Formes quadratiques : correction

Exercice 1.
Deux formes isométriques ont même discriminant. Or, 1 et 2 définissent la même classe dans $\mathbf{C}^\times/(\mathbf{C}^\times)^2$ (il n'y a rien à dire), $\mathbf{R}^\times/(\mathbf{R}^\times)^2$ (ils ont même signe) mais pas dans $\mathbf{Q}^\times/(\mathbf{Q}^\times)^2$: 2 n'est pas un carré. Les deux formes ne sont donc pas isométriques sur $\mathbf{Q}$.
En revanche, les deux formes ont même rang, donc elles sont isométriques sur $\mathbf{C}$ et même signature donc elles sont isométriques sur $\mathbf{R}$.

Exercice 2.

1. Écrivons
$$xy + yz = y(x+z) = \frac{1}{4}\left[((x+z)+y)^2 - ((x+z)-y)^2\right].$$
On peut alors déduire la forme polaire associée à la forme quadratique, qui est :
$$\varphi((x,y,z),(x',y',z')) = \frac{1}{4}\left[(x+z+y)\left(x'+z'+y'\right) - (x+z-y)\left(x'+z'-y'\right)\right].$$
Ainsi, il est facile d'en déduire la matrice dans la base canonique : c'est $\begin{pmatrix} 0 & \frac{1}{2} & 0 \\ \frac{1}{2} & 0 & \frac{1}{2} \\ 0 & \frac{1}{2} & 0 \end{pmatrix}$.
On peut déjà en déduire que son rang est 2. On peut également voir que son noyau est de dimension 1, engendré par $e_3 = (1,0,-1)$. Pour diagonaliser sa matrice, on peut compléter e_3 en une base orthogonale, en prenant $e_1 = (1,1,0)$ et $e_2 = (1,-1,0)$.
2. Remarquons qu'on peut écrire $q(x_1,\dots,x_n) = \sum_{1\leq i,j\leq n} x_i x_j - \sum_{i=1}^n x_i^2$. La matrice de q dans la base canonique est donc $\mathrm{A} - \mathrm{Id}$ où A est la matrice comportant uniquement des 1. Alors, A est symétrique, donc diagonalisable en base orthogonale. Elle est de rang 1, et de trace n, donc ses valeurs propres sont 0 (avec multiplicité $n-1$) et n (avec multiplicité 1). Dans cette même base orthogonale, la matrice de q est donc diagonale avec comme valeurs propres -1 (avec multiplicité $n-1$), et $n-1$ (simple). La signature de q est donc $(1, n-1)$.

Exercice 3.

1. Soit b la forme bilinéaire associée à q. Puisque (V, q) est non dégénéré, l'application
$$\begin{array}{ccc} \mathrm{V} & \to & \mathrm{V}^* \\ x & \mapsto & (y \mapsto b(x,y)) \end{array}$$
est un isomorphisme. Via cet isomorphisme, $\mathrm{U}^\perp$ est donc défini comme le lieu d'annulation commun des formes linéaires contenues dans un sous-espace vectoriel du dual V^* de dimension $\dim \mathrm{U}$. D'après les propriétés de la dualité, on a $\dim \mathrm{U}^\perp = \dim \mathrm{V} - \dim \mathrm{U}$.
Maintenant, dire que U est dégénéré signifie que quand on restreint la forme quadratique à U, son orthogonal n'est pas nul, c'est-à-dire précisément que $\mathrm{U} \cap \mathrm{U}^\perp \neq \{0\}$. On a donc bien U non dégénéré si et seulement si U et $\mathrm{U}^\perp$ sont en somme directe, ce qui, vu le décompte des dimensions effectué plus haut, conclut.
Remarque : ce résultat, sous la forme « $q_{|\mathrm{U}}$ non dégénérée $\Rightarrow \mathrm{V} = \mathrm{U} \oplus \mathrm{U}^\perp$ » est d'un emploi constant.

