m}(1-\frac{1}{p^{2k}})$

on voit donc en multipliant $A_p(S,\delta)$ et $A_p(S_1,T_1)$ que

$$A_p(S,T) = p^{mn-n(n+1)/2}\psi_{p,m,n}(s,t)\prod_{m-n<2k<m}(1-\frac{1}{p^{2k}})$$

comme annoncé. Les autres cas se traitent de même.

2.b. Le seul cas de nullité de $A_p(S,T)$ se produit lorsque $m = n$ et que st n'est pas un carré.

B.

1.a. et **1.b.** se traitent simultanément en observant que, lorsque q_1 et q_2 sont premiers entre eux, le lemme chinois induit un isomorphisme d'anneaux $M_{m,n}(\mathbb{Z}/q_1q_2\mathbb{Z}) \cong M_{m,n}(\mathbb{Z}/q_1\mathbb{Z}) \times M_{m,n}(\mathbb{Z}/q_2\mathbb{Z})$.

1.c. est immédiat à partir des questions ci-dessus.

2.a. Soit $\widetilde{T} = \pi_p(T)$. Soit $H_1 \in M_n(\mathbb{Z}/p\mathbb{Z})$. Soit $H_2 \in M_n(\mathbb{Z}/p\mathbb{Z})$ telle que $H_1 = \widetilde{T}H_2$; posons $H = \widetilde{X}H_2 \in M_{m,n}(\mathbb{Z}/p\mathbb{Z})$. On a ${}^t\widetilde{X}\widetilde{S}H = {}^tX\widetilde{S}\widetilde{X}H_2 = \widetilde{T}H_2 = H_1$.

2.b. Comme p est impair, toute matrice symétrique $H_1 \in S_n(\mathbb{Z}/p\mathbb{Z})$ s'écrit $H_2 + {}^tH_2$ pour une matrice $H_2 \in M_n(\mathbb{Z}/p\mathbb{Z})$; par la question précédente, il existe $H \in M_{m,n}(\mathbb{Z}/p\mathbb{Z})$ tel que ${}^t\widetilde{X}\widetilde{S}H = H_2$. Ceci montre la surjectivité de $H \mapsto {}^t\widetilde{X}\widetilde{S}H + {}^tH\widetilde{S}\widetilde{X}$.

2.c. Le noyau de l'application ci-dessus est de dimension $mn - n(n+1)/2$. Donc son cardinal est $p^{mn-n(n+1)/2}$.

3) On abrège $\pi_{p^\alpha}(X) = X_\alpha$. Si ${}^tX_\alpha S_\alpha X_\alpha = T_\alpha$, posons $Y = X + p^\alpha U$. Cherchons $U \in M_{m,n}(\mathbb{Z})$ de sorte que ${}^tYSY \equiv T \pmod{p^{\alpha+1}}$. On peut réécrire cette relation comme ${}^t(X + p^\alpha U)S(X + p^\alpha U) \equiv T \pmod{p^{\alpha+1}}$, ou encore, en posant ${}^tXSX = T + p^\alpha\Theta$: ${}^tUSX + {}^tXSU \equiv \Theta \pmod{p}$. Par la question 2.2, cette congruence a une solution $U \in M_{m,n}(\mathbb{Z})$.

4) Étant donnée $X \in M_{m,n}(\mathbb{Z})$ telle que ${}^tXSX \equiv T \pmod{p^\alpha}$, l'ensemble $\{\pi_p(U) \in M_{m,n}(\mathbb{Z}/p\mathbb{Z}); {}^tUSX + {}^tXSU \equiv \Theta \pmod{p}\}$ est une variété linéaire affine de direction de dimension $mn - n(n+1)/2$. C'est donc un ensemble d'ordre $p^{mn-n(n+1)/2}$. Ainsi, r_α est surjective et l'image inverse de chaque singleton est d'ordre $p^{mn-n(n+1)/2}$.

5) On en déduit que

$$A_{p^\alpha} = p^{(\alpha-1)(mn-n(n+1)/2)}p^{mn-n(n+1)/2}\psi_{p,m,n}(s,t)\prod_{m-n<2k<m}(1-\frac{1}{p^{2k}}) =$$

$$p^{\alpha(mn-n(n+1)/2}\psi_{p,m,n}(s,t)\prod_{m-n<2k<m}(1-\frac{1}{p^{2k}}).$$

6.a. On a

$$A_q(S,T) = A_{p_1^{\alpha_1}}(S,T)\dots A_{p_r^{\alpha_r}}(S,T) = q^{\alpha(mn-n(n+1)/2)}\prod_i \psi_{p_i,m,n}(s,t)\prod_{m-n<2k<m}(1-\frac{1}{p_i^{2k}})$$

6.b. La nullité de $A_q(S,T)$ ne se produit que lorsque $m = n$ et que st n'est pas un carré modulo l'un des facteurs premiers de q.

7.a. On a $A_{q_h}(S,T)/q_h^{mn-n(n+1)/2} = \prod_i \psi_{p_i,m,n}(s,t)\prod_{m-n<2k<m}(1-\frac{1}{p_i^{2k}})$ On a $m > n+2$ donc en particulier $m/2 > 3/2$ et $(m-n)/2 > 1$; donc les produits infinis $\prod_i(1-(\frac{(-1)^{m/2}s}{p_i})p_i^{-m/2})$ et $\prod_i(1-(\frac{(-1)^{(m-n)/2}st}{p_i})p_i^{-(m-n)/2})$ sont absolument convergents.

A fortiori les produits $\prod_i(1-\frac{1}{p_i^{2k}})$ pour $2k \in]m-n, m[$. Leur limite sont des nombres strictement positifs. Il en va donc de même pour leur produit fini.