2. (i) Via le changement de variables $\xi = (x+y)/2$, $\eta = (x-y)/2$, on a $\xi^2 - \eta^2 = xy$. Le plan quadratique $(k^2, (x,y) \mapsto xy)$ est donc hyperbolique.

   (ii) Soit (V, q) un plan quadratique non dégénéré et de discriminant -1. D'après le cours, on peut trouver une base (e_1, e_2) de V dans laquelle la matrice de q est $\mathrm{diag}(\lambda, \mu)$; l'hypothèse sur le discriminant implique que $-\lambda\mu$ est un carré (et λ et μ sont non nuls par non-dégénéréscence). Cela implique également que $-\lambda/\mu$ est un carré, et on peut donc écrire $\mu = -t^2\lambda$. Le vecteur $e1 + e2/t$ est donc isotrope et on se ramène au cas suivant.

   (iii) Soit (V, q) un espace non dégénéré et isotrope. Soit x un vecteur isotrope. Si b est la forme bilinéaire associée à q, on peut trouver par non-dégénérescence y tel que $b(x,y) = 1$. On a alors une base (x,y) (y ne peut pas être colinéaire à x car l'isotropie de x entraînerait alors $b(x,y) = 0$) avec les relations

   $$b(x,x) = 0 \qquad b(x,y) = 1 \qquad b(y,y) = \lambda \in k.$$

   Si on remplace y par $\widetilde{y} = y + \mu x$, seule cette dernière valeur change, de la façon suivante :

   $$b(y+\mu x, y+\mu x) = b(y,y) + 2\mu b(x,y) + \mu(x,x) = \lambda + 2\mu.$$

   On peut donc choisir μ pour avoir

   $$b(x,x) = 0 \qquad b(x,\widetilde{y}) = 1 \qquad b(\widetilde{y},\widetilde{y}) = 0,$$

   ce qui montre que q est isométrique à $(\xi,\eta) \mapsto \xi\eta$, et donc hyperbolique.

3. On démontre le théorème par récurrence sur $\dim \mathrm{U}$.
   - Si $\dim \mathrm{U} = 1$, soit x un générateur de U ; il est isotrope. La non-dégénérescence implique qu'on peut trouver y tel que $b(x,y) = 1$. Le plan engendré par x et y est alors non dégénéré (sa matrice dans une base est de la forme $\begin{pmatrix} 0 & 1 \\ 1 & * \end{pmatrix}$) et isotrope, donc c'est un plan hyperbolique et le théorème est montré.
   - Supposons le théorème démontré dans le cas $\dim \mathrm{U} = r-1$ et soit $\mathrm{U} \subset \mathrm{V}$ un espace vectoriel totalement isotrope de dimension r. Soit $(x_1, \dots, x_r)$ une base de U et U' l'espace vectoriel engendré par $(x_2, \dots, x_r)$. Par non-dégénérescence de V et d'après la formule des dimensions, l'orthogonal de U' contient *strictement* l'orthogonal de U. On peut donc trouver y_1 orthogonal à $x_2, \dots, x_r$ mais pas à x_1. Comme précédemment, le plan H engendré par x_1 et y_1 est hyperbolique, donc non dégénéré et $\mathrm{V} = \mathrm{H} \oplus \mathrm{H}^\perp$. L'orthogonal $\mathrm{H}^\perp$ contient U' et est non dégénéré (sinon, V le serait) donc on peut appliquer l'hypothèse de récurrence à $\mathrm{U}' \subset \mathrm{H}^\perp$ pour conclure.

4. D'après le théorème précédent, une forme isotrope contient un plan hyperbolique comme facteur direct : autrement dit, elle est isométrique à une forme du type

   $$(x_1, \dots, x_n) \mapsto x_1x_2 + q(x_3, \dots, x_n).$$

   Cette forme réprésente évidemment tous les $\lambda \in k^\times$ (il suffit de prendre $x_1 = \lambda$, $x_2 = 1$ et $x_3 = \cdots = x_n = 0$). Comme deux formes isométriques représentent clairement les mêmes scalaires, le résultat est démontré.

5. Un sens est direct : s'il existe x tel que $q(x) = \lambda$, le vecteur $(x,1)$ est isotrope pour la forme $(x,t) \mapsto q(x) - \lambda t^2$, c'est-à-dire pour $\mathrm{V} \oplus \langle -\lambda \rangle$. Réciproquement, supposons qu'il existe $(x,t) \in \mathrm{V} \times k$ non nul tel que $q(x) - \lambda t^2 = 0$. Si t est non nul, on a alors $q(x/t) = \lambda$; si $t = 0$, la forme q est alors isotrope et, d'après la question précédente, universelle : elle représente donc tous les scalaires, en particulier λ.

6. On commence par appeler V_{ti} le noyau de q. Il est clairement totalement isotrope. Soit V_0 un supplémentaire quelconque de V_{ti}. L'espace quadratique V_0 est non dégénéré (si un élément de V_0 était orthogonal à tout V_0, il serait orthogonal à tout V, donc dans V_{ti}, contradiction).

   Soit maintenant $\mathrm{V}_{\mathrm{hyp}} \subset \mathrm{V}_0$ un espace hyperbolique de dimension maximale. Puisque les espaces hyperboliques sont non dégénérés, son orthogonal dans V_0, V_{an}, vérifie $\mathrm{V}_{\mathrm{hyp}} \oplus \mathrm{V}_{\mathrm{an}} = \mathrm{V}_0$. Il reste simplement à démontrer que V_{an} est anisotrope. S'il admettait un vecteur x isotrope, le théorème de gonflement de Witt fournirait un plan hyperbolique $\mathrm{H} \subset \mathrm{V}_{\mathrm{an}}$, et l'existence de l'espace hyperbolique $\mathrm{V}_{\mathrm{hyp}} \oplus \mathrm{H} \subset \mathrm{V}_0$ contredirait la maximalité de $\mathrm{V}_{\mathrm{hyp}}$. On a donc bien démontré l'existence de la décomposition de Witt

$$(\mathrm{V}, q) = (\mathrm{V}_{\mathrm{ti}}, q_{\mathrm{ti}}) \oplus (\mathrm{V}_{\mathrm{hyp}}, q_{\mathrm{hyp}}) \oplus (\mathrm{V}_{\mathrm{an}}, q_{\mathrm{an}}).$$

7. La forme q restreinte à $\mathrm{Vect}(y)$ est non dégénérée (elle est isométrique à $\langle q(y) \rangle$) donc $\mathrm{V} = \mathrm{Vect}(y) \oplus \mathrm{Vect}(y)^\perp$. L'endomorphisme τ_y vaut clairement l'identité sur l'hyperplan $\mathrm{Vect}(y)^\perp$ alors que l'égalité

$$\tau_y(y) = y - \frac{2b(y,y)}{q(y)} y = -y$$

   montre qu'il vaut $-\mathrm{id}$ sur la droite $\mathrm{Vect}(y)$. La décomposition étant orthogonale, cela démontre simultanément que τ_y est une isométrie de (V, q) et une application linéaire de déterminant -1. C'est d'ailleurs également une involution. C'est la *réflexion par rapport à* $\mathrm{Vect}(y)^\perp$.

8. Un dessin euclidien dans le plan montre que la réflexion par rapport à $\mathrm{Vect}(x-y)^\perp$ pourrait être la solution. Le problème est que dans le cas général, le vecteur $x - y$ pourrait être isotrope. On peut tout de même faire marcher cette approche.