7.b. L'argument est identique car $A_{Q_h}(S,T)/Q_h^{mn-n(n+1)/2} = A_{q_h}(S,T)/q_h^{mn-n(n+1)/2}$

Rapport des correcteurs

Le problème portait sur l'étude, pour deux matrices symétriques S et T à coefficients dans $\mathbb{Z}$ données de tailles respectives m et n, des nombres $A_q(S,T)$ de solutions $X \in M_{m,n}(\mathbb{Z}/q\mathbb{Z})$ de la congruence ${}^tXSX \equiv T \pmod q$. On faisait l'hypothèse simplificatrice que les matrices sont définies positives et que q est premier à $2\det S \cdot \det T$.

La partie A concernait le cas où q est premier ; la partie B consistait à déduire le cas général du cas A. La partie $A.I$ proposait de calculer le nombre $A_p(S,T)$ pour $m = 2$ et $n = 1$ en distinguant selon que $-\det S$ est un carré ou non modulo p.

La première question de cette partie a semble-t'il posé problème à de nombreux candidats. Elle reposait sur l'identité remarquable $a^2-b^2 = (a-b)(a+b)$. Elle a occasionné les dénombrements les plus variés, conduisant parfois à des résultats absurdes. Pour les écrire, il a fallu que le candidat renonce au bon sens dont il aurait fait preuve en physique : une erreur de calcul peut conduire à trouver un cardinal égal à $\frac{p}{2}$ (pour p premier impair), ou à l'infini, pour un ensemble fini. Mais alors, le "bon sens physique", valable aussi en algèbre, aurait pu suggérer une relecture du calcul...

La confusion entre (auto)morphisme de corps, de groupes et d'espaces vectoriels a conduit certains candidats à ne pas vérifier la multiplicativité de F ainsi que la condition $F(1) = 1$, et inversement, elle en a conduit d'autres à vérifier l'additivité de N et à chercher son noyau comme l'ensemble des z tels que $N(z) = 0$.

Il faut essayer de dégager les structures algébriques concernées par les questions avant de se lancer dans les vérifications.

Atention dans $2.c$, on ne peut écrire sans précaution $\alpha = i\sqrt{-s}$ (vu que $i \in \mathbb{C}$ et $s \in \mathbb{F}_p$).

Dans $A.I$ et dans $B.1$, on a beaucoup vu d'énoncés de questions recopiés. C'est une remarque générale : recopier ou plagier l'énoncé ne rapporte rien !

La première question de $A.II$ a également surpris les correcteurs.On a vu des formes quadratiques définies et positives sur $\mathbb{F}_p$. La méthode de Gram-Schmidt ne s'applique que dans le contexte d'une forme quadratique réelle définie positive. C'est cependant souvent la méthode choisie pour montrer l'existence d'une base orthogonale dans le cadre du corps $\mathbb{F}_p$! Une erreur du même ordre a souvent été le recours à une "diagonalisation" de la forme quadratique avec matrice de passage orthogonale. Cette confusion classique dans le cadre réel de la réduction d'une forme quadratique avec la diagonalisation d'une matrice symétrique devient vraiment absurde sur $\mathbb{F}_p$ car une matrice symétrique n'est même plus nécessairement diagonalisable (comme le montre l'exemple de $\begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix}$ sur $\mathbb{F}_5$).

En fait, on traite la question $1.b$ de $A.I$ par récurrence sur la dimension. Il faut cependant rédiger les récurrences et non se contenter de les amorcer en finissant par un "et ainsi de suite".

Une erreur courante, moins grave certes, est de penser que dans l'écriture $S = {}^tPDP$, la matrice P est la matrice de passage de la base canonique de K^n à la base orthogonale construite, alors que c'est l'inverse.

La cyclicité de $K^\times$ a souvent été mal traitée ; les questions $4.a$-$4.d$ occasionnent des réponses floues voire fausses alors que les candidats peuvent penser les avoir traitées correctement.

Certains ont tenté d'adapter une démonstration différente de celle demandée, en général sans succès. Encore une remarque générale : pour obtenir les points d'une question, il s'agit de répondre exactement à la question telle qu'elle est posée, y compris s'il s'agit d'une question de cours.

Le simple bon sens montre qu'on ne répond pas à $A.II.1.b$ en citant le théorème du cours affirmant qu'il existe une base orthogonale, de même qu'on ne répond pas à $4.a$-$4.d$ en citant celui qui affirme que $K^\times$ est cyclique !

$A.III$ Le symbole de Legendre et les sommes de Gauss semblaient connus des candidats, mais trop souvent les calculs proposés se sont bornés à une suite d'égalités non justifiées (et parfois erronées, conduisant malgré tout au résultat). Les formules écrites laissent souvent entendre que l'ensemble dans lequel vivent les sommes de Gauss n'est pas clair : on lit souvent que si p divise b, $\sum_a \omega^{ab} = p = 0$ et que $e^{2i\pi/p} \in \mathbb{F}_p$ (!) La réalité est que les sommes de Gauss sont des nombres complexes !

La partie $A.III.3$ n'a été abordée que par très peu de candidats.

Dans $A.IV$, seule la première question a été souvent abordée.

Pour la partie $B1$, de nombreuses copies proposaient une démonstration très pénible de l'injectivité. Certains candidats ont montré qu'ils n'avaient pas compris le théorème chinois, qu'ils pouvaient néanmoins citer, puisqu'ils affirmaient que la surjectivité sur le produit résultait de la surjectivité sur chacun des facteurs. En général, seules les questions évidentes du $B.II$ ont été abordées. Les autres questions n'ont concerné que quelques candidats.