   On montre premièrement que parmi les deux vecteurs $x + y$ et $x - y$, au moins l'un des deux n'est pas isotrope : dans le cas contraire, on aurait d'après la *loi du parallélogramme*

$$q(x)+q(y) = b(x,x)+b(y,y) = b(x+y,x+y)+b(x-y,x-y) = q(x+y)+q(x-y) = 0,$$

   ce qui est exclu. Si $x - y$ n'est pas isotrope, on a

$$q(x-y) = b(x-y,x-y) = b(x,x)-2b(x,y)+b(y,y) = 2(b(x,x)-b(x,y)) = 2b(x,x-y)$$

   donc

$$\tau_{x-y}(x) = x - \frac{2b(x,x-y)}{q(x-y)}(x-y) = y.$$

   Et si $x + y$ n'est pas isotrope, en remplaçant y par $-y$, on a construit une isométrie envoyant x sur $-y$. Il suffit alors de composer par $-\mathrm{id}$ pour obtenir l'isométrie souhaitée.

9. Soit (V, q), (V_1, q_1) et (V_2, q_2) trois espaces quadratiques tels que

$$(\mathrm{V}, q) \oplus (\mathrm{V}_1, q_1) \simeq (\mathrm{V}, q) \oplus (\mathrm{V}_2, q_2).$$

   Puisque l'on peut diagonaliser la forme q, c'est-à-dire écrire (V, q) comme somme directe de droites quadratiques, il suffit, par récurrence, de prouver le résultat dans le cas où $\dim \mathrm{V} = 1$. La forme (V, q) est alors $\langle \lambda \rangle$ pour un certain $\lambda \in k$.
   - Supposons $\lambda = 0$. On peut écrire $\mathrm{V}_i = \mathrm{N}_i \oplus \mathrm{W}_i$ où N_i est le noyau de V_i et W_i en est un supplémentaire. N_i est d'ailleurs simplement un espace vectoriel avec la forme quadratique nulle, et une considération de rang prouve que $\dim \mathrm{N}_0 = \dim \mathrm{N}_1$.

Il suffit donc de démontrer le théorème de simplification de Witt dans le cas où V est totalement isotrope et les V_i non dégénérés pour démontrer que W_1 et W_2 sont isométriques, ce qui impliquera que V_1 et V_2 le sont.
Soit donc N un espace quadratique totalement isotrope et V_1, V_2 deux espaces quadratiques non dégénérés tels que $N \oplus V_1$ et $N \oplus V_2$ soient isométriques. En termes matriciels, cela signifie que les matrices définies par blocs $\begin{pmatrix} 0 & 0 \\ 0 & M_1 \end{pmatrix}$ et $\begin{pmatrix} 0 & 0 \\ 0 & M_2 \end{pmatrix}$ sont congruentes. Si on écrit $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ une matrice effectuant cette congruence et qu'on fait le calcul par blocs, on obtient la relation ${}^tDM_1D = M_2$, ce qui démontre que D est inversible puis que M_1 et M_2 sont congruentes.

– Supposons $\lambda \neq 0$ et soit $f : D_1 \oplus V_1 \to D_2 \oplus V_2$ une isométrie, où D_1 et D_2 sont deux droites quadratiques isométriques à $\langle\lambda\rangle$. Notons e_1 (resp. e_2) un vecteur générateur de D_1 (resp. D_2). La forme quadratique sur $D_2 \oplus V_2$ prend la même valeur, λ, en $f(e_1)$ et e_2. D'après ce qui précède, il existe donc une isométrie g de cette forme quadratique telle que $g(f(e_1)) = e_2$. L'isométrie $g \circ f$ est donc une isométrie $D_1 \oplus V_1 \to D_2 \oplus V_2$ envoyant bijectivement D_1 sur D_2. Elle envoie donc l'orthogonal du premier sur l'orthogonal du second, c'est-à-dire qu'elle réalise une isométrie $V_1 \to V_2$.

10. Imaginons que nous ayons deux décompositions de Witt :

$$V = V_{ti} \oplus V_{hyp} \oplus V_{an} = V'_{ti} \oplus V'_{hyp} \oplus V'_{an}.$$

On obtient directement que le noyau de l'espace quadratique V est V_{ti}. On a donc $V_{ti} = V'_{ti}$. Le théorème de simplification implique alors que $V_{hyp} \oplus V_{an} \simeq V'_{hyp} \oplus V'_{an}$ (en fait, on pourrait ici éviter d'utiliser ce théorème : il n'est pas très dur de se convaincre que la « partie non dégénérée » d'un espace quadratique est bien définie à isométrie près, par exemple en la définissant directement sur le quotient de V par son noyau.) V_{hyp} et V'_{hyp} sont les sommes de m et m' copies du plan hyperbolique, respectivement. Supposons $m' \geq m$. En appliquant le théorème de simplification, on obtient une isométrie $H \oplus V_{an} \simeq V'_{an}$ où H est la somme de $m' - m$ copies du plan hyperbolique. Puisque V'_{an} est anisotrope, il vient $m = m'$ (donc V_{hyp} et V'_{hyp} étaient isométriques !) et $V_{an} \simeq V'_{an}$. On a donc bien démontré que les types d'isométrie des facteurs étaient bien définis.

Remarquons qu'en revanche, à part V_{ti} qui est le noyau de V, les autres facteurs ne sont pas bien définis comme parties de V. En effet, la forme quadratique $(x, y) \mapsto y^2$, par exemple, va se décomposer sous la forme $V_{ti} \oplus V_{hyp} \oplus V_{an}$ avec $V_{ti} = \mathrm{Vect}(e_1)$ et $V_{hyp} = \{0\}$ mais toute droite supplémentaire de V_{ti} peut jouer le rôle de V_{an} ! (Bien sûr, la restriction de la forme quadratique à chacune de ces droites sera isométrique à la forme $\langle 1\rangle$, mais la droite elle-même n'est pas bien déterminée).

Il n'est pas difficile de déduire de ce qui précède que l'opération consistant à associer à deux formes anisotropes V et V′ la partie anisotrope $(V \oplus V')_{an}$ de leur somme directe munit l'ensemble des classes d'isométrie de formes anisotropes d'une loi de groupe. C'est ce qu'on appelle le *groupe de Witt* du corps k, souvent noté $W(k)$. À titre d'exercice, on pourra déterminer le groupe de Witt $W(\mathbf{R})$.

Exercice 4.

1. On sait qu'il y a $(q+1)/2$ carrés dans $\mathbf{F}_q$, donc lorsque y parcourt $\mathbf{F}_q$, $\frac{by^2-1}{a}$ prend $\frac{q+1}{2}$ valeurs. Nécessairement l'une de ces valeurs est un carré (il n'y a que $\frac{q-1}{2}$ non-carrés dans $\mathbf{F}_q$).

2. On choisit une base orthogonale pour Q, dans laquelle on a $\mathrm{Q}(x,y) = ax^2 + by^2$. Par la question précédente, on peut donc trouver un vecteur $e_1 = (x,y)$ tel que $\mathrm{Q}(e_1) = 1$. Soit alors e_2 un vecteur orthogonal à e_1. Si $\mathrm{Q}(e_2) = \lambda^2 \in \mathbf{F}_q^{*2}$, alors on peut remplacer e_2 par $\lambda^{-1}e_2$ pour obtenir la matrice identité. Par contre, si $\mathrm{Q}(e_2)$ n'est pas un carré, alors il est de la forme $\mathrm{Q}(e_2) = \lambda^2\alpha$, car les carrés forment un sous-groupe d'indice deux dans $\mathbf{F}_q^*$. On remplace alors e_2 par $\lambda^{-1}e_2$.
3. Procédons par récurrence sur n. Partant d'une base orthogonale $(e_1, \ldots, e_n)$, la question 1 affirme qu'il existe un vecteur ε_1 du plan $\mathrm{Vect}(e_1, e_2)$ tel que $\mathrm{Q}(\varepsilon_1) = 1$. On peut ensuite appliquer l'hypothèse de récurrence à l'hyperplan $\mathrm{Vect}(\varepsilon_1)^\perp$. Notons que des formes quadratiques correspondant aux deux classes ne peuvent être équivalentes car leurs discriminants sont différents.